DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 170, 171

RIN 0955–AA03

Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing

AGENCY: Office of the National Coordinator for Health Information Technology (ONC), Department of Health and Human Services (HHS).

ACTION: Final rule.

SUMMARY: This final rule implements the Electronic Health Record (EHR) Reporting Program provision of the 21st Century Cures Act by establishing new Conditions and Maintenance of Certification requirements for health information technology (health IT) developers under the ONC Health IT Certification Program (Program). This final rule also makes several updates to certification criteria and standards recognized by the Program. The Program updates include revised certification criteria for ''decision support interventions,'' ''patient demographics and observations,'' and ''electronic case reporting,'' as well as a new baseline version of the United States Core Data for Interoperability (USCDI) standard to Version 3. Additionally, this final rule provides enhancements to support information sharing under the information blocking regulations. The implementation of these provisions advances interoperability, improves algorithm transparency, and supports the access, exchange, and use of electronic health information (EHI). This final rule also updates numerous technical standards in the Program in additional ways to advance interoperability, enhance health IT certification, and reduce burden and costs for health IT developers and users of health IT.

DATES:

Effective date: This final rule is effective on February 8, 2024.

Incorporation by reference: The incorporation by reference of certain publications listed in the rule was approved by the Director of the Federal Register as of February 8, 2024.

FOR FURTHER INFORMATION CONTACT: Michael Lipinski, Office of Policy, Office of the National Coordinator for Health Information Technology, 202–690–7151.

SUPPLEMENTARY INFORMATION:

Table of Contents

I. Executive Summary
A. Purpose of Regulatory Action
1. Statutory Responsibilities and Implementation
2. Administration Executive Orders
3. Federal Coordination
B. Summary of Major Provisions
1. ONC Health IT Certification Program Updates
a. ''The ONC Certification Criteria for Health IT'' and Discontinuing Year Themed ''Editions''
b. New and Revised Standards and Certification Criteria
i. The United States Core Data for Interoperability Version 3 (USCDI v3)
ii. C–CDA Companion Guide Updates
iii. ''Minimum Standards'' Code Sets Updates
iv. Electronic Case Reporting
v. Decision Support Interventions and Predictive Models
vi. Synchronized Clocks Standard
vii. Standardized API for Patient and Population Services
viii. Patient Demographics and Observations Certification Criterion in § 170.315(a)(5)
ix. Updates to Transitions of Care Certification Criterion in § 170.315(b)(1)
x. Patient Right To Request a Restriction on Use or Disclosure
xi. Requirement for Health IT Developers To Update Their Previously Certified Health IT
2. Assurances Condition and Maintenance of Certification Requirements
3. Real World Testing—Inherited Certified Status
4. Insights Condition and Maintenance of Certification
5. Information Blocking Enhancements
C. Costs and Benefits
II. Background
A. Statutory Basis
1. Standards, Implementation Specifications, and Certification Criteria
2. Health IT Certification Program(s)
B. Regulatory History
C. General Comments on the HTI–1 Proposed Rule
III. ONC Health IT Certification Program Updates
A. ''The ONC Certification Criteria for Health IT'' and Discontinuing Year Themed ''Editions,'' Definition of Revised Certification Criterion, and Related Program Oversight
1. Discontinuing Year Themed ''Editions''
2. Definition of ''Revised Certification Criterion''
3. Program Oversight Related to Discontinuation of Editions
a. Records Retention
b. Records Retention—Complete EHR
B. Standards and Implementation Specifications
1. National Technology Transfer and Advancement Act
2. Compliance With Adopted Standards and Implementation Specifications
3. ''Reasonably Available'' to Interested Parties
C. New and Revised Standards and Certification Criteria
1. The United States Core Data for Interoperability Version 3 (USCDI v3)
a. Certification Criteria That Reference USCDI
b. USCDI Standard—Data Classes and Elements Added Since USCDI v1
2. C–CDA Companion Guide Updates
3. ''Minimum Standards'' Code Sets Updates
4. Electronic Case Reporting
5. Decision Support Interventions and Predictive Models
a. Requirements for Decision Support Interventions (DSI) Certification Criterion
b. Updates to Real World Testing Condition for CDS Criterion
6. Synchronized Clocks Standard
7. Standardized API for Patient and Population Services
a. Native Applications and Refresh Tokens
b. FHIR United States Core Implementation Guide Version 5.0.1
c. FHIR Endpoint for Service Base URLs
d. Access Token Revocation
e. SMART App Launch 2.0
8. Patient Demographics and Observations Certification Criterion in § 170.315(a)(5)
9. Updates to Transitions of Care Certification Criterion in § 170.315(b)(1)
10. Patient Right To Request a Restriction on Use or Disclosure
11. Requirement for Health IT Developers To Update Their Previously Certified Health IT
D. Assurances Condition and Maintenance of Certification Requirements
1. Condition of Certification
2. Maintenance of Certification Requirements
E. Real World Testing—Inherited Certified Status
F. Insights Condition and Maintenance of Certification
1. Background and Purpose
2. Insights Condition and Maintenance of Certification—Final Measures
3. Insights Condition and Maintenance of Certification—Requirements
4. Insights Condition and Maintenance of Certification—Process for Reporting
G. Requests for Information
1. Laboratory Data Interoperability Request for Information
2. Request for Information on Pharmacy Interoperability Functionality Within the ONC Health IT Certification Program Including Real-Time Prescription Benefit Capabilities
3. FHIR Standard
IV. Information Blocking Enhancements
A. General Comments Regarding Information Blocking Enhancements
B. Defined Terms
1. Offer Health Information Technology or Offer Health IT
a. Exclusion of Certain Funding Subsidy Arrangements From Offer Health IT Definition
b. Implementation and Use Activities That Are Not an Offering of Health IT
c. Consulting and Legal Services Exclusion From Offer Health IT Definition
2. Health IT Developer of Certified Health IT: Self-Developer Health Care Providers
3. Information Blocking Definition

C. Exceptions
1. Infeasibility
a. Infeasibility Exception—Uncontrollable Events Condition
b. Infeasibility Exception—Third Party Seeking Modification Use
c. Infeasibility Exception—Manner Exception Exhausted
2. TEFCA Manner Exception
D. Information Blocking Requests for Information
1. Additional Exclusions From Offer Health IT—Request for Information
2. Possible Additional TEFCA Reasonable and Necessary Activities—Request for Information
3. Health IT Capabilities for Data Segmentation and User/Patient Access—Request for Information
V. Incorporation by Reference
VI. Collection of Information Requirements
A. Independent Entity
B. Health IT Developers
C. ONC–ACBs
VII. Regulatory Impact Analysis
A. Statement of Need
B. Alternatives Considered
C. Overall Impact
1. Executive Orders 12866 and 13563—Regulatory Planning and Review Analysis
a. Costs and Benefits
b. Accounting Statement and Table
D. Regulatory Flexibility Act
E. Executive Order 13132—Federalism
F. Unfunded Mandates Reform Act of 1995
Regulation Text

I. Executive Summary

A. Purpose of Regulatory Action

The Office of the National Coordinator for Health Information Technology (ONC) is the principal federal entity charged with coordinating nationwide efforts to implement and use advanced health IT and to facilitate the electronic exchange of health information. ONC is at the forefront of the administration's health IT efforts and is a resource to the entire health system to support the adoption of health IT and the promotion of nationwide, standards-based health information exchange to improve healthcare. ONC is focused on two strategic objectives: (1) advancing the development and use of health IT capabilities; and (2) establishing expectations for data sharing. ONC's overall mission, consistent with the policies adopted in this final rule, is to create systemic improvements in health and care through the access, exchange, and use of data.

This final rule fulfills statutory requirements and aligns with administrative priorities; advances equity, innovation, and interoperability; and supports the access, exchange, and use of EHI. It also promotes the responsible development and use of artificial intelligence through transparency and improves patient care through policies that advance standards-based interoperability and EHI exchange, which are central to the Department of Health and Human Services' efforts to enhance and protect the health and well-being of all Americans.

1. Statutory Responsibilities and Implementation

The Secretary of Health and Human Services has delegated to ONC the responsibility to implement certain provisions in Title IV of the 21st Century Cures Act (Pub. L. 114–255, Dec. 13, 2016) (Cures Act) including: the Electronic Health Record (EHR) Reporting Program condition and maintenance of certification requirements under the ONC Health IT Certification Program (Program) and the identification of reasonable and necessary activities that do not constitute information blocking.[1] ONC is also responsible for implementing certain provisions of the Health Information Technology for Economic and Clinical Health Act (Pub. L. 111–5, Feb. 17. 2009) (HITECH Act) of 2009, including, but not limited to, requirements that the National Coordinator perform duties consistent with the development of a nationwide health information technology infrastructure that allows for the electronic use and exchange of information and that promotes a more effective marketplace, greater competition, and increased consumer choice, as well as requirements to keep, or recognize, a program or programs for the voluntary certification of health information technology.

This final rule adopts new and revised standards and requirements for the certification of health IT under the Program. For example, key provisions of this final rule implement the EHR Reporting Program through new Conditions and Maintenance of Certification requirements (referred herein as the Insights Condition) for developers of certified health IT, which will provide transparency into the use and benefits of certified health IT, with an initial focus on interoperability. This final rule revises several Program certification criteria, including criteria related to decision support, electronic case reporting, and standards-based application programming interfaces (APIs), as well as raises the baseline version of the USCDI from Version 1 to Version 3. The adoption of new and revised standards and criteria in this final rule will facilitate interoperability through standardized health information and functionality, which will lead to better care and health outcomes for patients, while reducing burden and costs. Finally, this rule continues to implement the provisions of the Cures Act to improve information sharing—and address information blocking—by providing refined definitions of statutory terms and further identifying practices that are reasonable and necessary and, therefore, do not constitute information blocking.

2. Administration Executive Orders

In addition to fulfilling the HITECH Act's and Cures Act's requirements described above, this final rule supports implementation of Executive Orders (E.O.) 13994, 13985, 14036, 14058, 14091, and 14110. The President issued E.O. 13994 on January 21, 2021, to ensure a data-driven response to COVID–19 and future high-consequence public health threats. The Cures Act and the information blocking provisions in the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program (85 FR 25642) (ONC Cures Act Final Rule) took critical steps to making data available across the healthcare system. Adoption of USCDI v3 in this rule facilitates the gathering, sharing, and publication of public health and emergency response data (*e.g.,* the COVID–19 pandemic) by capturing and promoting the sharing of key data elements related to public health. The updates to API Conditions and Maintenance of Certification requirements, as discussed in section III.C.7, continue the implementation of ONC's statutory responsibilities and efforts to develop and standardize APIs and to help individuals and other authorized health care providers, including those engaged in public health, securely access EHI through the broader adoption of standardized APIs.[2] [3] Additionally, this final rule

[1] Reasonable and necessary activities that do not constitute information blocking, also known as information blocking exceptions, are identified in 45 CFR part 171 subparts B and C. ONC's official website, *HealthIT.gov,* offers a variety of resources on the topic of Information Blocking, including fact sheets, recorded webinars, and frequently asked questions. To learn more, please visit: *https://www.healthit.gov/topic/information-blocking/.*

[2] ONC. (2022, October 18). *API Resource Guide.* ONC Health IT Certification Program API Resource Guide. Retrieved March 16, 2023, from *https://onc-healthit.github.io/api-resource-guide/.*

[3] Section 4002 of the 21st Century Cures Act (Cures Act) establishes a condition of certification that requires health IT developers to publish application programming interfaces (APIs) that allow ''health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor

Continued

adopts consensus-based, industry-developed health IT standards for certified Health IT Modules to support electronic case reporting. As discussed in section III.C.4, among other benefits, electronic case reporting facilitates faster and more efficient disease tracking, prevention, and case management. It also provides more timely and complete data to public health agencies than manual or non-standardized reporting.

We are also committed to advancing health equity, and this final rule is consistent with E.O. 13985 of January 20, 2021, Advancing Racial Equity and Support for Underserved Communities Through the Federal Government,[4] and E.O. 14091 of February 16, 2023, Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government.[5] Section 1 of E.O. 13985 states that ''the Federal Government should pursue a comprehensive approach to advancing equity for all, including people of color and others who have been historically underserved, marginalized, and adversely affected by persistent poverty and inequality.'' Section 1 of E.O. 13985 also states that ''because advancing equity requires a systematic approach to embedding fairness in decision-making processes, executive departments and agencies must recognize and work to redress inequities in their policies and programs that serve as barriers to equal opportunity.'' As noted above, we have adopted USCDI v3 in this final rule to meet statutory responsibilities discussed in section II.A to improve the standardization of health information that is accessed, exchanged, and used within certified health IT. The USCDI v3 standard includes data elements on patient demographics (such as sexual orientation and gender identity) and social determinants of health (SDOH), as discussed in sections III.C.1 and III.C.8 of this final rule. These updates help capture more accurate and complete patient characteristics that are reflective of patient diversity and inclusion, which could potentially help data users address disparities in health outcomes for all patients, including those who may be marginalized and underrepresented. The use of USCDI v3 also supports data users' abilities to identify, assess, and analyze gaps in care, which could in turn be used to inform and address the quality of healthcare through interventions and strategies. This could lead to better patient care, experiences, and health outcomes.

Section 1 of E.O. 14091 also requires the Federal Government to ''promote equity in science and root out bias in the design and use of new technologies, such as artificial intelligence.'' Section 8 of E.O. 14091 requires agencies to ''prevent and address discrimination and advance equity for all'' and to ''consider opportunities to prevent and remedy discrimination, including by protecting the public from algorithmic discrimination.'' The E.O. states that the Federal Government shall continue to ''advance equity in health, including mental and behavioral health and well-being.'' We are committed to the concept of ''health equity by design'',[6] in which health equity considerations are identified and incorporated from inception and throughout the technology design, build, and implementation process. We consider health equity by design to incorporate health equity strategies, tactics, and patterns as guiding principles for software and IT development, enforced by technical architecture, data, and information governance process, and built into the technology at every layer. In this final rule we apply the concept of health equity by design to bring transparency to the quality and performance of intelligence and machine learning-based decision support tools in healthcare. As discussed in section III.C.5, the ''decision support intervention,'' (DSI) certification criterion is supportive of the goals of E.O. 14091 and advances health equity by design by making it known to users of Health IT Modules certified to the DSI criterion whether patient demographic, SDOH, or health assessment data are used in DSIs. Other finalized policies: (1) establish a definition for algorithm-based and model-based ''predictive'' DSIs; (2) require Health IT Modules certified to the DSI criterion to enable users to access information about the design, development, training, and evaluation of Predictive DSIs, including descriptions of training data and information on whether the Predictive DSI was tested and evaluated for fairness; (3) require developers of certified health IT to apply risk management practices for all Predictive DSIs that are supplied by the developer of certified health IT as part of its Health IT Module; and (4) make summary information regarding these practices available publicly.

Additionally, the DSI certification criterion and surrounding transparency requirements are especially aligned with E.O. 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, issued October 30, 2023.[7] The finalized DSI requirements will improve transparency, promote trustworthiness, and incentivize the development and wider use of fair, appropriate, valid, effective, and safe Predictive DSIs to aid decision-making in healthcare. The resulting information transparency increases public trust and confidence in these technologies so that the benefits of these technologies may expand in safer, more appropriate, and more equitable ways. This transparency also informs wider discussions, including those across industry, academia, and government, regarding how to evaluate and communicate performance related to Predictive DSIs, consistent with Section 8 of the E.O., ''Protecting Consumers, Patients, Passengers, and Students.''

The finalized DSI certification criterion also aligns with the public availability and transparency policy goals of the Office of Science and Technology Policy (OSTP) memorandum ''Ensuring Free, Immediate, and Equitable Access to Federally Funded Research.'' [8] The memorandum provides policy guidance to federal agencies and departments to promote improved public access to and transparency of federally funded

technology or standards, as provided for under applicable law.'' The Cures Act's API Condition of Certification requirement also states that a developer must, through an API, ''provide access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws.'' The API Conditions and Maintenance of Certification requirements and certification criteria are identified in 45 CFR part 170.

[4] United States, Executive Office of the President [Joseph Biden]. Executive Order 13985: Advancing Racial Equity and Support for Underserved Communities Through the Federal Government. Jan 20, 2021. 86 FR 7009–7013, *https://www.federalregister.gov/documents/2021/01/25/2021-01753/advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government.*

[5] United States, Executive Office of the President [Joseph Biden]. Executive Order 14091: Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government. Feb 16, 2023. 88 FR 10825–10833, *https://www.federalregister.gov/documents/2023/02/22/2023-03779/further-advancing-racial-equity-and-support-for-underserved-communities-through-the-federal.*

[6] *HealthIT.gov: Embracing Health Equity by Design. https://www.healthit.gov/buzz-blog/health-it/embracing-health-equity-by-design.*

[7] United States, Executive Office of the President [Joseph Biden]. Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. Oct. 20, 2023. 88 FR 75191. *https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.*

[8] Ensuring Free, Immediate, and Equitable Access to Federally Funded Research. Office of Science and Technology Policy (OSTP) (2022). *https://www.whitehouse.gov/wp-content/uploads/2022/08/08-2022-OSTP-Public-access-Memo.pdf.*

research. The finalized DSI certification criterion aligns with the goals of the memorandum by establishing requirements to make information available through § 170.315(b)(11)(iv), including information created through federally funded research and evaluations, that will enable users to determine if a Predictive DSI supplied by a health IT developer as part of its Health IT Module is acceptably fair, appropriate, valid, effective, and safe.

President Biden's E.O. 14036, Promoting Competition in the American Economy, issued on July 9, 2021, established a whole-of-government effort to promote competition in the American economy and reaffirmed the policy stated in E.O. 13725 of April 15, 2016 (Steps to Increase Competition and Better Inform Consumers and Workers to Support Continued Growth of the American Economy).[9] This final rule fosters competition by advancing foundational standards for certified API technology, which enable—through applications (apps) and without special effort—improved legally permissible sharing of EHI among clinicians, patients, researchers, and others. As described in section III.C.7, competition is advanced through these improved API standards that can help individuals connect to their information and can help authorized health care providers, involved in the patient's care, securely access information. For example, these standards are designed to foster an ecosystem of new applications that can connect through the API technology to provide patients with improved electronic access to EHI.

Further, as described in section IV, this final rule provides enhancements to support information sharing under the information blocking regulations and promote innovation and competition, as well as address market consolidation. As we have noted, addressing information blocking is critical for promoting innovation and competition in health IT and for the delivery of healthcare services to individuals. In both the ONC Cures Act Proposed Rule (84 FR 7508) and Final Rule (85 FR 25790 through 25791), we discussed how the information blocking provisions provide a comprehensive response to the issues identified by empirical and economic research. This research suggested that information blocking may weaken competition, encourage consolidation, and create barriers to entry for developers of new and innovative applications and technologies that enable more effective uses of EHI to improve population health and the patient experience.[10] We explained that the information blocking provisions of the Public Health Service Act (PHSA) itself expressly addresses practices that impede innovation and advancements in EHI access, exchange, and use, including care delivery enabled by health IT (section 3022(a)(2)(C)(ii) of the PHSA). Actors subject to the information blocking provisions may,[11] among other practices, attempt to exploit their control over interoperability elements to create barriers to entry for competing technologies and services that offer greater value for health IT customers and users, provide new or improved capabilities, and enable more robust access, exchange, and use of EHI (85 FR 25820).[12] Information blocking may not only harm competition in health IT markets, but also in markets for healthcare services (85 FR 25820). In the ONC Cures Act Final Rule, we described practices that dominant market health care providers may leverage and use to control access and use of their technology, resulting in technical dependence and possibly leading to barriers to entry by would-be competitors, as well as making some market health care providers vulnerable to acquisition or inducement into arrangements that enhance the market power of incumbent health care providers to the detriment of consumers and purchasers of healthcare services (85 FR 25820). The implementation of the new information blocking provisions detailed in section IV of this final rule promote innovation, encourage market competition, and address consolidation in the interest of the patient to advance interoperability, improve transparency, and support the access, exchange, and use of EHI.

Lastly, in support of E.O. 14058, Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government, issued on December 16, 2021, we are committed to advancing the equitable, inclusive, and effective delivery of services with a focus on the experience of individuals, health IT developers, and health care providers.[13] As required by section 4002 of the Cures Act and included in the ONC Cures Act Final Rule (85 FR 25717), we established certain Conditions and Maintenance of Certification requirements, which express initial and ongoing requirements for health IT developers and their certified Health IT Module(s) under the Program. This final rule implements the EHR Reporting Program Condition and Maintenance of Certification requirement outlined in the Cures Act by establishing—within the Program—a new Condition and Maintenance of Certification hereafter referred to as the ''Insights Condition.'' As discussed in section III.F, the implementation of the Insights Condition provides transparent reporting to address information gaps in the health IT marketplace and provides insights on the use of specific certified health IT functionalities. The implementation of this new Condition and Maintenance of Certification requirement will allow ONC to gain a better understanding of the use of health IT and provide ONC with information about consumers' experience with certified health IT.

3. Federal Coordination

We strive to improve federal agency coordination. ONC works with the Centers for Medicare & Medicaid Services (CMS) to ensure that the certification timelines we have established complement timelines for CMS programs that reference ONC regulations, such as the Medicare Promoting Interoperability Program and

[9] United States, Executive Office of the President [Joseph Biden]. Executive Order 14036: Promoting Competition in the American Economy. Jul 9, 2021. 86 FR 36987–36999, *https://www.federalregister.gov/documents/2021/07/14/2021-15069/promoting-competition-in-the-american-economy.*

[10] *See, e.g.,* Martin Gaynor, Farzad Mostashari, and Paul B. Ginsberg, Making Health Care Markets Work: Competition Policy for Health Care, 16–17 (Apr. 2017), available at *http://heinz.cmu.edu/news/news-detail/index.aspx?nid=3930;* Diego A. Martinez et al., A Strategic Gaming Model For Health Information Exchange Markets, Health Care Mgmt. Science (Sept. 2016). (''[S]ome healthcare provider entities may be interfering with HIE across disparate and unaffiliated providers to gain market advantage.'') Niam Yaraghi, A Sustainable Business Model for Health Information Exchange Platforms: The Solution to Interoperability in Healthcare IT (2015), available at *http://www.brookings.edu/research/papers/2015/01/30-sustainable-business-model-health-information-exchange-yaraghi;* Thomas C. Tsai Ashish K. Jha, Hospital Consolidation, Competition, and Quality: Is Bigger Necessarily Better? 312 J. AM. MED. ASSOC. 29, 29 (2014).

[11] The information blocking regulations in 45 CFR part 171 apply to health care providers, health IT developers of certified health IT, and health information networks (HIN) and health information exchanges (HIE), as each is defined in 45 CFR 171.102. Any individual or entity that meets one of these definitions is an ''actor'' and subject to the information blocking regulation in 45 CFR part 171.

[12] See also Martin Gaynor, Farzad Mostashari, and Paul B. Ginsberg, Making Health Care Markets Work: Competition Policy for Health Care, 16–17 (Apr. 2017), available at *http://heinz.cmu.edu/news/news-detail/index.aspx?nid=3930.*

[13] United States, Executive Office of the President [Joseph Biden]. Executive Order 14058: Transforming Federal Customer Experience and Service Delivery To Rebuild Trust in Government. Dec 13, 2021. 86 FR 71357–71366, *https://www.federalregister.gov/documents/2021/12/16/2021-27380/transforming-federal-customer-experience-and-service-delivery-to-rebuild-trust-in-government.*

the Promoting Interoperability performance category of the Merit-based Incentive Payment System (MIPS). In the interest of clarity and cohesion among HHS components, we have aligned some of our compliance dates to the calendar year for consistency with calendar-year based performance periods in CMS programs when participants may be required to use updated certified health IT. We believe this approach reduces confusion for participants in these programs and better serves the public interest.

B. Summary of Major Provisions

1. ONC Health IT Certification Program Updates

a. ''The ONC Certification Criteria for Health IT'' and Discontinuing Year Themed ''Editions''

We noted in the HTI–1 Proposed Rule that we no longer believed that it was helpful or necessary to maintain an ''edition'' naming convention or to adopt entirely new editions of certification criteria to encapsulate updates over time (88 FR 23750). Instead, we conveyed that there should be a single set of certification criteria, which would be updated in an incremental fashion in closer alignment to standards development cycles and regular health IT development timelines. In section III.A, we discuss our final policy to rename all certification criteria within the Program simply as ''ONC Certification Criteria for Health IT.''

b. New and Revised Standards and Certification Criteria

i. The United States Core Data for Interoperability Version 3 (USCDI v3)

We noted in the HTI–1 Proposed Rule that because USCDI is the standard for data required to be accessible through certified health IT for numerous certification criteria, expanding the data elements and data classes included in USCDI increases the amount of data available to be used and exchanged for patient care (88 FR 23751). To expand standardized data reporting, we have finalized the proposal to codify USCDI v1 in § 170.213(a) and to add USCDI v3 to § 170.213 (to be codified as § 170.213(b)). We have incorporated USCDI v3 by reference in § 170.299 as of the effective date of this final rule. Lastly, we have finalized that the USCDI v1 (July 2020 Errata) in the USCDI standard in § 170.213(a) will expire on January 1, 2026. As codified in § 170.213, only USCDI v3 will be available in the Program as of January 1, 2026.

ii. C–CDA Companion Guide Updates

As discussed in section III.C.2, we have finalized the adoption of the HL7® CDA® R2 Implementation Guide: C–CDA Templates for Clinical Notes STU Companion Guide, Release 4.1—US Realm (C–CDA Companion Guide R4.1) in § 170.205(a)(6) because it is the only version that provides guidance and clarifications for specifying data in USCDI v3.

iii. ''Minimum Standards'' Code Sets Updates

In the 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications Final Rule (2015 Edition Final Rule), we established a policy of adopting newer versions of ''minimum standards'' code sets that frequently update (80 FR 62612). Adopting newer versions of these code sets enables improved interoperability and implementation of health IT with minimal additional burden (77 FR 54170). We discussed in the HTI–1 Proposed Rule that, if adopted, newer versions of these minimum standards code sets would serve as the baseline for certification, and developers of certified health IT would be able to use newer versions of these adopted standards on a voluntary basis (88 FR 23751). We have finalized, as discussed in section III.C.3, the adoption of the versions we had proposed of the following minimum standards code sets:

- § 170.207(a)—Problems
- § 170.207(c)—Laboratory tests
- § 170.207(d)—Medications
- § 170.207(e)—Immunizations
- § 170.207(f)—Race and ethnicity
- § 170.207(m)—Numerical references
- § 170.207(n)—Sex
- § 170.207(o)—Sexual orientation and gender information
- § 170.207(p)—Social, psychological, and behavioral data
- § 170.207(r)—Provider type
- § 170.207(s)—Patient insurance

In addition to the finalized adoption of the minimum standards code sets listed above, we have finalized proposed updates to certification criteria that reference those minimum standards. These criteria include § 170.315(a)(5)(i)(A)(*1*) and (*2*), (a)(5)(i)(C) through (E), (a)(12), (b)(1)(iii)(B)(*2*), (b)(1)(iii)(G)(*3*), (b)(6)(ii)(B)(*2*), (c)(4)(iii)(C), (c)(4)(iii)(E), (c)(4)(iii)(G) through (I), (f)(1)(i)(B) and (C), (f)(3)(ii), and (f)(4)(ii).

We have finalized the proposal to change the heading of § 170.207(o) to ''sexual orientation and gender information'' to acknowledge that § 170.207(o) includes standard code sets to support gender-related data items in addition to standard code sets to support sexual orientation.

iv. Electronic Case Reporting

As discussed in section III.C.4 of this final rule, we have finalized the revisions to the ''transmission to public health agencies—electronic case reporting'' criterion in § 170.315(f)(5) to adopt consensus-based, industry-developed electronic standards and implementation guides (IGs) to replace all functional, descriptive requirements in the present criterion in § 170.315(f)(5). These standards will support the following requirements for Health IT Modules certified to § 170.315(f)(5): (i) create a case report for electronic transmission; (ii) consume and process a case report response; and (iii) consume and process electronic case reporting trigger codes. We note that these electronic standards are standards-based representations of the functional requirements described in the existing criterion in § 170.315(f)(5) as described in section III.C.4 of this preamble.

v. Decision Support Interventions and Predictive Models

As discussed in section III.C.5 of this final rule, we have finalized the adoption of the certification criterion, ''decision support interventions (DSI)'' in § 170.315(b)(11). The DSI criterion is a revised certification criterion, serving both an iterative update and replacement criterion for the ''clinical decision support (CDS)'' certification criterion in § 170.315(a)(9) (88 FR 23751). The DSI criterion, as finalized, ensures that Health IT Modules certified to § 170.315(b)(11) reflect an array of contemporary functionalities, support data elements important to health equity, and enable the transparent use of predictive models and algorithms to aid decision-making in healthcare.

We have adopted a new definition for Predictive Decision Support Intervention, (also referred to hereafter as Predictive DSI) in § 170.102, and we have finalized that Health IT Modules certified to § 170.315(b)(11) must enable a limited set of identified users to select (*i.e.,* activate) evidence-based and Predictive DSIs, as described in § 170.315(b)(11)(iii). Additionally, we have finalized that Health IT Modules certified to § 170.315(b)(11) must support ''source attributes''—categories of technical performance and quality information—for both evidence-based

and Predictive DSIs in § 170.315(b)(11)(iv).

We have *not* finalized proposed requirements that Health IT Modules clearly indicate when source attributes from *other parties* are unavailable. Rather, we have finalized that Health IT Modules certified to § 170.315(b)(11) must enable a limited set of identified users to access complete and up-to-date descriptions of all source attributes related to evidence-based DSIs and Predictive DSIs that are supplied by the developer of certified health IT as part of their Health IT Module, as described in § 170.315(b)(11)(v)(A). Moreover, we have finalized in § 170.315(b)(11)(v)(B) requirements that Health IT Modules certified to § 170.315(b)(11) must enable a limited set of identified users to record and change source attributes listed in paragraphs § 170.315(b)(11)(iv)(A) and (B).

We have also finalized in § 170.315(b)(11)(vi) that intervention risk management (IRM) practices must be applied for each Predictive DSI supplied by the health IT developer as part of its Health IT Module, including requirements to subject Predictive DSIs to risk analysis and risk mitigation related to validity, reliability, robustness, fairness, intelligibility, safety, security, and privacy. We note that for governance practices, we have finalized in § 170.315(b)(11)(vi)(C) requirements for Health IT Modules to be subject to policies and implemented controls for governance, including how data are acquired, managed, and used. Consistent with the other IRM practices, these policies and implemented controls must be applied for all Predictive DSIs supplied by the health IT developer as part of its Health IT Module.

Additionally, in consideration of comments received and the scope reductions we have made to this final certification criterion, we determined that a supportive Maintenance of Certification requirement as part of the Assurances Condition of Certification is necessary to implement our policy objectives and proposals fully. Specifically, we have included in this final rule a Maintenance of Certification requirement at 45 CFR 170.402(b)(4) that reinforces a health IT developer's ongoing responsibility to review and update, as necessary, source attribute information in § 170.315(b)(11)(v)(A) and (B), risk management practices described in § 170.315(b)(11)(vi), and summary information provided through § 170.523(f)(1)(xxi). We have finalized in § 170.402(b)(4) that developers with products certified to § 170.315(b)(11) will need to comply with this Maintenance of Certification requirement starting January 1, 2025.

Finally, we have finalized our proposals to facilitate this transition from one version of the criterion to the other by updating the 2015 Edition Base EHR definition in § 170.102,[14] which is being replaced with a definition of Base EHR, to include an option for a Health IT Module to meet the definition by either being certified to the existing CDS version of the certification criterion in § 170.315(a)(9), or being certified to the revised DSI criterion in § 170.315(b)(11), for the period up to, and including, December 31, 2024. On and after January 1, 2025, only the DSI criterion in § 170.315(b)(11) will be included in the Base EHR definition and the adoption of the criterion in § 170.315(a)(9) will expire on January 1, 2025. We discuss in section III.C.5.b of this preamble policies that would constitute changes to the CDS criterion, as the new DSI criterion.

vi. Synchronized Clocks Standard

We have finalized, as discussed in section III.C.6, the removal of the current named specification for clock synchronization, which is Network Time Protocol (NTP v4 of RFC 5905), in § 170.210(g). Additionally, we have finalized the requirement for any network time protocol (NTP) standard to be used that can ensure a system clock has been synchronized and meets time accuracy requirements.

vii. Standardized API for Patient and Population Services

We have finalized, as discussed in section III.C.7, the proposed revisions to the ''standardized API for patient and population services'' certification criterion in § 170.315(g)(10). We have finalized the requirement that a certified Health IT Module's authorization server issues a refresh token according to the implementation specification adopted in § 170.215(c).

We have also finalized the proposed revisions in § 170.315(g)(10)(vi) to specify that Health IT Modules presented for certification that allow short-lived access tokens to expire, in lieu of immediate access token revocation, must have such access tokens expire within one hour of the request. This revised requirement aligns with industry standard practice for short-lived access tokens, provides clarity and consistent expectations that developers revoke access or expire access privileges within one hour of a request, and offers patients an assurance that an application's access to their data will be revoked or expired within one hour of a request.

We have also adopted the HL7® FHIR® US Core Implementation Guide (IG) STU version 6.1.0 (FHIR US Core 6.1.0) in § 170.215(b)(1)(ii). This version of the US Core IG provides the latest consensus-based capabilities aligned with USCDI v3 data elements for FHIR APIs.

Additionally, we have finalized the proposal to amend the API Condition and Maintenance of Certification requirements by adding the requirement that Certified API Developers with patient-facing apps must meet the publication requirements associated with service base URLs according to a specified format.

We have adopted the Substitutable Medical Applications, Reusable Technologies (SMART) App Launch Implementation Guide Release 2.0.0 (SMART v2 Guide) in § 170.215(c)(2), which replaces the SMART Application Launch Framework Implementation Guide Release 1.0.0 (SMART v1 Guide) as the standard in § 170.215(a)(3) (finalized in this rule as § 170.215(c)(1)). Adoption of this standard impacts the certification criterion in § 170.315(g)(10) in several subparagraphs. The SMART v2 Guide builds on the features of the SMART v1 Guide by including new features and technical revisions based on industry consensus, including features that reflect security best practices. The SMART v1 Guide will continue to be available as a standard for use in the Program through December 31, 2025. Beginning January 1, 2026, the SMART v2 Guide will be the only version of the IG available for use in the Program.

viii. Patient Demographics and Observations Certification Criterion in § 170.315(a)(5)

We have finalized, as discussed in section III.C.1 of this final rule, the adoption of USCDI v3, which includes certain data elements, namely Sex, Sexual Orientation, and Gender Identity, that are also data elements in § 170.315(a)(5). As discussed in section III.C.8 of this preamble, to ensure consistency, we have finalized the name change of the certification criterion in § 170.315(a)(5) from ''demographics'' to ''patient demographics and observations.'' Additionally, to ensure consistent capture of these data elements across health IT, we carry these changes into their respective data elements in § 170.315(a)(5), as discussed in section III.C.8.

[14] In section III.C.5.a.i., we discuss finalizing our proposal to adopt a definition of ''Base EHR'' and remove the prior definition of ''2015 Edition Base EHR.''

We have finalized the replacement of the specific concepts referenced in § 170.315(a)(5)(i)(D) and (E), Sexual Orientation and Gender Identity, respectively, with the Systematized Nomenclature of Medicine Clinical Terms U.S. Edition (SNOMED CT®) code set, as referenced in the standard in § 170.207(o)(3). We have also finalized our proposal that the adoption of the code sets referenced in § 170.207(n)(1) will expire on January 1, 2026, and that health IT developers can continue to use the specific codes in the current terminology standard through December 31, 2025, in order to provide adequate time for Health IT Modules certified to particular certification criteria to transition to the updated terminology standards.

We have finalized the addition of Sex Parameter for Clinical Use as a new data element in § 170.315(a)(5)(i)(F). As discussed in section III.C.1 of this final rule, we proposed Sex for Clinical Use in the HTI–1 Proposed Rule and have revised the title of Sex for Clinical Use to instead be Sex Parameter for Clinical Use (SPCU) to align with changes made by the HL7 Gender Harmony Project and updated the title in § 170.315(a)(5)(i)(F). The data element definition did not change. Additionally, we have finalized new data elements—Name to Use in § 170.315(a)(5)(i)(G) and Pronouns in § 170.315(a)(5)(i)(H)—to facilitate data capture that supports providers' ability to provide culturally competent care for their patients.

ix. Updates to Transitions of Care Certification Criterion in § 170.315(b)(1)

We have finalized, as discussed in section III.C.9, the proposed updates to the ''transitions of care'' certification criterion (§ 170.315(b)(1)) to align it with our adoption of USCDI v3 in § 170.213(b). This change ensures that Health IT Modules certified to § 170.315(b)(1) are capable of accessing, exchanging, and using USCDI data elements referenced in the standards in § 170.213.

x. Patient Right To Request a Restriction on Use or Disclosure

We stated in the HTI–1 Proposed Rule that we believed that individuals should be provided a reasonable opportunity and technical capability to make informed decisions about the collection, use, and disclosure of their electronic health information (88 FR 23753). The Health Insurance Portability and Accountability Act (HIPAA) [15] Privacy Rule [16] provides individuals with several legal, enforceable rights that empower them to manage their health information. We made several proposals in support of the HIPAA Privacy Rule's individual right to request restriction of certain uses and disclosures of their protected health information [17] (PHI) (*see also* 45 CFR 154.522(a)). In this final rule, we have finalized a requirement for Health IT Modules certified to the ''view, download, and transmit to a 3rd party,'' certification criterion in § 170.315(e)(1) to support an ''internet-based method'' for a patient to request a restriction as proposed. Based on the feedback received from numerous interested parties, we have decided not to finalize the remainder of our proposals for patient requested restrictions at this time. We will continue to monitor standards development efforts in this space.

xi. Requirement for Health IT Developers To Update Their Previously Certified Health IT

We have finalized our proposal to add text to the introductory text in § 170.315 stating that health IT developers participating in the Program must update their certified Health IT Modules and provide that updated certified health IT to customers in accordance with the timelines defined for a specific criterion or standard included in § 170.315. More specifically, we have finalized, as discussed in section III.C.11, that health IT developers with health IT certified to any of the certification criteria in § 170.315 will need to update their previously certified Health IT Modules to be compliant with any revised certification criterion adopted in § 170.315, including any new standards adopted in 45 CFR part 170 subpart B and capabilities included in the revised certification criterion. We have further finalized the requirement that health IT developers will also need to provide the updated health IT to customers of the previously certified health IT according to the dates established for that criterion and any applicable standards.

2. Assurances Condition and Maintenance of Certification Requirements

We have finalized, as discussed in section III.D, additional Assurances Condition and Maintenance of Certification requirements. We have finalized as a Condition of Certification that a health IT developer must provide an assurance that it will not interfere with a customer's timely access to interoperable health IT certified under the Program. To support this assurance, we have finalized two accompanying Maintenance of Certification requirements. We have finalized that a health IT developer must update a Health IT Module, once certified to a certification criterion adopted in § 170.315, to all applicable revised certification criteria, including the most recently adopted capabilities and standards included in the revised certification criterion. We have also finalized that a health IT developer must provide all Health IT Modules certified to a revised certification criterion to its customers of such certified health IT. In response to comments and to provide regulatory clarity, we have revised the separate ''timely access'' or ''timeliness'' requirements for each of the two proposed Maintenance of Certification requirements. Rather than relying on independent timeliness requirements for previously certified health IT, the maintenance requirements now cross-reference timeframes specified in 45 CFR part 170, while still maintaining the proposed minimum 12-month timeframe for new customers.

3. Real World Testing—Inherited Certified Status

Section 4002(a) of the Cures Act added a new Condition and Maintenance of Certification requirement that health IT developers must successfully test the real-world use of health IT for interoperability in the type(s) of setting(s) in which such technology would be marketed. Many health IT developers update their certified Health IT Module(s) on a regular basis, leveraging the flexibility provided through ONC's Inherited Certified Status (ICS).[18] Because of the way that ONC issues certification identifiers, this updating can cause an existing certified Health IT Module to be recognized as new within the Program. Regular updating, especially on a frequent basis (such as quarterly or semi-annually), creates an anomaly that could result in existing certified Health IT Modules being inadvertently excluded from the real world testing reporting requirements (88 FR 23753).

To ensure that all developers continue to test the real-world use of their technology as required, we have finalized, as discussed in section III.E,

[15] Public Law 104–191,110 Stat. 1936 (August 21, 1996), codified at 42 U.S.C. 1320d–1320d8.

[16] 45 CFR part 160 and subparts A and E of part 164.

[17] 45 CFR 160.103 (definition of ''Protected health information'').

[18] See 2015 Edition Cures Update Fact Sheet: *https://www.healthit.gov/sites/default/files/page/2022-03/Cures-Update-Fact-Sheet.pdf.*

the proposal to eliminate this anomaly by requiring health IT developers to include in their real world testing results report the newer version of those certified Health IT Module(s) that are updated using ICS after August 31 of the year in which the plan is submitted. This will ensure that health IT developers fully test all applicable certified Health IT Module(s) as part of their real world testing requirements.

4. Insights Condition and Maintenance of Certification

The Cures Act specified requirements in section 4002(c) to establish an EHR Reporting Program to provide reporting on certified health IT in the categories of interoperability, usability and user-centered design, security, conformance to certification testing, and other categories as appropriate to measure the performance of EHR technology. The Cures Act also specified, in text added at section 3009A(b) of the Public Health Service Act, that a health IT developer be required, as a Condition and Maintenance of Certification requirement under the ONC Health IT Certification Program, to submit responses to reporting criteria in accordance with the EHR Reporting Program established with respect to all certified technology offered by such developer. For clarity, we refer to the Condition and Maintenance of Certification associated with the ''EHR Reporting Program'' as the ''Insights Condition and Maintenance of Certification'' (also referred to as the ''Insights Condition'') throughout this final rule. We believe this descriptive name captures the essence of this requirement and will help avoid confusion that might occur through use of the term ''EHR Reporting Program.''

In section III.F, we have adopted seven reporting measures for developers of certified health IT that focus initially on the interoperability category, emphasizing four areas of interoperability: (1) individuals' access to electronic health information; (2) public health information exchange; (3) clinical care information exchange; and (4) standards adoption and conformance. Through this first set of finalized measures, we intend to provide insights on the interoperability category specified in the Cures Act. We intend to explore the other Cures Act categories (security, usability and user-centered design, conformance to certification testing, and other categories to measure the performance of EHR technology) in future years.

We have also finalized, as discussed in section III.F, the implementation of the Insights Condition requirements in § 170.407 in three phases over three years, where health IT developers to which the requirements apply, will be required to report on some of the measures earlier than others. For each final measure, we have included information on the rationale for adopting the measure, the final metrics, and other key topics. The Insights Condition will provide transparent reporting, address information gaps in the health IT marketplace, and provide insights on the use of health IT.

5. Information Blocking Enhancements

As discussed in section IV.B.1 of this preamble, we have finalized a definition of ''offer health information technology'' or ''offer health IT'' for purposes of the information blocking regulations in 45 CFR part 171. This definition of ''offer health IT,'' as finalized in § 171.102, narrows the applicability of the ''health IT developer of certified health IT'' definition in 45 CFR 171.102. The definition of ''offer health IT,'' finalized in 45 CFR 171.102, will generally continue to include holding out for sale, selling, or otherwise supplying certified health IT to others on commercial or other terms. However, our finalized definition of ''offer health IT'' explicitly excludes certain activities and arrangements. First, the ''offer health IT'' definition excludes making available funding to obtain or maintain certified health IT, provided the funding is made available without condition(s) limiting the interoperability, or use of the technology to access, exchange or use electronic health information for any lawful purpose (*see* paragraph (1) of the offer health IT definition). Second, the finalized ''offer health IT'' definition also explicitly codifies that health care providers or other health IT users do not ''offer health IT'' when they engage in certain health IT implementation and use activities, regardless of whether they obtain that health IT from a commercial developer or a reseller or develop it themselves (*see* paragraph (2) of the offer health IT definition).

We have also finalized (in paragraph (3) of the ''offer health IT'' definition) an exclusion from the ''offer health IT'' definition that applies to certain consulting and legal services. This consulting and legal services exclusion (*see* subparagraph (3)(iii)) encompasses supplying health IT in complement to the other items, supplies, facilities, and services that a consultant handles for a clinician practice or other health care provider in a comprehensive (''turn key'') package of services for administrative or operational management (*see* section IV.B.1.c.iii of this preamble). The consulting and legal services exclusion from the ''offer health IT'' definition also encompasses assistance by health IT consultants with the selection, implementation, and use of health IT as specified in subparagraph (3)(ii) and legal services furnished by outside counsel as specified in subparagraph (3)(i).

As discussed in section IV.B.2, we have modified the ''health IT developer of certified health IT'' definition so that it is clear that health care providers who self-develop certified health IT will continue to be excluded from this definition if they do not engage in activities falling within the ''offer health IT'' definition. The updated § 171.102 health IT developer of certified health IT definition we have finalized represents a change from prior policy to the extent that a health care provider that is a self-developer would not meet the definition of ''health IT developer of certified health IT'' if they supply certified health IT to one or more other health care provider(s) under a comprehensive and predominantly non-health IT administrative or operations management services arrangement consistent with subparagraph (3)(iii) (under the consulting and legal services exclusion from the 45 CFR 171.102 ''offer health IT'' definition). Previously, health care providers who self-developed certified health IT were excluded from the 45 CFR 171.102 ''health IT developer of certified health IT'' definition if they self-developed the Health IT Module(s) for their ''own use'' (85 FR 25799 and 25956).

We have finalized revisions to the text of § 171.103, which defines ''information blocking'' for purposes of 45 CFR part 171, to remove paragraph (b) that established a period of time during which electronic health information (EHI) for purposes of the information blocking provision (§ 171.103) was limited to a subset of EHI that was identified by the data elements represented in the USCDI standard adopted in § 170.213. As established in the ONC Cures Act Final Rule (85 FR 25793, 85 FR 25876, and 85 FR 25956), that period of time ended on May 2, 2022. The end date of that period of time was extended to October 5, 2022, in the subsequent interim final rule with comment titled ''Information Blocking and the ONC Health IT Certification Program: Extension of the Compliance Dates and Timeframes in Response to the COVID–19 Public Health Emergency'' (85 FR 70064). On and after October 6, 2022, the scope of EHI for purposes of the ''information blocking'' definition (§ 171.103) is EHI as defined in § 171.102 (88 FR 23754, *see also* 85 FR 25793, 25876, 70069, and

70085). October 5, 2022, has passed. Therefore, the paragraph (which had been designated paragraph (b), as codified) limiting the ''information blocking'' definition to the subset of EHI for the specified time period is no longer needed. We have re-designated remaining paragraphs of § 171.103 as discussed in section IV.B.3 and as shown in updated text we have finalized in § 171.103 (*see* Regulation Text, *see also* discussion in section IV.B.3).

We note that in the HTI–1 Proposed Rule we did not propose to change the scope of EHI for purposes of the information blocking definition (88 FR 23754). We simply proposed to update the CFR text to remove paragraph (b) from § 171.103 that had temporarily—until October 5, 2022—limited the scope of the information blocking definition to the subset of EHI represented by USCDI v1 (88 FR 23864 and 23916). Similarly, because we included the same time period in reference to the scope of EHI in two paragraphs of the Content and Manner Exception (§ 171.301(a)(1) and (2)), we proposed to revise § 171.301 to remove from the regulatory text the existing § 171.301(a)(1) and (2) as no longer necessary (88 FR 23754). We have finalized the revisions to § 171.301 to remove the regulatory text in subparagraphs (a)(1) and (2) as no longer necessary and rename § 171.301 the Manner Exception. We have finalized the redesignation of the paragraphs now codified within § 171.301, so that different paragraphs are now designated (a)(1) and (2) rather than the paragraphs we have removed as no longer necessary (*see* discussion in sections IV.B.3 and IV.C.2, *see also* Regulation Text for revised and redesignated paragraphs of § 171.301).

As explained in section IV.C.1, we have finalized revisions to the Infeasibility Exception codified in 45 CFR 171.204 both by adding two new conditions and by revising one existing condition for improved clarity. First, we have finalized revisions to the *uncontrollable events* condition in § 171.204(a)(1) to further clarify when an actor's practice meets the *uncontrollable events* condition. Our finalized revision to § 171.204(a), the *uncontrollable events* condition of the Infeasibility Exception, is discussed in Section IV.C.1.a. Second, we have added two new conditions to be codified as subparagraphs (a)(3) and (a)(4) and have, therefore, redesignated the *infeasible under the circumstances* condition as subparagraph (a)(5). The *infeasible under the circumstances* condition was previously designated as subparagraph (a)(3) of § 171.204.

The first new infeasibility condition in § 171.204(a)(3) (discussed in Section IV.C.1.b) will apply to an actor's practice of denying a third party's request to enable use of EHI in order to modify EHI, including, but not limited to, creation and deletion functionality, provided the request is not from a health care provider requesting such use from an actor that is their business associate.[19] In support of this new condition, we have finalized as proposed a definition of ''business associate'' in § 171.102. That definition is, by cross-reference to 45 CFR 160.103, the HIPAA Privacy Rule's definition of ''business associate.''

The second new infeasibility condition in § 171.204(a)(4), discussed in Section IV.C.1.c, will apply where an actor has exhausted the Manner Exception in § 171.301, including offering at least two alternative manners in accordance with § 171.301(b), including one manner that uses either technology certified to standard(s) adopted in 45 CFR part 170 that is specified by the requestor (§ 171.301(b)(1)(i)) or published content and transport standards consistent with § 171.301(b)(1)(ii). The actor cannot meet this new condition if the actor currently provides a substantial number of individuals or entities similarly situated to the requestor with the same requested access, exchange, or use of the requested EHI.

As discussed in section IV.C.3, we have finalized a new subpart D under part 171 for information blocking exceptions that involve practices related to actors' participation in the Trusted Exchange Framework and Common Agreement (TEFCA℠). In this new subpart D, we have established a standalone TEFCA Manner Exception, in § 171.403, that is based on a proposed *TEFCA manner* condition of the Manner Exception that was included in the HTI–1 Proposed Rule. The new exception provides that an actor's practice of not fulfilling a request to access, exchange, or use EHI in any alternative manner besides via TEFCA will not be considered information blocking when the practice follows certain conditions, which are discussed in more detail in section IV.C.3. Both the actor and requestor must be part of TEFCA, and the requestor must be able to access, exchange, or use the requested EHI via TEFCA. In consideration of comments and our stated policy goals, any fees or license agreements *must* satisfy the Fees (§ 171.302) and Licensing (§ 171.303) exceptions, which is counter to our initial proposed position. Further, in consideration of our stated policy goals and comments we received, the exception is *not* available when the requestor has requested access, exchange, or use via FHIR-based APIs.

In section IV.D, we discuss information blocking requests for information that we included in section IV.C of the HTI–1 Proposed Rule (88 FR 23873).

C. Costs and Benefits

Executive Orders 12866[20] and 13563[21] direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Executive Order 14094[22] entitled ''Modernizing Regulatory Review'' (hereinafter, the Modernizing E.O.) amends section 3(f) of Executive Order 12866 (Regulatory Planning and Review). The amended section 3(f) of Executive Order 12866 defines a ''significant regulatory action'' as an action that is likely to result in a rule that may: (1) have an annual effect on the economy of $200 million or more (adjusted every 3 years by the Administrator of the Office of Information and Regulatory Affairs (OIRA) for changes in gross domestic product); or adversely affect in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, local, territorial, or Tribal governments or communities; (2) create a serious inconsistency or otherwise interfere with an action taken or planned by another agency; (3) materially alter the budgetary impacts of entitlement grants, user fees, or loan programs or the rights and obligations of recipients thereof; or (4) raise legal or policy issues for which centralized review would meaningfully further the President's priorities or the principles set forth in this Executive Order, as specifically authorized in a timely manner by the Administrator of OIRA in each case. OMB has determined that this final rule is a significant regulatory action, as the potential economic

[19] See definition of ''business associate'' at 45 CFR 160.103. Business associates include a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

[20] *https://www.archives.gov/files/federal-register/executive-orders/pdf/12866.pdf.*

[21] *https://obamawhitehouse.archives.gov/the-press-office/2011/01/18/executive-order-13563-improving-regulation-and-regulatory-review.*

[22] *https://www.whitehouse.gov/briefing-room/presidential-actions/2023/04/06/executive-order-on-modernizing-regulatory-review/.*

impacts associated with this final rule could be greater than $200 million per year. Accordingly, we have prepared a Regulatory Impact Analysis (RIA) that, to the best of our ability, presents the costs and benefits of this final rule. We have estimated the potential monetary costs and benefits of this final rule for the health IT community, including costs and benefits as they relate to health IT developers, health care providers, patients, and the Federal Government (*i.e.,* ONC), and have broken those costs and benefits out by section. In accordance with E.O. 12866, we have included the RIA summary table as Table 37.

We note that we have rounded all estimates to the nearest dollar and that all estimates are expressed in 2022 dollars as it is the most recent data available to address all cost and benefit estimates consistently. The wages used to derive the cost estimates are from the May 2022 National Occupational Employment and Wage Estimates reported by the U.S. Bureau of Labor Statistics.[23] We also note that estimates presented in the following ''Employee Assumptions and Hourly Wage,'' ''Quantifying the Estimated Number of Health IT Developers and Products,'' and ''Number of End Users that Might Be Impacted by ONC's Proposed Regulations'' sections are used throughout the RIA.

We estimate that the total annual cost for this final rule for the first year after it is finalized (including one-time costs), based on the cost estimates outlined throughout the RIA, would result in $437 million. The total undiscounted perpetual cost over a 10-year period for this final rule (starting in year three), would result in $477 million. We estimate the total costs to health IT developers to be $914 million and estimate the government (ONC) costs to be between $56,800 to $113,600.

We estimate the total annual benefit for this final rule would be on average $1.0 billion. We estimate the total undiscounted perpetual annual net benefit for this final rule (starting in year three), would be $124 million.

II. Background

A. Statutory Basis

The Health Information Technology for Economic and Clinical Health Act (HITECH Act), Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111–5), was enacted on February 17, 2009. The HITECH Act amended the Public Health Service Act (PHSA) and created ''Title XXX—Health Information Technology and Quality'' (Title XXX) to improve healthcare quality, safety, and efficiency through the promotion of health IT and electronic health information (EHI) exchange.

The 21st Century Cures Act, Public Law 114–255 (Cures Act), was enacted on December 13, 2016, to accelerate the discovery, development, and delivery of 21st century cures, and for other purposes. The Cures Act, through Title IV—Delivery, amended the HITECH Act by modifying or adding certain provisions to the PHSA relating to health IT.

Section 119 of Title I, Division CC of the Consolidated Appropriations Act, 2021, Public Law 116–260 (CAA), enacted on December 27, 2020, requires prescription drug plan (PDP) sponsors to implement one or more real-time benefit tools (RTBTs) that meet the requirements described in the statute, after the Secretary has adopted a standard for RTBTs and at a time determined appropriate by the Secretary. For purposes of the requirement to implement a real-time benefit tool in section 1860D–4(o)(1) of the Social Security Act, described above, the CAA provides that one of the requirements for an RTBT is that it can integrate with electronic prescribing and EHR systems of prescribing healthcare professionals for the transmission of formulary and benefit information in real time to such professionals. The statute requires incorporation of RTBTs within both the Medicare Part D prescription drug program and the Program. Specifically, the law amends the definition of a ''qualified electronic health record'' (qualified EHR) in section 3000(13) of the PHSA to require that a qualified EHR must include (or be capable of including) an RTBT.

1. Standards, Implementation Specifications, and Certification Criteria

The HITECH Act established two Federal advisory committees, the Health IT Policy Committee (HITPC) and the Health IT Standards Committee (HITSC). Each was responsible for advising the National Coordinator for Health Information Technology (National Coordinator) on different aspects of standards, implementation specifications, and certification criteria.

Section 4003(e) of the Cures Act amended sections 3002 and 3003 of the PHSA by replacing, in an amended section 3002, the HITPC and HITSC with one committee named the Health Information Technology Advisory Committee (Health IT Advisory Committee or HITAC). Section 3002(a) of the PHSA, as added by the Cures Act, establishes that the HITAC recommends to the National Coordinator policies and standards, implementation specifications, and certification criteria, relating to the implementation of a health information technology infrastructure, nationally and locally, that advances the electronic access, exchange, and use of health information. Further described in section 3002(b)(1) of the PHSA, this includes recommending to the National Coordinator a policy framework to advance interoperable health information technology infrastructure, updating recommendations to the policy framework, and making new recommendations, as appropriate. Section 3002(b)(2)(A) of the PHSA specifies that in general, the HITAC shall recommend to the National Coordinator for purposes of adoption under section 3004, standards, implementation specifications, and certification criteria and an order of priority for the development, harmonization, and recognition of such standards, specifications, and certification criteria. Like the process previously required of the former HITPC and HITSC, section 3002(b)(5) of the PHSA requires the HITAC to develop a schedule, updated annually, for the assessment of policy recommendations, which the Secretary publishes in the **Federal Register**.

Section 3004 of the PHSA establishes a process for the adoption of health IT standards, implementation specifications, and certification criteria and authorizes the Secretary to adopt such standards, implementation specifications, and certification criteria. As specified in section 3004(a)(1), the Secretary is required, in consultation with representatives of other relevant federal agencies, to jointly review standards, implementation specifications, and certification criteria endorsed by the National Coordinator under section 3001(c) and subsequently determine whether to propose the adoption of such standards, implementation specifications, or certification criteria. Section 3004(a)(3) requires the Secretary to publish all such determinations in the **Federal Register**.

Section 3004(b)(3) of the PHSA, titled Subsequent Standards Activity, provides that the Secretary shall adopt additional standards, implementation specifications, and certification criteria as necessary and consistent with the schedule published by the HITAC. We consider this provision in the broader

[23] May 2021 National Occupational Employment and Wage Estimates, United States. U.S. Bureau of Labor Statistics. *https://www.bls.gov/oes/current/oes_nat.htm.*

context of the HITECH Act and Cures Act to grant the Secretary the authority and discretion to adopt standards, implementation specifications, and certification criteria that have been recommended by the HITAC and endorsed by the National Coordinator, as well as other appropriate and necessary health IT standards, implementation specifications, and certification criteria.

2. Health IT Certification Program(s)

Section 3001(c)(5) of the PHSA provides the National Coordinator with the authority to establish a certification program or programs for the voluntary certification of health IT. Section 3001(c)(5)(A) specifies that the National Coordinator, in consultation with the Director of the National Institute of Standards and Technology (NIST), shall keep or recognize a program or programs for the voluntary certification of health IT that is in compliance with applicable certification criteria adopted under section 3004 of the PHSA. The certification program(s) must also include, as appropriate, testing of the technology in accordance with section 13201(b) of the HITECH Act. Section 13201(b) of the HITECH Act requires that, with respect to the development of standards and implementation specifications, the Director of NIST shall support the establishment of a conformance testing infrastructure, including the development of technical test beds. Section 13201(b) also indicates that the development of this conformance testing infrastructure may include a program to accredit independent, non-federal laboratories to perform testing.

Section 4003(b) of the Cures Act added section 3001(c)(9)(B)(i) to the PHSA, which requires the National Coordinator ''to convene appropriate public and private stakeholders'' with the goal of developing or supporting a Trusted Exchange Framework and a Common Agreement (collectively, TEFCA℠) for the purpose of ensuring full network-to-network exchange of health information. Section 3001(c)(9)(B) outlines provisions related to the establishment of a Trusted Exchange Framework for trust policies and practices and a Common Agreement for exchange between health information networks (HINs)—including provisions for the National Coordinator, in collaboration with the NIST, to provide technical assistance on implementation and pilot testing of TEFCA. Section 3001(c)(9)(C) requires the National Coordinator to publish TEFCA on its website and in the **Federal Register**.

Section 4002(a) of the Cures Act amended section 3001(c)(5) of the PHSA by adding section 3001(c)(5)(D), which requires the Secretary, through notice and comment rulemaking, to require conditions of certification and maintenance of certification for the Program. Specifically, the health IT developers or entities with technology certified under the Program must, in order to maintain such certification status, adhere to certain conditions and maintenance of certification requirements concerning information blocking; assurances regarding appropriate exchange, access, and use of electronic health information; communications regarding health IT; APIs; real world testing; attestations regarding certain conditions and maintenance of certification requirements; and submission of reporting criteria under the EHR Reporting Program in accordance with section 3009A(b) of the PHSA.

B. Regulatory History

The Secretary issued an interim final rule with request for comments on January 13, 2010, ''Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology'' (75 FR 2014), which adopted an initial set of standards, implementation specifications, and certification criteria. On March 10, 2010, the Secretary issued a proposed rule, ''Proposed Establishment of Certification Programs for Health Information Technology'' (75 FR 11328), that proposed both temporary and permanent certification programs for the purposes of testing and certifying health IT. A final rule establishing the temporary certification program was published on June 24, 2010, ''Establishment of the Temporary Certification Program for Health Information Technology'' (75 FR 36158), and a final rule establishing the permanent certification program was published on January 7, 2011, ''Establishment of the Permanent Certification Program for Health Information Technology'' (76 FR 1262).

We have engaged in multiple rulemakings to update standards, implementation specifications, certification criteria, and the certification program, a history of which can be found in the October 16, 2015 final rule ''2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications'' (80 FR 62602) (2015 Edition Final Rule). The history can be found at 80 FR 62606. A correction notice was published for the 2015 Edition Final Rule on December 11, 2015 (80 FR 76868), to correct preamble and regulatory text errors and clarify requirements of the Common Clinical Data Set (CCDS), the 2015 Edition privacy and security certification framework, and the mandatory disclosures for health IT developers.

The 2015 Edition Final Rule established a new edition of certification criteria (''2015 Edition health IT certification criteria'' or ''2015 Edition'') and a new 2015 Edition Base EHR definition. The 2015 Edition established the minimum capabilities and specified the related minimum standards and implementation specifications that certified electronic health record technology (CEHRT) would need to include to support the achievement of ''meaningful use'' by eligible clinicians, eligible hospitals, and critical access hospitals under the Medicare and Medicaid EHR Incentive Programs (EHR Incentive Programs) (now the Medicare Promoting Interoperability Program and the Promoting Interoperability performance category of MIPS) when the 2015 Edition is required for use under these and other programs referencing the CEHRT definition. The 2015 Edition Final Rule also adopted a proposal to change the Program's name to the ''ONC Health IT Certification Program'' from the ONC HIT Certification Program, modified the Program to make it more accessible to other types of health IT beyond EHR technology and for health IT that supports care and practice settings beyond the ambulatory and inpatient settings, and adopted new and revised Principles of Proper Conduct (PoPC) for ONC-Authorized Certification Bodies (ONC–ACBs).

After issuing a proposed rule on March 2, 2016, ''ONC Health IT Certification Program: Enhanced Oversight and Accountability'' (81 FR 11056), we published a final rule by the same title (81 FR 72404) (EOA Final Rule) on October 19, 2016. The EOA Final Rule finalized modifications and new requirements under the Program, including provisions related to our role in the Program. The EOA Final Rule created a regulatory framework for our direct review of health IT certified under the Program, including, when necessary, requiring the correction of non-conformities found in health IT certified under the Program and suspending and terminating certifications issued to Complete EHRs and Health IT Modules. The EOA Final Rule also set forth processes for us to

authorize and oversee accredited testing laboratories under the Program. In addition, it included provisions for expanded public availability of certified health IT surveillance results.

On March 4, 2019, the Secretary published a proposed rule titled, ''21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program'' (84 FR 7424) (ONC Cures Act Proposed Rule). The ONC Cures Act Proposed Rule proposed to implement certain provisions of the Cures Act that would advance interoperability and support the access, exchange, and use of electronic health information. We also requested comment in the ONC Cures Act Proposed Rule (84 FR 7467) as to whether certain health IT developers should be required to participate in TEFCA as a means of providing assurances to their customers and ONC that they are not taking actions that constitute information blocking or any other action that may inhibit the appropriate exchange, access, and use of EHI, with the goal of developing or supporting TEFCA for the purpose of ensuring full network-to-network exchange of health information.

On May 1, 2020, a final rule was published titled, ''21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program'' (85 FR 25642) (ONC Cures Act Final Rule). The ONC Cures Act Final Rule implemented certain provisions of the Cures Act, including Conditions and Maintenance of Certification requirements for health information technology (health IT) developers, the voluntary certification of health IT for use by pediatric health providers, and reasonable and necessary activities that do not constitute information blocking. The ONC Cures Act Final Rule also implemented certain parts of the Cures Act to support patients' access to their EHI, and the implementation of information blocking policies that support patient electronic access. Additionally, the ONC Cures Act Final Rule modified the 2015 Edition health IT certification criteria and Program in other ways to advance interoperability, enhance health IT certification, and reduce burden and costs, as well as improving patient and health care provider access to EHI and promoting competition. On November 4, 2020, the Secretary published an interim final rule with comment period titled, ''Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID–19 Public Health Emergency'' (85 FR 70064) (Cures Act Interim Final Rule). The Cures Act Interim Final Rule extended certain compliance dates and timeframes adopted in the ONC Cures Act Final Rule to offer the healthcare system additional flexibilities in furnishing services to combat the COVID–19 pandemic, including extending the applicability date for information blocking provisions to April 5, 2021.

On January 19, 2022, we published a notice titled, ''Notice of Publication of the Trusted Exchange Framework and Common Agreement'' (87 FR 2800) (''TEFCA''). The notice fulfilled an obligation under section 3001(c)(9)(C) of the PHSA, which requires the National Coordinator for Health Information Technology to publish on the Office of the National Coordinator for Health Information Technology's public internet website, and in the **Federal Register**, the trusted exchange framework and common agreement developed under the PHSA.

On April 18, 2023, the Secretary published a proposed rule titled, ''Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing'' (HTI–1) (88 FR 23746) (HTI–1 Proposed Rule). The HTI–1 Proposed Rule proposed to implement the Electronic Health Record (EHR) Reporting Program provision of the 21st Century Cures Act by establishing new Conditions and Maintenance of Certification requirements for health IT developers under the Program. The HTI–1 Proposed Rule also proposed several updates to certification criteria and implementation specifications recognized by the Program, including a revised certification criterion for decision support and revised certification criteria for ''patient demographics and observations'' and ''electronic case reporting.'' Additionally, the HTI–1 Proposed Rule proposed to establish a new baseline version of the United States Core Data for Interoperability (USCDI). The HTI–1 Proposed Rule also proposed enhancements to support information sharing under the information blocking regulations. The implementation of these provisions would advance interoperability, improve transparency, and support the access, exchange, and use of electronic health information. The HTI–1 Proposed Rule also proposed to update the Program in additional ways to advance interoperability, enhance health IT certification, and reduce burden and costs and is subject of this final rule.

C. General Comments on the HTI–1 Proposed Rule

Comments. Numerous commenters expressed support for the overall direction of the HTI–1 Proposed Rule and its policy goals, including improved interoperability, standardization, reporting requirements, and electronic health information exchange. Many commenters also stated that the updated standards and certification criteria in the HTI–1 Proposed Rule would enhance patient and clinical access and enable health care providers to better meet patients' needs. A few commenters commended us for the protections for patients' privacy provided by the standards in the HTI–1 Proposed Rule. A few commenters also expressed appreciation for ONC providing clarity on certification criteria for certified health IT. A number of commenters stated that they looked forward to working with ONC and cooperating with the public and private sectors on improving interoperability for EHI.

Response. We appreciate the support expressed by many commenters. This final rule maintains the direction of the HTI–1 Proposed Rule, and we also look forward to ongoing collaboration with public and private sector partners as we implement the provisions of this final rule.

Comments. Many commenters expressed concern that the timeline for compliance deadlines for the standards in the HTI–1 Proposed Rule was too aggressive and that it was unrealistic for the health IT community to meet the requirements. Several commenters recommended delaying the compliance deadlines until at least two years after the date of publication of the final rule or providing a temporary enforcement safe harbor for developers and providers who are in the process of implementing the required changes. One commenter suggested that the timeline for adoption might be too aggressive and lead to health IT developers producing Health IT Modules that meet certification standards without providing the intended substantive benefits for patients and providers. A few commenters suggested that ONC create a standardized framework and cycle for adopting and requiring new and revised standards for certification criteria. Commenters suggested that ONC give more consideration to the burden placed on the health IT community by the requirements of both ONC and CMS standards, and work with CMS and other HHS agencies to more closely align standards and compliance dates.

Response. We appreciate commenters' concerns about the timelines for

conformance to new standards and certification criteria for the Program. After consideration of comments, we have finalized the adoption of certain certification criteria and standards with a compliance date of January 1, 2026, instead of the proposed compliance date of January 1, 2025, and noted in the specific certification criteria or standards each specific adopted conformance date. We have finalized the adoption of § 170.315(a)(5); (b)(1), (2), and (9); (e)(1); (f)(5); and (g)(6), (9), and (10) with a compliance date of January 1, 2026. We believe that these updated compliance dates, which are approximately two years from when this final rule published in the **Federal Register**, for certain criteria will allow developers increased flexibility and alleviate burden by allowing additional time for developers to prioritize updates, while also ensuring timely implementation of the requirements for health care providers and patients. We note that the compliance date defines the date by which a health IT developer with a Health IT Module certified to any revised certification criterion, as defined in § 170.102, must update the Health IT Module and provide such update to their customers in order for the Health IT Module to maintain certification.

In response to commenters' recommendations for a standardized framework and cycle for updates to certification criteria, we appreciate commenters' concerns about the long-term timeline for updates to ONC Certification Criteria for Health IT. We have finalized our proposed approach to discontinue the use of year themed editions for ONC Certification Criteria for Health IT and adopt an incremental approach to updates to ONC Certification Criteria for Health IT. We believe that an incremental approach to updates will allow for a more consistent and transparent update cycle. We plan to issue clear guidance and timelines for when updates would be required.

Comments. A number of commenters stated that the HTI–1 Proposed Rule and ONC's rulemaking schedule is overly complex, including a broad range of proposed changes to regulations. Some commenters recommended simplifying the proposals in this rule or creating a process to introduce more simplified regulatory updates in the future.

Response. We appreciate the concerns expressed about the complexity and broad scope of the changes to standards and the Program in this rule. Upon consideration of all the comments we have received, we have made adjustments, such as an extended implementation timeline for most standards and certification criteria and modified requirements for Health IT Modules certified to § 170.315(b)(11), in this final rule to alleviate the potential burden on developers of certified health IT and health care providers.

Comments. Some commenters stated that the adoption of a singular set of standards for EHI could have harmful effects for Health IT Modules. A few commenters were concerned that the standards in the HTI–1 Proposed Rule would not allow for specific standards for specialized or small health care providers. A few commenters were concerned that the requirements in the HTI–1 Proposed Rule could make health care providers dependent on collaboration with health IT developers to meet their obligations and could increase EHR fees for physicians or create bottlenecks that prevent physicians from adopting new EHR technology. Some commenters recommended that ONC provide assistance and guidance for providers to understand new requirements, and consider patient accessibility, particularly the limitations of patient literacy regarding healthcare and health IT, for requirements for patients' records. A number of commenters were concerned that the HTI–1 Proposed Rule's requirements for interoperability and patient access would not adequately protect patients' private information. Several commenters also recommended that ONC require greater transparency from health IT developers to foster an accessible health IT marketplace for consumers.

Response. We believe the updated standards and certification criteria will improve health IT interoperability and functionality for providers and patients. We thank commenters for their comments regarding privacy concerns and recognize the importance of addressing the privacy and confidentiality of sensitive information. Recognizing this, the Program establishes the standards, implementation specifications, and functional requirements for certified health IT to manage and exchange data but does not control the collection or use of data. For more on patient requested restrictions on sharing of their health information, we refer readers to section III.C.10 on modifications to the ''view, download, and transmit to 3rd party'' certification criterion in § 170.315(e)(1), which addresses patients' (and their authorized representatives') ability to use an internet-based method to request a restriction to be applied for any data expressed in the standards in § 170.213. We also appreciate commenters recommending that we require greater transparency from health IT developers to foster an accessible health IT marketplace for consumers. As stated in the HTI–1 Proposed Rule (88 FR 23831) and this final rule, data collected and reported under the Insights Condition will address information gaps in the health IT marketplace and provide insights on the use of certified health IT. We believe that consumers will benefit from the increased transparency that the reporting requirements of Insights Condition will provide.

While we believe that the language that we use in this rule provides clarity on the effects of this rule, as we did with the HTI–1 Proposed Rule, we will develop, as appropriate, resources such as infographics, FAQs, and fact sheets and provide webinars among other forms of educational materials and outreach to explain the effects of this rule for developers, providers, and patients.

Comments. One commenter requested that ONC adopt a definition of ''health IT developer'' to provide more clarity regarding what entities may be considered developers for certification criteria.

Response. We thank commenters for their feedback. We decline to adopt a new definition for ''health IT developer'' in this rule. Adopting a new definition for ''health IT developer'' would be out of scope for this rule because we did not propose a definition of ''health IT developer'' in the HTI–1 Proposed Rule.

Comments. One commenter recommended ONC include non-patient facing facilities (*e.g.,* radiology) in the certified health IT requirements. This commenter stated that by establishing specialty-specific or size-specific health IT requirements, the goal of promoting interoperability across the healthcare landscape may be better achieved.

Response. We thank the commenter for their feedback. Including non-patient facing facilities in the certified health IT requirements was out of the HTI–1 Proposed Rule's scope. As we did not propose such changes to health IT requirements in the HTI–1 Proposed Rule, these changes would also be out of scope for this rule.

Comments. A few commenters raised issues that are out of scope for this rule, including concerns specifically about CMS policies and requirements.

Response. We reiterate that comments regarding CMS program requirements are out of scope as we cannot change CMS policy. We refer to readers to CMS programs for further information.

Comments. Some commenters requested that ONC provide technical

assistance for the implementation of the requirements of this rule.

Response. We thank commenters for their feedback. As we did with the HTI–1 Proposed Rule, we will develop, as appropriate, resources such as infographics, FAQs, and fact sheets and provide webinars among other forms of educational materials and outreach to explain the effects of this rule for interest parties.

Comments. Several commenters identified issues that were out of scope for our proposal, such as requesting potential changes to the Cures Act and other federal legislation, and developing state local public health infrastructure and regulations with state and local health agencies.

Response. We appreciate commenters' interest in federal legislation, and state and local public health infrastructure and regulations. Because we did not propose changes related to these areas in the HTI–1 Proposed Rule, these comments are out of scope, and we decline to finalize the recommended changes in this rule. ONC does not have the authority to change federal legislation through rulemaking. ONC looks forward to communicating with state and local public health agencies for the implementation of this rule and the development of future rulemaking.

Comments. We also received numerous comments that were out of scope or that recommended that ONC adopt new requirements that we did not propose and are not addressed in this rulemaking.

Response. We thank commenters for their input. These comments are out of scope for the HTI–1 Proposed Rule in that we did not propose changes to the requirements the comments addressed, and we decline to finalize such changes.

III. ONC Health IT Certification Program Updates

A. ''The ONC Certification Criteria for Health IT'' and Discontinuing Year Themed ''Editions,'' Definition of Revised Certification Criterion, and Related Program Oversight

1. Discontinuing Year Themed ''Editions''

In the HTI–1 Proposed Rule, we stated that we no longer believed it was helpful or necessary to maintain an ''edition'' naming convention or to adopt entirely new editions of certification criteria to encapsulate updates over time (88 FR 23750). Instead, we proposed that there should be a single set of certification criteria, which would be updated in an incremental fashion in closer alignment to standards development cycles and regular health IT development timelines. We proposed in the HTI–1 Proposed Rule to rename all certification criteria within the Program simply as ''ONC Certification Criteria for Health IT'' (88 FR 23759). We explained that maintaining a single set of ''ONC Certification Criteria for Health IT'' would create more stability for users of health IT and Program partners, such as CMS, as well as make it easier for developers of certified health IT to maintain their product certificates over time. Unchanged certification criteria would no longer be duplicated as separate criteria under multiple editions. Accordingly, we proposed to rename § 170.315 as the ''ONC Certification Criteria for Health IT'' and replace all references throughout 45 CFR part 170 to the ''2015 Edition'' with this new description (this would impact the wording, though not the substance or effect, of §§ 170.102, 170.405, 170.406, 170.523, 170.524, and 170.550, as shown in the revised regulation text).

Comments. Many commenters were supportive of ONC's proposed approach to discontinue the use of year-themed editions for ONC Certification Criteria for Health IT, stating that it would reduce confusion. Commenters generally indicated that the change from year themed editions to adopting the name ''ONC Certification Criteria for Health IT'' would be understood by health IT developers, patients, and health care providers. Commenters stated and agreed that the previous naming convention inaccurately implied the age and outdatedness of the certification criteria and contributed to confusion about which edition was required for Program adherence. A number of commenters agreed that the change to incremental updates of certification criteria would be more efficient and allow for more flexibility than the edition-based updates to certification criteria that ONC has previously adopted. One commenter stated that such an approach would be more appropriate given the rapid pace at which health IT evolves. Another commenter favored the use of clear, regular, step-by-step updates in small portions, rather than complete overhauls of certification criteria. The commenter also favored a predictable timeline for updates based on standards development cycles with reasonable development timelines.

Alternatively, some commenters expressed concern that discontinuing year-themed editions and adopting incremental advancement for certification criteria would create too much burden for developers of certified health IT and health care providers around updating Health IT Modules. Commenters stated that adopting incremental updates to many criteria instead of edition-based updates to criteria could lead to too many and too frequent deadlines for developers and providers to comply with and a significant added burden in cost and time. Commenters raised concerns that incremental standards updates may divert developer resources away from implementing provider requests. A few developers recommended that ONC adopt a regular cycle for updates and compliance to certification criteria and provide adequate time between revisions to criteria that accommodate typical development timelines for Health IT Modules. Numerous commenters contended that the proposed approach to discontinue the use of year-themed editions for ONC health IT certification criteria in favor of using the title ''ONC Certification Criteria for Health IT'' would not add sufficient clarity to the Program or would actually make the Program more difficult to understand. Commenters stated that the incremental updates for certification criteria could make it difficult for developers and consumers to understand which iterations of revised and updated standards are the most recently adopted criteria that Health IT Modules need to be certified to. A few commenters stressed that ONC should provide specificity and education regarding the standards that are necessary to participate in federal interoperability programs. Some commenters recommended that ONC create a listing of information on certification criteria that health IT developers and consumers could reference to determine the most up-to-date standards for a certification criterion and Health IT Module certified to such criterion. A few commenters requested greater clarity on how much responsibility consumers as opposed to developers would bear for maintaining the certification for Health IT Modules with the adoption of incremental advancements. One commenter was concerned that developers might charge providers the costs for updates and recommended that ONC add a requirement for developers to inform health care providers of the meaning of a ''provider product'' and the consequences of declining updates to health IT for participation in other federal programs.

Response. We thank all commenters for their thoughtful feedback. Upon consideration of all comments received on this proposal, we have finalized our approach as proposed. As noted in the

HTI–1 Proposed Rule (FR 23759), we believe that there should be a single set of certification criteria, which would be updated in an incremental fashion in closer alignment to standards development cycles and regular health IT development timelines. To finalize this proposal, we renamed all certification criteria within the Program simply as ''ONC Certification Criteria for Health IT.'' We believe maintaining a single set of ''ONC Certification Criteria for Health IT'' will create more stability for users of health IT and Program partners, such as CMS, as well as make it easier for developers of certified health IT to maintain their product certificates over time. In addition, we believe that this approach will have the benefit of reducing administrative burden for health IT developers participating in the Program. Previously, duplicative references to separate certification criteria under multiple, year-themed editions created administrative burden for health IT developers by requiring developers to seek an updated certificate attributed to the ''new'' duplicated certification criterion even in circumstances when the certification criterion remained substantively unchanged. Under this approach, unchanged certification criteria would no longer be duplicated as separate criteria under multiple editions. Accordingly, we renamed § 170.315 as the ''ONC Certification Criteria for Health IT'' and replaced all references throughout 45 CFR part 170 to the ''2015 Edition'' with this new description (this impacted the wording, though not the substance or effect, of §§ 170.102, 170.405, 170.406, 170.523, 170.524, and 170.550, as shown in the revised regulation text).

With respect to those commenters that expressed reservations, discontinuing the use of year-themed editions for ONC Certification Criteria for Health IT will not impose a significant burden on implementers. Our intent with this approach is to maintain a single set of certification criteria that have been updated to include the most recent versions of adopted standards, and to establish an incremental approach to health IT updates over time. In fact, this has been embedded within the Program's approach all along because of the way we revised only certain certification criteria within an edition change. Moreover, in the ONC Cures Act Final Rule, we stated our belief that this kind of approach should also include development timelines based on the updates required for each criterion and a transition period allowing for either the prior adopted standard or the new standard to be used for a reasonable period of time (before shifting to exclusive use of the new standard). We further noted our belief that this approach can help to reduce the burden on health IT developers and health care providers and could allow health IT developers to implement updates in the manner most appropriate for their product and customers (85 FR 25665). We have received significant positive feedback expressing that the incremental approach to updates is generally beneficial as a long-term approach. Specifically, feedback conveyed that a consistent, transparent, incremental update cycle that includes the following features would be preferred by some: (1) regular updates to recognize standards advancement and an allowance for voluntary standards advancement between updates, (2) incremental updates rather than ''wholesale'' product overhauls, (3) a predictable timeline for updates based on standards development cycles with reasonable development timelines, and (4) a reasonable development timeline for any new criterion based on specific development needs. We plan to issue clear guidance and timelines for when updates would be required. In consideration of the overall support from commenters, we have finalized our proposed approach to discontinue the use of year themed editions for ONC Certification Criteria for Health IT.

In response to commenters that indicated we did not provide adequate specificity or education in our HTI–1 Proposed Rule, we appreciate the commenters' concerns and agree with the need for educational materials and resources. We intend to make updates to ONC website materials, engage in public presentations and webinars, and revise the Certified Health IT Product List (CHPL) database to make clear which certification criteria, standards, and implementation specifications are valid under the Program at a given point in time. Between the ONC website and the CHPL updates, we are confident that interested parties will have the necessary information regarding both certification criteria and certified health IT products. We will also develop educational resources so that purchasers and users understand which Health IT Modules have met their obligations under the Program by updating their Health IT Modules to revised certification criteria.

In response to the commenter suggestion that ONC add a requirement for developers to inform health care providers of the meaning of a ''provider product'' and the consequences for declining updates to health IT regarding participation in federal reporting programs, we thank the commenter for their comment. However, we have not proposed any requirements related to the term, ''provider product,'' and decline to finalize any such requirements in this final rule. Although we are not at this time requiring developers to inform health care providers of the consequences of declining updates to health IT, we encourage developers to be transparent with customers about the benefits of updates and impacts of declining them. We understand there are costs associated with updating new technology and also with foregoing participation in a federal program that requires the use of certified health IT. Therefore, we encourage developers to ensure that their customers are fully informed about all impacts before making a decision on updates.

Comments. Several commenters requested further clarity on issues related to the impact of the proposed approach on public health entities. Commenters noted that an approach should include an ''expiration date'' or identify minimum standards to ensure public health and other entities receiving data from certified health IT do not maintain support for outdated standards. Commenters also stated that the proposed approach should recognize the cost and implementation burden for public health agencies associated with updating standards, and that all regulatory impact analyses, including for the current rule, should include estimated costs for public health agencies, laboratories, and their intermediaries. Further, commenters recommended more attention on public input procedures, including from public health, and asked ONC to ensure that regulations do not update standards without verifying that public health authorities can meet the updated standards. Finally, one commenter suggested that ONC reference the authority of state, local, and territorial public health agencies within the standards update process to ensure clarity for users.

Response. We thank commenters for their input. We have identified in several places within 45 CFR part 170 subpart B, and within several certification criteria in 45 CFR part 170 subpart C, ''expiration dates'' and dates after which a standard or certification criterion is no longer valid within the context of the Program. We believe these dates will ensure public health and other entities receiving data from certified health IT do not maintain support for outdated standards. We understand concerns about the broader

overall downstream impact of this rulemaking on entities beyond developers of certified health IT, which are specifically regulated under authorities delegated to ONC. This rule's impact analysis measures the estimated costs for developers of certified health IT to meet new Program requirements, for example, to develop or modify the technical functionality of their certified health IT or adopt a new standard or standard version. These are the expected direct costs of the rule's final policies on developers of certified health IT. However, we recognize that developers of certified health IT are largely private businesses that operate in a competitive marketplace and that they may not bear all costs to meet these requirements. We include in the ''Costs and Benefits'' section of the Regulatory Impact Analysis the estimated impact on certified health IT end users. In this case, health care providers, such as hospitals and clinicians. We believe these estimates provide a general, but not necessarily comprehensive, understanding of the possible pass-through costs borne by users of certified health IT.

We also plan to issue educational resources explaining, consistent with standards and timelines adopted in this rule, when updates would be required. In addition, we actively engage with public health agencies to ensure that the regulatory process for updating standards represents their input. Finally, we indicate the authority of state, local, and territorial laws and requirements where appropriate.

Comments. One commenter stated that they did not support the change to an ''edition-less'' format because the availability of the Standards Version Advancement Process (SVAP) allows health IT developers to upgrade to approved standards on a voluntary basis. The commenter urged ONC to consider the following steps to mitigate burden on health IT developers: provide a minimum implementation time of 24 months for any new or updated criteria, utilize the SVAP process over required updates where feasible, accept ''evidence-based'' attestations for the purposes of certification, and work with other HHS agencies on awareness around updates to certification criteria.

Response. As noted above, we plan to issue educational resources explaining, consistent with standards and timelines adopted in this rule, when updates would be required. In the ONC Cures Act Final Rule, as part of the Real World Testing Condition of Certification, we finalized a ''flexibility'' within the associated Maintenance of Certification that we refer to as the SVAP (85 FR 25775). This flexibility permits health IT developers to voluntarily use newer versions of adopted standards in their certified Health IT Modules so long as certain conditions are met. These conditions are not limited to, but notably include, successful real world testing of the Health IT Module using the new version(s) subsequent to the inclusion of these newer standards and implementation specification versions in the Health IT Module's certification. We established the SVAP not only to meet the Cures Act's goals for interoperability, but also in response to the feedback ONC has received through prior rulemakings and engagements, which advocated for ONC to establish a predictable and timely approach within the Program to keep pace with the industry's standards development efforts (85 FR 25775). We continue to support the SVAP, but we also believe it is necessary to discontinue the use of year-themed editions for ONC Certification Criteria for Health IT and adopt incremental updates to the Program. While SVAP allows flexibility for the voluntary adoption of newer versions of standards, the incremental Program updates will ensure aligned minimum requirements within the health IT industry that advance interoperability.

Comments. One commenter stated that moving to an ''edition-less'' approach would require ONC–ACBs to provide increased oversight to ensure certified health IT meets the specific compliance dates provided in regulation. Another commenter stated that ONC should provide a minimum of six months for developers and ONC–ACBs to implement this change, such as removing references to the 2015 Edition from documentation related to the Program.

Response. We thank commenters for their feedback; however, we disagree that moving to an ''edition-less'' approach will require ONC–ACBs to conduct more oversight than under the edition-based construct. We note that while an ''edition-less'' approach may require different levels of documentation of oversight than currently exist in the Program, this approach will also likely reduce documentation and oversight in other areas given that health IT developers will not update Health IT Modules to all certification criteria at once, which was the case under the edition-based approach.

Comments. All comments received were supportive of revising the text from ''time-limited certification and certification status for certain 2015 Edition certification criteria'' in § 170.550(m) to ''time-limited certification and certification status for certain ONC Certification Criteria for Health IT.'' Commenters noted that our proposal for time-limited certification should require products be clearly labeled and advertised as time-limited and include a description of which aspects of the product/certification are time-limited. Additionally, commenters requested we make a filterable tag in the CHPL and/or provide a list of the time-limited products separately.

Response. We appreciate the support expressed by many commenters, and we have finalized the removal of ''2015 Edition'' from § 170.550(m). We look forward to ongoing collaboration with public and private sector partners as we implement the provisions of this final rule.

After consideration of these comments, we have finalized our proposed approach to discontinue year-themed editions. Specifically, we have renamed § 170.315 as the ''ONC Certification Criteria for Health IT'' and replaced references to the ''2015 Edition'' in §§ 170.102, 170.405, 170.406, 170.523, 170.524, and 170.550, with this description.

2. Definition of ''Revised Certification Criterion''

In the HTI–1 Proposed Rule, we described the use of terms meant to describe the status of certification criteria for use in the Program from the 2011 to 2014 Edition transition (88 FR 23760). We also referenced the definitions finalized in the 2015 Edition Final Rule for the following terms:

- ''New'' certification criteria are those that as a whole only include capabilities never referenced in previously adopted certification criteria editions and to which a Health IT Module presented for certification to the 2015 Edition could have never previously been certified.
- ''Revised'' certification criteria are those that include the capabilities referenced in a previously adopted edition of certification criteria as well as changed or additional new capabilities; and to which a Health IT Module presented for certification to the 2015 Edition could not have been previously certified to all of the included capabilities.
- ''Unchanged'' certification criteria are those that include the same capabilities as compared to prior certification criteria of adopted editions; and to which a Health IT Module presented for certification to the 2015 Edition could have been previously certified to all the included capabilities (80 FR 62608).

We proposed that these same terms as applied to the certification criteria would continue to be used by the Program in the absence of a year-named edition. However, for clarity, we proposed to define ''revised certification criterion (or criteria)'' in § 170.102 to mean a certification criterion that meets at least one of the following: (1) has added or changed the capabilities described in the existing criterion in 45 CFR 170 part C; (2) has an added or changed standard or implementation specification referenced in the existing criterion in 45 CFR part 170 subpart B; or (3) is specified through notice and comment rulemaking as an iterative or replacement version of an existing criterion in 45 CFR part 170 subpart C.

We stated in the HTI–1 Proposed Rule that we would continue to use these terms when: communicating proposals for future criteria, such as revising a criterion that will maintain its place in the CFR or establishing a new criterion that is an iterative or replacement criterion in the Program; establishing scenarios for when gap certification is an option for developers of certified health IT; and setting expiration dates or applicable timelines related to standards and certification criteria. Through the development of educational resources, such as fact sheets [24] and resource guides,[25] these designations will help users and the public understand to which versions of standards and certification criteria a Health IT Module may be certified when multiple versions of standards or certification criteria are available under the Program. In the HTI–1 Proposed Rule, we proposed applicability or implementation timelines for both our certification criteria and the standards adopted in 45 CFR part 170 by establishing the dates by which an existing version of a criterion or standard is no longer applicable and by establishing a date by which a new or revised certification criterion or standard version is adopted (88 FR 23760).

Comments. Most commenters supported our proposed definition of ''revised certification criterion (or criteria).''

Response. We appreciate the feedback from commenters. We believe the revised certification criterion (or criteria) definition provides clarity around our approach for setting applicability or implementation timelines for both our certification criteria and the standards adopted in 45 CFR part 170. We have finalized our definition for revised certification criterion (or criteria) as proposed.

Comments. Some commenters suggested better coordination with the Centers for Medicare & Medicaid Services (CMS) to ensure that our definition is consistent and aligned with the Medicare Promoting Interoperability (PI) Program or MIPS Promoting Interoperability performance category.

Response. We appreciate the comment and will continue to coordinate and work with our federal partners, including CMS, on points of intersection for potential future rulemaking. We note that the CY 2024 Physician Fee Schedule Proposed Rule [26] has a discussion related to this policy, and we invite readers to review the discussion at 88 FR 52547.

Comments. One commenter inquired how users of a certified Health IT Module that has been certified to multiple certification criteria that have been revised and included overlapping timeframes for standards updates will know if the Health IT Module is compliant.

Response. ONC has included in the Code of Federal Regulations (CFR) revisions to certification criteria, standards, and implementation specifications—and their associated timelines. To meet a certification requirement, a Health IT Module would need to be updated to the most recently adopted capabilities and standards indicated in the CFR within the timelines specified. For example, if a finalized revised certification criterion references a new standard this year that must be adopted by 2027, and we subsequently revised this certification criterion through rulemaking again in 2026 with a newer version of that standard to be adopted by 2028, then the Health IT Module would need to be updated to the new standard identified this year in the CFR by 2027 and subsequently be updated to the standard identified through rulemaking in 2026 by 2028.

Comments. One commenter inquired how an update to an existing criterion will be identified on the CHPL.

Response. ONC will establish clear requirements and timelines for all revised criteria within the CHPL. To support effective communication of the updates, we will implement a practical approach to facilitate transparency using the CHPL.

Table 1 below includes the revised certification criteria we have finalized in this rule.

TABLE 1—LIST OF FINALIZED HEALTH IT CERTIFICATION CRITERIA

Revised Certification Criteria	
§ 170.315(a)(5)	Clinical—Patient demographics and observations (currently Demographics).
§ 170.315(a)(9)	Clinical—Clinical decision support (CDS) at § 170.315(a)(9) (to be moved to the ''Care Coordination'' certification criteria as the ''decision support intervention'' criterion at § 170.315(b)(11)'').
§ 170.315(b)(1)	Care Coordination—Transitions of care.
§ 170.315(e)(1)	Patient Engagement—View, download, and transmit to 3rd party.
§ 170.315(f)(5)	Public Health—Transmission to public health agencies—electronic case reporting.
§ 170.315(g)(10)	Design and Performance—Standardized API for patient and population services.
Revised Certification Criteria (standards updates)	
§ 170.315(a)(12)	Clinical—Family health history.
§ 170.315(b)(2)	Care Coordination—Clinical information reconciliation and incorporation.
§ 170.315(b)(6)	Care Coordination—Data export.
§ 170.315(b)(9)	Care Coordination—Care plan.
§ 170.315(c)(4)	Clinical Quality Measures—Clinical quality measures—filter.
§ 170.315(f)(1)	Public Health—Transmission to immunization registries.
§ 170.315(f)(3)	Public Health—Transmission to public health agencies—reportable laboratory tests and values/results.

[24] See 2015 Edition Cures Update Fact Sheet: *https://www.healthit.gov/sites/default/files/page/2022-03/Cures-Update-Fact-Sheet.pdf.*

[25] See API Resource Guide: *https://onc-healthit.github.io/api-resource-guide/.*

[26] ''Medicare and Medicaid Programs; CY 2024 Payment Policies Under the Physician Fee Schedule and Other Changes to Part B Payment and Coverage Policies; Medicare Shared Savings Program Requirements; Medicare Advantage; Medicare and Medicaid Provider and Supplier Enrollment Policies; and Basic Health Program'' (88 FR 52262).

TABLE 1—LIST OF FINALIZED HEALTH IT CERTIFICATION CRITERIA—Continued

§ 170.315(f)(4)	Public Health—Transmission to cancer registries.
§ 170.315(g)(3)	Design and Performance—Safety-enhanced design.
§ 170.315(g)(6)	Design and Performance—Consolidated CDA creation performance.
§ 170.315(g)(9)	Design and Performance—Application access—all data request.

In the HTI–1 Proposed Rule, we included proposed modifications to our approach for setting applicability or implementation timelines for each certification criteria and the applicable standards adopted in 45 CFR part 170 (88 FR 23761). In this final rule, we have finalized that proposal to incorporate the applicable timelines and ''expiration dates'' for capabilities and standards updates within each individual criterion or standard.

We direct readers to section III.C.11 of this final rule for further discussion of the requirements for health IT developers voluntarily participating in the Program related to health IT certification updates.

3. Program Oversight Related to Discontinuation of Editions

a. Records Retention

In the ONC Cures Act Final Rule, we revised the Principles of Proper Conduct for ONC–ACBs and ONC–ATLs by amending the records retention policies to include the ''life of the edition'' (85 FR 25710 through 25713). Specifically, we clarified that the records retention provisions in §§ 170.523 and 170.524 included the ''life of the edition'' as well as three years after the retirement of an edition related to the certification of Complete EHRs and Health IT Modules. We explained that ''[b]ecause the 'life of the edition' begins with the codification of an edition of certification criteria in the CFR and ends on the effective date of the final rule that removes the applicable edition from the CFR, the start and end dates for the 'life of the edition' are published in the **Federal Register** in the rulemaking actions that finalize them. The period of three years beyond the 'life of the edition' begins on the effective date of the final rule that removes the applicable edition from the CFR, thus the three-year period after removal from the CFR continues through three full calendar years following that date'' (85 FR 25710).

In the HTI–1 Proposed Rule, we proposed to maintain a single set of ''ONC Certification Criteria for Health IT'' and not an edition, so we therefore proposed to revise § 170.523 and § 170.524 (88 FR 23762). We proposed that the period of three years begins on the effective date of the final rule that removes the applicable ONC certification criterion or criteria for health IT from the CFR, thus the three-year period after removal from the CFR continues through three full calendar years following that date (in addition to the calendar year in which it was removed). We also retained the ''Complete EHR'' language in these sections because beginning with the 2015 Edition, Complete EHR certifications could no longer be issued. However, since the 2014 Edition was not removed from the CFR until the ONC Cures Act Final Rule, which became effective on June 30, 2020, records would need to be retained (including Complete EHRs) until June 30, 2023.

Comments. A majority of commenters, including individuals, professional trade associations, and other interested parties expressed support for the ONC–ATLs retaining the records of Complete EHRs' and Health IT Modules' testing through a minimum of three years from the effective date of the removal of those certification criteria from the CFR. Commenters indicated such requirements were reasonable, particularly in relation to the retirement of the edition concept, and they indicated that these records could better facilitate surveillance and enforcement of certification criteria and transparency for customers. One commenter highlighted the importance of retaining those records for historical documentation regarding their health IT vendors' certification status. One commenter suggested ONC expand the three-year requirement to six years, to align with the HIPAA Privacy Rule's retention period.

Response. We appreciate the commenters' support for continuing our current three-year retention policy and our proposed modifications that the retention policy would be effective for three full calendar years beginning on the effective date of the final rule that removes the applicable ONC certification criterion or criteria for health IT from the CFR. We agree that maintaining those records for historical documentation is important and have finalized our policy as proposed. We do not believe that a six-year retention policy is needed at this time because it may result in more burden than is warranted. However, we will continue to monitor the effectiveness of our existing retention policy and consider changes as needed, including consulting with Federal partners that conduct federal program enforcement, such as the HHS OIG.

Comments. Commenters suggested ONC establish an organized system of documentation management for each Health IT Module/developer to be shared on the CHPL to streamline the process and enhance efficiency; to adopt new indicators of current certification status each time a criterion certified as part of a Health IT Module is incrementally updated; and to create a special coding system that represents the most current year of certification for Health IT Modules to support oversight and compliance requirements health care providers may have with other programs such as the CMS Quality Payment Program.

Response. We appreciate commenters identifying options for enhancing how the Program documents certification status for Health IT Modules as we retire the year-themed edition approach. We note that the CHPL primarily serves as a comprehensive repository of certified health IT products and their corresponding certification details. While it provides information about certified health IT products, it does not specifically serve as a documentation management system for Modules/developers. The CHPL provides transparency and access to certification information, including the certification criteria used for certifying a Health IT Module, test results, and certified health IT product details. It serves as a valuable resource for users to verify the certification status and capabilities of Health IT products. Overall, we will take these comments, and related comments received, into consideration as we implement removal of year-themed editions in the Program.

b. Records Retention—Complete EHR

In the HTI–1 Proposed Rule, we proposed to retain the ''Complete EHR'' language in §§ 170.523 and 170.524 even though, beginning with the 2015 Edition, Complete EHR certifications could no longer be issued. We did so because the records for 2014 Edition Complete EHR certifications still needed to be retained until the records retention timeframe expired on June 30, 2023. Though not specifically stated in the HTI–1 Proposed Rule, the removal of

the ''Complete EHR'' language from all reference points in §§ 170.523 and 170.524 could have been reasonably anticipated once June 30, 2023, had passed. Therefore, since the date has now passed and because retaining ''Complete EHR'' in the regulation text may cause confusion for the public, we have removed all remaining references to the ''Complete EHR'' language in §§ 170.523 and 170.524.

B. Standards and Implementation Specifications

1. National Technology Transfer and Advancement Act

The National Technology Transfer and Advancement Act (NTTAA) of 1995 (15 U.S.C. 3701 *et seq.*) and the Office of Management and Budget (OMB) Circular A–119 [27] require the use of, wherever practical, technical standards that are developed or adopted by voluntary consensus standards bodies to carry out policy objectives or activities, with certain exceptions. The NTTAA and OMB Circular A–119 provide exceptions to electing only standards developed or adopted by voluntary consensus bodies, namely when doing so would be inconsistent with applicable law or otherwise impractical. Agencies have the discretion to decline the use of existing voluntary consensus standards if it is determined that such standards are inconsistent with applicable law or otherwise impractical, and instead use a government-unique standard or other standard. In addition to the consideration of voluntary consensus standards, the OMB Circular A–119 recognizes the contributions of standardization activities that take place outside of the voluntary consensus standards process. Therefore, in instances where use of voluntary consensus standards would be inconsistent with applicable law or otherwise impracticable, other standards should be considered that meet the agency's regulatory, procurement, or program needs, deliver favorable technical and economic outcomes, and are widely utilized in the marketplace.

In this final rule, we use voluntary consensus standards except for:

- The standard adopted in § 170.213, the United States Core Data for Interoperability Version 3 (USCDI v3), is a hybrid of government policy (*i.e.,* determining which data to include in the USCDI) and voluntary consensus standards (*i.e.,* the vocabulary and code set standards attributed to USCDI data elements); and
- The standard adopted in § 170.207(f)(3) for race and ethnicity.

We are not aware of any voluntary consensus standards that could serve as an alternative for the purposes we describe in further detail throughout this final rule including establishing a baseline set of data that can be exchanged across care settings for a wide range of uses. We refer readers to section III.C.1 of this preamble for a discussion of the USCDI.

Comments. One commenter suggested ONC look at the work of the FHIR accelerators as meeting the requirements of 'voluntary consensus bodies' outlined in the OMB Circular A–119 for standards and frameworks that fall outside of the HL7 process. The commenter stated that as an example, CARIN has worked with FAST to develop a framework for how digital identity is federated across healthcare participants with the CARIN/HHS Healthcare Digital Identity Federation Proof of Concept report in which ONC participated. The commenter encouraged ONC to leverage the open-source work that has been done to advance digital identity federation in future rulemaking.

Response. We thank commenters for their input. We will consider leveraging the work that the commenter suggested in future rulemakings.

2. Compliance With Adopted Standards and Implementation Specifications

In accordance with Office of the Federal Register regulations related to ''incorporation by reference,'' 1 CFR part 51, which we follow when we adopt proposed standards and implementation specifications in any subsequent final rule, the entire standard or implementation specification document is deemed published in the **Federal Register** when incorporated by reference therein with the approval of the Director of the Federal Register. Once published, compliance with the standard and implementation specification includes the entire document unless we specify otherwise. If an element of the IG is optional or permissive in any way, it will remain that way for testing and certification unless we specified otherwise in regulation. In such cases, the regulatory text would preempt the permissiveness of the IG.

3. ''Reasonably Available'' to Interested Parties

The Office of the Federal Register has established requirements for materials (*e.g.,* standards and implementation specifications) that agencies propose to incorporate by reference in the Code of Federal Regulations (79 FR 66267; 1 CFR 51.5(b)). To comply with these requirements, in section V (''Incorporation by Reference'') of this preamble, we provide summaries of, and uniform resource locators (URLs) to, the standards and implementation specifications we have adopted and subsequently incorporate by reference in the Code of Federal Regulations. To note, we also provide relevant information about these standards and implementation specifications throughout the relevant sections of this final rule.

C. New and Revised Standards and Certification Criteria

1. The United States Core Data for Interoperability Version 3 (USCDI v3)

As discussed in the HTI–1 Proposed Rule, the USCDI is a standardized set of health data classes and constituent data elements for nationwide, interoperable health information exchange [28] (88 FR 23751). USCDI v1 established a baseline set of data that can be commonly exchanged across care settings for a wide range of uses and is a required part of certification criteria in the 2015 Edition Cures Update. For the overall structure and organization of USCDI, including data classes and data elements in USCDI v1, please see the discussion in the ONC Cures Act Final Rule (85 FR 25669–25670), as well as *www.healthIT.gov/uscdi.*

We stated in the ONC Cures Act Final Rule that we intended to utilize a predictable, transparent, and collaborative process to expand USCDI, including providing the public with the opportunity to comment on USCDI's expansion (85 FR 25670). We also noted that developers of certified health IT would be able to use the Standards Version Advancement Process (SVAP) to voluntarily implement and use a newer, National Coordinator-approved version of USCDI without waiting for ONC to propose and adopt via rulemaking an updated version of the USCDI (85 FR 25669). We, therefore, established a process for expanding USCDI based on public input and submissions of new data elements and classes.[29] To enable these submissions, we created the ONC New Data Element and Class (ONDEC) submission system, which provides the public with the opportunity to submit new data

[27] *https://www.whitehouse.gov/wp-content/uploads/2020/07/revised_circular_a-119_as_of_1_22.pdf.*

[28] *https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi.*

[29] *https://www.healthit.gov/buzz-blog/interoperability/uscdi-onc-new-data-element-and-class-submission-system-now-available.*

elements for consideration for inclusion in future versions of USCDI.[30]

In the HTI–1 Proposed Rule, we proposed to update the USCDI standard in § 170.213 by adopting the newly released USCDI v3 and establishing a January 1, 2025, expiration date for USCDI v1 (July 2020 Errata) for purposes of the Program. We proposed to add USCDI v3 in § 170.213(b) and incorporate it by reference in § 170.299. Specifically, we proposed in the HTI–1 Proposed Rule to adopt USCDI v3 (October 2022 Errata). We also proposed to codify the existing reference to USCDI v1 (July 2020 Errata) in § 170.213(a). Lastly, we proposed that as of January 1, 2025, any developers seeking certification for their Health IT Modules to criteria that reference the standards in § 170.213 would need to be capable of exchanging the data elements that comprise USCDI v3.

Comments. We received a large number of comments expressing overall support for our proposals to adopt USCDI v3 in § 170.213(b) and for USCDI v1 to expire on January 1, 2025. Many commenters specifically supported the inclusion of SDOH data elements in USCDI v3 and noted that more accurate and complete patient characteristics will help address health disparities. Several commenters in support of our proposals specifically agreed with the proposed deadline. Commenters supporting our proposal also noted that it would reduce burden, advance interoperability, support quality measurement initiatives, and support providers' ability to acquire and share the information needed to provide the best care for their patients.

Response. We thank commenters for the support of our proposals and for recognizing potential benefits such as reduced burden, increased interoperability, more complete data, and the ability to support quality measurement initiatives and better address health disparities.

Comments. We received numerous comments that expressed concern about the proposed deadline and advocated for an extension. These comments generally expressed concern about the burden on developers posed by the proposed deadline, stating that more time would be needed to successfully adopt USCDI v3, including development, implementation, and testing, and stressed that it would be a large undertaking for developers as well as for health care providers. Some commenters recommended moving the deadline to the end of the calendar year which is no shorter than 24 months from the publication of this final rule. Some commenters suggested extending the compliance deadline by six months, and others suggested compliance dates of December 31, 2025, or January 1, 2026. Several commenters mentioned the need for ONC to coordinate with CMS on timelines, and one mentioned the need to allow providers a ''flex'' year after the certification deadline during which to upgrade. Some comments suggested aligning compliance deadlines with the availability of scalable FHIR-based API standards, which they stated could help support successful implementation of USCDI v3, while others suggested waiting to adopt USCDI v3 until after Release 4 of the C–CDA Companion Guide is finalized. Some commenters stated that USCDI v3 should not be required until all of the standards supporting USCDI v3 are officially published.

Additionally, a number of commenters requested clarification from ONC related to the proposed adoption of USCDI v3. This included clarification on future updates to USCDI; how USCDI works with CMS rules and programs; the applicability of USCDI v2 once USCDI v3 is adopted; the distinction between USCDI, USCDI+ and US Core; the lack of vocabulary standards for some USCDI v3 data elements; and the expectations regarding data sharing.

Response. We thank commenters for expressing a desire for an extension on proposed deadlines. USCDI v3 includes all data elements in USCDI v2, as well as additional data elements. In response to commenters' feedback, we have extended the deadline for the expiration of USCDI v1 in § 170.213 to January 1, 2026. We believe the extended time, combined with the fact that USCDI v3 has been publicly available since July 2022, will make it feasible for all interested parties to meet the revised deadline. We note that USCDI v3 has been available for use in the Program using the FHIR US Core 6.1.0 and C–CDA Companion Guide R4.1 through SVAP effective September 11, 2023.[31] In response to comments suggesting that USCDI v3 lacks vocabulary standards, in the USCDI v3 standard ONC has identified applicable vocabulary standards for those USCDI data elements where a coded value is expected, a standard code set is currently in use, and where the submitters and commenters have provided evidence of current use. Further terminology bindings are defined in the C–CDA Companion Guide and HL7 US Core Implementation Guide.

In response to the comment requesting that ONC explain the distinction between USCDI, USCDI+, and US Core, we note that the USCDI+ program was not referenced in the HTI–1 Proposed Rule. USCDI+ supports the identification and establishment of domain or program-specific datasets that will operate as extensions to USCDI and uses similar processes as the USCDI, such as seeking input from the Health IT Advisory Committee and other interested partners to stimulate public engagement and help shape USCDI+ datasets.

As we have described previously, the USCDI is a standardized set of health data classes and constituent data elements for nationwide, interoperable health information exchange. In order for the USCDI to be implemented with specific exchange modalities or functionalities, additional specifications are required to provide guidance on how the USCDI should be implemented in the context of that exchange method. The US Core and C–CDA implementation guides are aligned to specific versions of USCDI and provide the implementation specification and expectations for each particular version of USCDI. In this case, we have finalized USCDI v3 and the applicable FHIR US Core Implementation Guide (FHIR US Core 6.1.0) and C–CDA Companion Guide (C–CDA Companion Guide R4.1), both of which provide guidance on how to implement the updates from USCDI v1 to USCDI v3.

We recognize that we stated in the HTI–1 Proposed Rule that we would consider adopting the most up-to-date versions of the FHIR US Core and C–CDA Companion Guide specifications that align with the updates to USCDI v3 (FHIR US Core 6.0.0 and C–CDA Companion Guide R4). However, after the publishing of FHIR US Core 6.0.0 and C–CDA Companion Guide R4, HL7 found errors with how the guides implemented data elements in USCDI v3 and had to make updates to those specifications to align with USCDI v3 and ensure that USCDI v3 can be implemented in Health IT Modules. Adopting FHIR US Core 6.1.0 and C–CDA Companion Guide R4.1 is necessary for developers of certified health IT to have appropriate implementation guidance to meet the criteria adopted in this final rule that reference USCDI v3. Based on public comments on this and prior rulemakings, we believe that the health IT industry, healthcare standards developers, and health care providers expect and support ONC making such

[30] *https://www.healthit.gov/isa/ONDEC.*

[31] *https://www.healthit.gov/sites/default/files/2023-07/2023_SVAP_Fact_Sheet.pdf.*

determinations so that the adopted version of standards are the most up-to-date available and are feasible for real-world implementation (see, for example, 85 FR 25677 and 25708).

In response to comments regarding how CMS or other federal programs incorporate USCDI into rules and programs, we note that ONC receives submissions and comments from federal partners, including CMS, on USCDI content and will continue to work towards alignment where appropriate with these partners.

In response to comments on future updates to USCDI, we clarify that USCDI generally expands annually to keep pace with clinical, technology, and policy changes.[32] ONC follows a predictable, transparent, and collaborative process for updating USCDI that allows interested parties to submit new data elements and classes for future versions of USCDI through the ONDEC submission system. Regarding applicability, USCDI v2 will not be available for new and updating certifications via SVAP after December 31, 2023. We erroneously stated in the HTI–1 Proposed Rule that USCDI v2 would remain available via SVAP until December 31, 2024 (88 FR 23764); however, our intention was that USCDI v2 would remain available via SVAP until it sunsets. USCDI v2 sunsets on December 31, 2023 and will no longer be available via SVAP after that date.[33]

Comments. We received numerous comments expressing concerns about privacy and the implementation of USCDI v3. These commenters generally noted that USCDI v3 includes data elements that may contain sensitive health information, including mental health, substance use, and reproductive health information, the disclosure of which could increase the risk of harassment or harm toward providers and patients. Several of these commenters noted the need for ONC to create education materials around the fact that USCDI v3 does not require sharing of sensitive information. Some commenters recommended that ONC remove data elements that provide personally identifiable information that does not support the provision of care. Several comments encouraged ONC to consider requiring granular data segmentation policies concurrently with adopting USCDI v3. Commenters also requested that ONC consider removing any personally identifiable data elements in USCDI that do not provide value in order to avoid re-identification, or alternatively to revise policies that require automatic inclusion of all data elements in the USCDI.

Response. We thank commenters for their feedback regarding the importance of addressing the privacy and confidentiality of sensitive information. The adoption of USCDI v3 sets a new baseline for the capability of Health IT Modules certified to particular certification criteria to capture and exchange data but does not dictate when and how either of those two actions occur. We have not adopted new or additional privacy standards related to controlling sensitive data that may be represented in USCDI data elements. However, our existing criteria in § 170.315(b)(7) and (b)(8) include support for privacy and security labels in health information exchange workflows and these criteria reference the HL7® Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1 adopted in § 170.205(o)(1) and incorporated by reference in § 170.299. In addition, we have adopted a new requirement as part of the certification criterion in § 170.315(e)(1) in support of the HIPAA Privacy Rule's individuals' ''right to request a restriction'' as discussed in section III.C.10. For more on patient requested restrictions on sharing of their health information, we refer readers to section III.C.10 for discussion on modifications to the ''view, download, and transmit to 3rd party'' certification criterion in § 170.315(e)(1), stating that patients (and their authorized representatives) must be able to use an internet-based method to request a restriction to be applied for any data expressed in the standards in § 170.213. The HIPAA Privacy Rule provides federal protections for PHI held by covered entities and gives individuals an array of rights with respect to that information.

Comments. We received multiple comments expressing concern about provider burden, including administrative, cognitive, and documentation burden associated with USCDI data elements. Some commenters also expressed concerns about the cost burden of implementing USCDI v3, noting that it could require numerous downstream standards updates, migration costs, costs to standardize and use unconstrained data, and costs related to software, IT infrastructure, workforce recruiting and training, and ongoing operational costs. Several commenters were particularly concerned about the potential costs to public health organizations and to small and rural providers, which may have limited budgets or resources to devote to the implementation of EHR systems capable of collecting and sharing data according to the USCDI v3 standard. Several commenters suggested that ONC provide resources and support to providers to help reduce provider burden. One commenter proposed a test or pilot to ensure that burdens are not shifted to providers when USCDI v3 is implemented. Another commenter proposed that ONC consider regulations to prevent developers of certified health IT from increasing fees due to the update to USCDI v3.

Response. We thank commenters for the feedback regarding implementation burden and the adoption of USCDI v3. As we have noted, the adoption of USCDI v3 sets a new baseline for the *capability* of Health IT Modules certified to particular certification criteria to capture and exchange data. USCDI v3 does not dictate when and how either of those two actions occur, including with what frequency health care providers document information that could be captured as part of the data elements within USCDI v3. We also note that we have established a predictable, transparent, and collaborative expansion process for USCDI based on public evaluation of previous versions and submissions by the health IT community. Each of the data elements in USCDI v3 has been evaluated for overall value, maturity, and ease of implementation. In addition, the data elements (as applicable) are represented by health IT standard terminologies, technical specifications, or implementation guides, and are used extensively in production electronic systems. We intend to provide implementation resources such as implementation guide validators for both HL7 C–CDA and FHIR corresponding implementation guides to USCDI v3. However, we decline to conduct a test pilot or create additional regulations focused on burden and USCDI v3 at this time.

We appreciate the comments related to implementation burden for rural and small providers and understand concerns about the overall downstream impact of the HTI–1 Proposed Rule on entities beyond developers of certified health IT to which ONC authorities apply. As part of our Regulatory Impact Analysis in section VII, we have identified that developers of certified health IT are largely private businesses who operate in a competitive marketplace, and they may not bear all costs to meet regulatory requirements.

Comments. Several commenters expressed concerns about data quality when USCDI v3 is implemented and suggested that ONC work with the

[32] *https://www.healthit.gov/sites/default/files/page/2023-07/Standards_Bulletin_2023-2.pdf.*

[33] *https://www.healthit.gov/topic/standards-version-advancement-process-svap.*

industry on developing standards. Several commenters expressed concerns about the lack of use cases and standards related to USCDI v3 and suggested that ONC develop those.

Response. We thank commenters for their feedback. We work directly with HL7 to finalize HL7® FHIR® US Core and C–CDA Companion Guide specifications for each published version of USCDI, including USCDI v3. These specifications include terminology bindings to value sets drawn from standard code sets, where appropriate. To further support implementation of USCDI v3, we will update the C–CDA validator [34] and Inferno [35] test tools to align with USCDI v3 and validate the quality of the data. We will continue to identify opportunities to work with industry to improve data quality. For example, we recently awarded a Leading Edge Acceleration Project (LEAP) award to explore enabling easy access to high-quality, standardized healthcare data, with a focus on USCDI in FHIR and open-source platforms.[36]

Comments. Several commenters expressed concern that not all data elements in USCDI v3 are applicable to all users and urged that ONC allow EHRs flexibility in adopting USCDI v3. These commenters generally urged ONC to allow EHRs to add only the data elements needed by their users. Commenters also urged ONC to explore a modular approach for USCDI that would group data elements to support specific use cases, noting that this would help reduce burden and costs while improving care.

Response. We thank commenters for the input suggesting that ONC allow flexibility in supporting USCDI v3 data classes and data elements for purposes of the Program. We decline to allow developers to be selective in which USCDI v3 data classes and data elements they support for purposes of the Program. The USCDI standard is intended to provide a common set of data classes and data elements in support of nationwide health information exchange, therefore, partial adoption of the USCDI standard would impact the effectiveness of the standard and impede interoperability. Additionally, we recognize that not all USCDI v3 data elements originate in an EHR, however Health IT Modules certified to particular certification criteria must be able to capture and exchange the values when available.

Comments. One commenter suggested that ONC establish a framework for certification of specialty EHRs and non-EHRs to help promote USCDI uptake across the care continuum.

Response. We thank the commenter for their suggestion that ONC establish a framework for certification to support specialty EHRs and non-EHRs to promote USCDI uptake across the care continuum. At this time, we decline to provide selective certification frameworks for purposes of the Program. The USCDI standard is intended to provide a common set of data classes and data elements in support of nationwide health information exchange.

Comments. Several commenters expressed a preference for USCDI v4 over USCDI v3, noting that it will help the healthcare marketplace and encourage competition. One comment encouraged ONC to finalize USCDI v4 in 2023 and require support by the end of 2024.

Response. We thank commenters for the comments in support of USCDI v4. However, we did not propose, and therefore decline to adopt, USCDI v4 in the USCDI standards in § 170.213 at this time. We have adopted USCDI v3 in § 170.213(b) as proposed. Additionally, we note that implementation guides are not yet released to support USCDI v4.

Comments. A number of commenters generally encouraged ONC to work with CMS on timelines and on alignment with program requirements, including aligning future USCDI updates with CMS programs.

Response. We thank commenters for the comments regarding working with CMS and assure commenters that we work closely with CMS across multiple programs and initiatives on aligning program requirements and deadlines. We will continue to do so in the future. Those CMS programs include, but are not limited to, the Quality Payment Program, Inpatient Quality Reporting Program, and Medicare Promoting Interoperability Program, as well as regulatory proposals such as the Interoperability and Prior Authorization Proposed Rule (87 FR 76238).[37]

Comments. Several commenters encouraged ONC to maintain awareness of state agency data exchange requirements and to work to alleviate discrepancies, noting that the variances in USCDI versioning pose challenges industry-wide if not aligned with state and federal regulations.

Response. We thank commenters for the comments regarding state agency data exchange requirements and assure commenters that we monitor and are aware of state and federal regulations impacting adoption of USCDI v3.

Comments. There were a number of comments requesting technical support, education, and other resources or actions from ONC related to adopting and implementing USCDI v3. These included addressing semantic differences across health systems, developing mappings and value sets for data elements, improving the specificity and testing requirements for USCDI, expediting the availability of high-quality testing tools, developing and publicizing an analysis of which USCDI elements are interoperable, and aligning data standardization efforts across programs.

Response. We acknowledge the comments requesting resources and technical support from ONC related to adoption of USCDI v3. We maintain a variety of resources and technical support related to USCDI, including numerous resources related to the Program. Resources include Certification Companion Guides (CCGs) and Test Procedures related to specific certification criterion to assist developers that are seeking to certify to the criteria.[38] Any considerations for implementing USCDI in compliance with these criteria are, additionally, outlined in these resources. In addition, there is a USCDI CCG that includes clarifications for specific data classes and elements as they relate to terminology standards and/or implementation guides. The Program offers testing and conformance methods for verification that a product meets criteria requirements. Other technical documentation may be found on ONC's website: *https://www.healthit.gov/uscdi*.

Comments. There were also a number of commenters that made suggestions for future versions of USCDI. Commenters suggested improving the USCDI interface and allowing comment on proposed value sets. Various commenters suggested adding specific

[34] *https://site.healthit.gov/sandbox-ccda/ccda-validator*.

[35] *https://inferno.healthit.gov/*.

[36] *https://www.healthit.gov/sites/default/files/page/2023-04/LEAP%20FY2023%20SEN_508.pdf*.

[37] ''Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Advancing Interoperability and Improving Prior Authorization Processes for Medicare Advantage Organizations, Medicaid Managed Care Plans, State Medicaid Agencies, Children's Health Insurance Program (CHIP) Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally-Facilitated Exchanges, Merit-Based Incentive Payment System (MIPS) Eligible Clinicians, and Eligible Hospitals and Critical Access Hospitals in the Medicare Promoting Interoperability Program.'' (87 FR 76238). *See https://www.federalregister.gov/documents/2022/12/13/2022-26479/medicare-and-medicaid-programs-patient-protection-and-affordable-care-act-advancing-interoperability*.

[38] *https://www.healthit.gov/topic/certification-ehrs/certification-health-it*.

data elements in future versions of USCDI, including the following:

- marital status
- education
- water insecurity
- value-based care
- prescription drug insurance information
- advance directive documentation
- clinical orders
- care experience preference
- newborn delivery information
- vaccine administration date
- vaccination event record type
- medical record number
- mother's maiden name
- multiple birth indicator
- birth order

Response. We thank commenters for the feedback and suggestions regarding future versions of USCDI. The USCDI v3 is a published standard at *https://www.healthit.gov/isa/sites/isa/files/2022-10/USCDI-Version-3-October-2022-Errata-Final.pdf* and thus it is not possible to add new data elements to USCDI v3 through the rulemaking process or other means at this time. We direct commenters to the USCDI website, available at *https://www.healthit.gov/uscdi,* where the public is invited to enter comments on leveled data elements or submit new data elements for consideration in future versions of USCDI.

a. Certification Criteria That Reference USCDI

As discussed in the HTI–1 Proposed Rule, the USCDI standard is currently cross-referenced, via cross-reference to § 170.213, in certain certification criteria (88 FR 23763). The criteria cross-referencing to USCDI via cross-reference to § 170.213 are as follows:

- ''Care coordination—Transitions of care—Create'' (§ 170.315(b)(1)(iii)(A)(*1*));
- ''Care coordination—Clinical information reconciliation and incorporation—Reconciliation'' (§ 170.315(b)(2)(iii)(D)(*1*) through (*3*));
- ''Patient engagement—View, download, and transmit to 3rd party—View'' (§ 170.315(e)(1)(i)(A)(*1*));
- ''Design and performance—Consolidated CDA creation performance'' (§ 170.315(g)(6)(i)(A));
- ''Design and performance—Application access—all data request—Functional requirements'' (§ 170.315(g)(9)(i)(A)(*1*)); and
- ''Design and performance—Standardized API for patient and population services—Data response'' (§ 170.315(g)(10)(i)(A) and (B)).

We noted in the HTI–1 Proposed Rule that § 170.315(f)(5) also currently references § 170.213; however, we proposed to rely on specific IGs for that criterion, rather than reference § 170.213 (88 FR 23763). We proposed that through December 31, 2024, a Health IT Module certified to the criteria above that cross-reference § 170.213 may be certified by complying with (1) USCDI v1; (2) USCDI v2 under SVAP; and (3) USCDI v3 (88 FR 23763). We proposed to allow only USCDI v3 after this date for the criteria that cross-reference § 170.213.

We noted in the HTI–1 Proposed Rule that a developer of certified health IT will not be required to provide technology updates for certified criteria or standards to a user who declined such updates; however, if such an update is not provided, that version of the Health IT Module will no longer be considered certified under the Program (88 FR 23764).

In the HTI–1 Proposed Rule, we proposed in the preamble to add introductory text to § 170.213 noting that the Secretary adopts the following standards as the standards available for representing EHI (88 FR 23764), and we proposed in the regulatory text to add introductory text to § 170.213 stating the Secretary adopts the following versions of the USCDI standard (88 FR 23907). This discrepancy was inadvertent, and we clarify that we intended to propose introductory text to § 170.213 stating the Secretary adopts the following versions of the USCDI standard. We also proposed to include the date the adoption of the standard in § 170.213(a) expires. Consistent with our proposals in sections III.A and III.C.11, we proposed this expiration date to be January 1, 2025. Health IT developers with Health IT Modules certified to certification criteria that reference § 170.213 would have to update such certified health IT to USCDI v3 and provide it to customers by December 31, 2024. Further, we proposed that Health IT Modules certified to the above-listed certification criteria would need to update their Health IT Modules to accommodate USCDI v3 data elements using the FHIR US Core Implementation Guide Version 5.0.1 in § 170.215(b)(1)(ii) and the HL7 CDA® R2 IG: C–CDA Templates for Clinical Notes R2.1 Companion Guide, Release 3 in § 170.205(a)(6). We noted in the HTI–1 Proposed Rule that if the FHIR US Core Implementation Guide and the HL7 CDA® R2 IG: C–CDA Templates for Clinical Notes R2.1 Companion Guide are updated before the date of publication of this final rule, it would be our intent to consider adopting the updated versions that support USCDI v3.

We refer to the term ''expires'' in standards throughout this final rule, and it means that the standard is unavailable for use in the Program, or any other programs that may cite the standard, as of the expiration date.

Additionally, because we finalized in the ONC Cures Act Final Rule that the Common Clinical Data Set (CCDS) would no longer be applicable for certified Health IT Modules 24 months after the publication date of the ONC Cures Act Final Rule (85 FR 25671), and then extended that date to December 31, 2022, in the interim final rule titled ''Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID–19 Public Health Emergency'' (85 FR 70073), we proposed to remove references to CCDS in the following sections of 45 CFR 170.315: § 170.315(b)(1)(iii)(A)(*2*); (e)(1)(i)(A)(*2*); (g)(6)(i)(B); and (g)(9)(i)(A)(*2*). In each of those sections, we proposed to instead include a reference to USCDI. Because § 170.315(b)(6)(ii)(A), which also references CCDS, is still available for the period before December 31, 2023, we did not propose to remove the reference to CCDS in that section.

Comments. A number of commenters expressed support for ONC's proposals regarding certification criteria that reference USCDI. Commenters stated this would support health equity by design, help capture more accurate and complete patient data, and help address health disparities.

Response. We thank commenters for support of our proposals and for recognizing the potential benefits. We note that the implementation guides we proposed in the HTI–1 Proposed Rule aligned with USCDI v2, and since the publication of the HTI–1 Proposed Rule, HL7 released updated FHIR US Core and C–CDA Companion Guides that align with the updates to USCDI v3. However, after the publishing of US Core 6.0.0 and C–CDA Companion Guide 4.0, HL7 found errors with how the guides implemented data elements in USCDI v3 and had to make updates to those specifications to align with USCDI v3 and to ensure that USCDI v3 can be implemented in Health IT Modules. Given the adoption of USCDI v3, we have finalized the FHIR US Core 6.1.0 and C–CDA Companion Guide R4.1, which are the most recent versions that align with USCDI v3. FHIR US Core 6.1.0 and C–CDA Companion Guide R4.1 have not added any substantial functionality or requirements. We do not believe adoption of FHIR US Core 6.1.0 and C–CDA Companion Guide R4.1 would contribute to a greater

implementation burden, and FHIR US Core 6.1.0 and C–CDA Companion Guide R4.1 are the only versions of their respective implementation guides that fully align with and support the complete USCDI v3.

As discussed earlier in this section, we recognize that we stated in the HTI–1 Proposed Rule that we would consider adopting the most up-to-date versions of the FHIR US Core and C–CDA Companion Guide specifications that align with USCDI v3 *FHIR US Core 6.0*~~1~~*.0 and C–CDA Companion Guide R4)*~~.1~~. However, after the publishing of *FHIR* US Core 6.0.0 and C–CDA Companion Guide R4, HL7 found errors with how the guides implemented data elements in USCDI v3 and had to make updates to those specifications to align with USCDI v3 and ensure that USCDI v3 can be implemented in Health IT Modules. Adopting FHIR US Core 6.1.0 and C–CDA Companion Guide R4.1 is necessary for developers of certified health IT to have appropriate implementation guidance to meet the criteria adopted in this final rule that reference USCDI v3. Based on public comments on this and prior rulemakings, we believe that the health IT industry, healthcare standards developers, and health care providers expect and support ONC making such determinations so that the adopted version of standards are the most up-to-date available and are feasible for real-world implementation (see, for example, 85 FR 25677 and 25708).

Comments. Several commenters suggested ONC should establish a more formal schedule for adopting future versions of USCDI into the Program, in addition to requests for clarification on the availability of USCDI v2 under SVAP. Commenters also recommended updating SVAP to allow at least two new versions of the same standard (*e.g.,* USCDI v2 and USCDI v3) to be available under SVAP at a time.

Response. We thank the commenters for the suggestion. Generally, ONC updates USCDI on an annual basis, usually over the summer after an extensive public comment period. We decline to adopt a more formalized schedule; however, we promote widely the availability of draft versions of USCDI and engage heavily with interested parties, including the HITAC on new versions. As finalized in this rule, developers of certified health IT are able to certify Health IT Modules to certification criteria that reference USCDI v1 until it expires on January 1, 2026. Beginning on January 1, 2026, only USCDI v3 will be available in § 170.213 as the USCDI standard for use by developers of certified health IT. Under SVAP, developers of certified health IT had the opportunity to certify their Health IT Modules to certification criteria that reference USCDI using USCDI v2 from July 2021 through December 2023. Because we approved a newer version of USCDI—USCDI v3 in July 2023 as part of approved standards for 2023 SVAP—Health IT Modules not already certified to USCDI v1 or v2 may adopt USCDI v3 instead. USCDI v2 will not be available for new and updating certifications via SVAP after December 31, 2023. In this final rule, we have codified USCDI v3 in § 170.213(b), and thus it will not be necessary to use the SVAP process to advance to USCDI v3 after this final rule is effective. In general, these comments are out of scope for this final rule as we did not request feedback on the SVAP program as part of the HTI–1 Proposed Rule.

b. USCDI Standard—Data Classes and Elements Added Since USCDI v1

USCDI v3 includes all data elements defined in USCDI v1 and USCDI v2, as well as additional data elements added in USCDI v3. In the HTI–1 Proposed Rule, we described the data classes and data elements in USCDI v3 that are not included in USCDI v1, as well as any data classes or data elements that were changed through the USCDI update processes when comparing USCDI v3 to USCDI v1 (88 FR 23764). For the overall structure and organization of the USCDI standard, including USCDI v3, we urged the public to consult *www.healthIT.gov/uscdi*. We proposed that each of the data classes or data elements listed below be included in the USCDI standard in § 170.213 and be incorporated by reference in § 170.299 as part of our proposal to adopt USCDI v3.

i. Social Determinants of Health (SDOH)

SDOH [39] are the conditions in which people live, learn, work, and play, and these conditions affect a wide range of health and quality-of-life risks and outcomes.[40] In the HTI–1 Proposed Rule, we stated that USCDI v3 includes four SDOH data elements that represent aspects of SDOH data related to the use or purpose of the SDOH data rather than being based on the domain (88 FR 23764). These data elements are SDOH Assessment in the Assessment and Plan of Treatment data class, SDOH Goals in the Goals data class, SDOH Interventions in the Procedures data class, and SDOH Problems/Health Concerns in the Problems data class.

Comments. A number of commenters expressed general support for inclusion of SDOH-related data elements in USCDI v3, often noting that the access, exchange, and use of these elements by Health IT Modules certified to particular certification criteria would support the availability of more information and better care for patients, as well as more equitable public health interventions.

Response. We thank commenters for the comments expressing support for the inclusion of SDOH-related data elements in USCDI v3 and for recognizing the benefits.

Comments. Several commenters did not support the inclusion of data elements related to SDOH at this time, stating that the proposed data elements fail to capture a comprehensive view of all SDOH and that there is a lack of standards related to these data elements. Commenters also suggested that SDOH-related data elements only be required as part of USCDI v3 once FHIR-based APIs and implementation guides are available.

Response. We thank commenters for their comments voicing concern that SDOH data elements as written in USCDI v3 are not comprehensive enough, lack standards, and should only be required once FHIR-based APIs and implementation guides are available. We note that there are available and applicable standards. Specifically, FHIR US Core 6.1.0 and C–CDA Companion Guide R4.1 support USCDI v3 and align with the SDOH data elements in USCDI v3. We note that both FHIR US Core 6.1.0 and C–CDA Companion Guide R4.1 are incremental updates which address errors and misalignments in their respective prior versions. FHIR US Core 6.1.0 and C–CDA Companion Guide R4.1 have not added any substantial functionality or requirements. We do not believe adoption of FHIR US Core 6.1.0 and C–CDA Companion Guide R4.1 would contribute to a greater implementation burden, and FHIR US Core 6.1.0 and C–CDA Companion Guide R4.1 are the only versions of their respective implementation guides that fully align with and support the complete USCDI v3.

As mentioned earlier, we recognize that we proposed different versions of the US Core and C–CDA Companion Guide specifications but stated that we would consider newer versions that align with USCDI v3 (FHIR US Core 6.0.0 and C–CDA Companion Guide R4). However, after the publishing of FHIR US Core 6.0.0 and C–CDA Companion Guide R4, HL7 found errors with how

[39] See SDOH Toolkit for more information, *https://www.healthit.gov/sites/default/files/2023-02/Social%20Determinants%20of%20Health%20Information%20Exchange%20Toolkit%202023_508.pdf*.

[40] *https://www.healthit.gov/topic/health-it-health-care-settings/social-determinants-health*.

the guides implemented data elements in USCDI v3 and had to make updates to those specifications to align with USCDI v3 and ensure that USCDI v3 can be implemented in Health IT Modules. Adopting FHIR US Core 6.1.0 and C–CDA Companion Guide R4.1 is necessary for developers of certified health IT to have appropriate implementation guidance to meet the criteria adopted in this final rule that reference USCDI v3. Based on public comments on this and prior rulemakings, we believe that the health IT industry, healthcare standards developers, and health care providers expect and support ONC making such determinations so that the adopted version of standards are the most up-to-date available and are feasible for real world implementation (see, for example, 85 FR 25677 and 25708).

In addition, the HL7 Gravity Project's Social Determinants of Health Clinical Care Release 2.0.0 Implementation Guide was published in October 2022.[41] While the Gravity Project's Social Determinants of Health Clinical Care Implementation Guide does not encompass all possible SDOH aspects, it does define exchange standards for multiple key domains.

Comments. Commenters also urged that SDOH data be protected to ensure the privacy and security of the information, with some commenters urging ONC to adopt granular data segmentation requirements along with USCDI v3.

Response. We thank commenters for noting their concerns regarding SDOH data, specifically the importance of addressing the privacy and confidentiality of sensitive information. The adoption of USCDI v3 sets a new baseline for the capability of Health IT Modules certified to specific certification criteria to capture and exchange data but does not dictate when and how either of those two actions occur. We did not propose and are not adopting privacy protections or standards related to controlling sensitive data that may be represented in USCDI data elements, including granular data segmentation requirements. However, we have adopted a new technical requirement as part of the certification criterion in § 170.315(e)(1) in support of the development and use of technology to enable the HIPAA Privacy Rule's individuals' ''right to request a restriction'' as discussed in section III.C.10. For more on patient requested restrictions on sharing of their health information, we refer readers to section III.C.10 on modifications to the ''view, download, and transmit to 3rd party'' certification criterion in § 170.315(e)(1) stating that patients (and their authorized representatives) must be able to use an internet-based method to request a restriction to be applied for any data expressed in the standards in § 170.213. As noted in the HTI–1 Proposed Rule (88 FR 23765), in the 2015 Edition, ONC adopted a certification criterion to enable users of Health IT Modules(s) certified to that criterion with the functionality to electronically capture, modify, and access SDOH data elements—that is information that identifies common SDOH conditions in a standardized manner—in § 170.315(a)(15) social, psychological, and behavioral data (80 FR 62631). These functionalities are intended to support users with the ability to use technology to comply with applicable existing legal requirements or organizational policies that may require such data collection and broader, existing industry interests and efforts to collect and use this data to inform clinical decision-making and improve patient care by looking at the whole patient, including leveraging other types of care such as home and community-based services. ONC supports the use of technology to improve the standardized capture of a set of health data elements to support the healthcare industry's need to electronically capture the underlying data they need or want to collect for healthcare. ONC will continue working with our federal partners in their efforts to educate interested parties, including both health care providers and patients,[42] regarding the access, exchange, and use of information about patients and the use of certified health IT.

Comments. One commenter suggested that a base set of SDOH criteria for each of the SDOH elements be required, while optional criteria could be added based on the hospital or provider's specific situation.

Response. We thank the commenter for their suggestion. USCDI v3 includes data elements for SDOH Problems/Health Concerns, SDOH Assessment, SDOH Goals, and SDOH Interventions. For the purposes of the Program, developers with Health IT Modules certified to specific certification criteria must support all USCDI v3 data elements, including the SDOH data elements for Problems/Health Concerns, Assessment, Goals, and Interventions. Under these required data elements, those health IT developers may support any of the SDOH domains such as referrals, food insecurity, transportation, and housing security. The USCDI standard is intended to provide a common set of data classes and data elements to support nationwide health information exchange and interoperability, and partial adoption of the USCDI standard would impair its effectiveness in doing so.

Comments. Commenters had a variety of recommendations related to including SDOH data elements in USCDI v3. Several comments suggested that ONC partner with standards organizations and others in the industry in developing and implementing SDOH data elements. Commenters also suggested that when developing SDOH data elements, ONC should seek input from patients and advocates representing those with health disparities. Commenters also suggested that ONC work with CMS and state Medicaid agencies on capturing and sharing SDOH data. One commenter suggested aligning SDOH data collection across federal and state healthcare program reporting requirements.

Response. We thank commenters for the recommendations related to including SDOH data elements in USCDI v3. We work closely with the HL7 FHIR Gravity Accelerator to develop and implement SDOH data elements. We also support the HL7 Gravity Pilots Affinity Group and support testing through connectathons and pilots. Throughout the spring of 2023, we engaged interested parties and the community in the ONC SDOH Information Exchange Learning Forum, resulting in the creation of an ONC SDOH Information Exchange Toolkit.[43] In 2021, we funded a Leading Edge Acceleration Project for Referral Management to Address SDOH Aligned with Clinical Care.

The HL7 FHIR Gravity Accelerator participants include individuals, patients, advocates, representatives from payer organizations, social services organizations, health IT developers, provider associations, and other government participants, including CMS.

Comments. Several commenters suggested that ONC provide support to providers and their staff to implement SDOH data elements and ensure SDOH data is collected, used, and shared appropriately. Commenters suggested that education and training on SDOH

[41] *http://hl7.org/fhir/us/sdoh-clinicalcare/STU2/.*

[42] See *e.g., https://www.healthit.gov/topic/patient-access-health-records/patient-access-health-records.*

[43] *https://www.healthit.gov/sites/default/files/2023-02/Social%20Determinants%20of%20Health%20Information%20Exchange%20Toolkit%202023_508.pdf.*

data elements, including definitions and use cases, is needed for the industry, and several commenters suggested that ONC develop standards, value sets, and mappings related to SDOH data elements.

Response. We thank commenters for the input regarding the need for support and resources. To support the adoption and implementation of SDOH data elements, ONC published the SDOH Information Exchange Toolkit to further support communities working toward achieving health equity through SDOH information exchange and the use of interoperable, standardized data. The Toolkit is intended to provide information on the exchange of SDOH information to interested parties of all experience levels, as well as identify approaches to advance SDOH information exchange goals. The audience for the Toolkit includes states, payers, health care provider networks, human services providers, and community-based services entities.

Comments. One commenter sought clarification regarding the Medicare Promoting Interoperability Program requirements and the SDOH Problems/Health data element and whether there is a need for an option to indicate ''None.''

Response. We thank commenters for the feedback seeking clarification regarding the Medicare Promoting Interoperability Program requirements for the SDOH Problems/Health data element. ONC refers the commenter to CMS for their program requirements.

ii. Care Team Member

In USCDI v1, the Care Team Member data class had one data element to capture all aspects about a care team member. USCDI v3 includes five Care Team Member data elements: Name, Identifier, Role, Location, and Telecom.

Comments. Several commenters specifically supported the inclusion in USCDI v3 of the Care Team Member Name and Identifier data elements. However, several commenters had concerns about the Care Team Member data elements. These commenters suggested removal of the Care Team Member Name and Identifier data elements to protect providers or, alternatively, to let providers opt out of having their information included and noted that providers may be at risk of personal harm if their identity is known. Other commenters noted that without standards, organizations will implement the data elements differently. One commenter recommended that a value set and coding be provided for the Care Team Member Role data element.

Response. We thank commenters for the comments regarding Care Team Member Name, Role and Identifier data elements. We work with the HL7 community to develop vocabulary applicable to USCDI data elements to ensure standard implementation of these data elements. In addition, we note that the USCDI v3 is a standard as a whole and has been adopted in whole, as proposed. As conveyed elsewhere in our responses, the adoption of USCDI v3 sets a new baseline for the capability of Health IT Modules certified to particular certification criteria to capture and exchange such data but does not dictate when and how either of those two actions occur. Specifically, in the Program, we establish requirements for Health IT Modules to enable a user to capture or exchange data. We do not establish requirements in the Program for an entity to use a certified Health IT Module or for the user of a Health IT Module to capture or record specific data.

iii. Clinical Notes

For the data element Discharge Summary Note in the Clinical Notes data class, we specified additional requirements in USCDI v3 including admission and discharge dates and locations, discharge instructions, and reason(s) for hospitalization, which are also required elements in the ''transitions of care'' certification criterion (§ 170.315(b)(1)).

Comments. We received several comments supporting the Clinical Notes data class and data elements, including Discharge Summary Note. One commenter noted that standardizing the presentation of this information will improve consistency and reliability. Another commenter focused on the specified Logical Observation Identifiers Names and Codes (LOINC®) codes and recommended linking them to International Classification of Diseases, Tenth Revision, Clinical Modification (ICD–10–CM) –Z codes and/or SNOMED–CT, which represent concepts rather than specific questions and answers, and recommended considering one-to-many bindings. One commenter sought clarification regarding whether ONC certification would require support for both structured and unstructured narrative findings.

Response. We thank commenters for the comments on the Clinical Notes data class and data elements regarding standardization. Health IT developers certifying Health IT Modules to certification criteria that reference USCDI v3 must align with the applicable vocabulary standards as defined in USCDI v3 and with the requirements in the C–CDA Companion Guide R4.1 and FHIR US Core 6.1.0 that list concept codes from the LOINC Document Ontology to identify the note type. Many certification criteria reference the USCDI standard, which comprises either structured or unstructured narrative notes.

iv. Clinical Tests

USCDI v3 includes a data class for Clinical Tests, which has two data elements, Clinical Test and Clinical Test Result/Report. This is a new data class as compared to USCDI v1.

Comments. We received several comments expressing concerns regarding the Clinical Tests data class and data elements. One commenter expressed concerns about the Clinical Tests Results/Report data element, stressing that human interpretation is needed and that it could be dangerous to send test results without ''normal'' or ''abnormal'' indicators, or a reference range. One commenter sought clarification regarding whether ONC will require support for both structured and unstructured narrative findings. One commenter noted that the availability of clinical tests in EHR systems varies substantially.

Response. We appreciate the comments regarding concerns about how the Clinical Tests data elements are implemented. The two data elements represent the minimum information necessary to convey patient data for non-laboratory and non-diagnostic imaging tests, such as electrocardiograms and visual acuity. We agree with the commenter that supplemental data such as ''normal,'' ''abnormal,'' or reference ranges provide valuable information. However, the USCDI v3 is a published standard at *www.healthit.gov/uscdi* and thus it is not possible to add new data elements to USCDI v3 through the rulemaking process or other means at this time. We direct commenters to the USCDI website available at *https://www.healthit.gov/uscdi* where the public is invited to enter comments on leveled data elements or submit new data elements for consideration in future version of USCDI. Health IT developers are encouraged to work with their customers to exchange data that adds value. The Clinical Test data element must be represented with a LOINC® code to indicate the specific test performed or planned. The Clinical Test Result/Report data element may be structured and represented using a code set such as SNOMED CT U.S. Edition, or unstructured and represented with free text. The Program does not require

the use of standardized vocabularies for Clinical Test Result/Report.

ONC acknowledges that clinical test availability varies within and across EHR systems. However, Health IT Modules certified to criteria that reference the USCDI standards in § 170.213 must have the capability to exchange clinical test data.

v. Diagnostics Imaging

USCDI v3 includes the Diagnostic Imaging data class and its two elements: Diagnostic Imaging Test and Diagnostic Imaging Report. This is a new data class as compared to USCDI v1.

Comments. We received comments on the Diagnostic Imaging data class noting that many specialty health IT systems may not integrate with or support imaging services, and a requirement to support this data class could be infeasible for some systems or result in unused capabilities.

Response. We thank commenters for their input. We understand that many specialty health IT systems do not integrate with or support imaging services. The data elements in the Diagnostic Imaging data class are not specific to the actual images that may be housed or supported in an image storing system, but rather are based on types of diagnostic imaging referenced by LOINC® codes and the interpreted imaging test results in a report. USCDI is not specific to a setting of care, a healthcare specialty, or a specific category of health IT user; the standard provides a common set of data classes and data elements that can be used for nationwide, interoperable health information exchange. To ensure interoperability for the core set of data in the USCDI, it is important for developers of certified health IT to support the complete USCDI where required for health IT certification criteria in the Program. To the extent that such specialty health IT systems are not certified to certification criteria that reference § 170.213, then they would not have to support this data class.

vi. Encounter Information

USCDI v3 includes the Encounter Information data class, which includes five data elements: Encounter Type, Encounter Diagnosis, Encounter Time, Encounter Location, and Encounter Disposition. This is a new data class as compared to USCDI v1.

Comments. One commenter expressed specific agreement and support of the Encounter Information data class. Several comments expressed concerns, including regarding a lack of standards. One commenter recommended only adopting the Encounter Diagnosis data element since it does have a standard. One commenter expressed concern that Encounter Information would identify information about pregnancy termination services that could be misused and lead to administrative or criminal investigations of patients and providers. Another commenter sought confirmation regarding whether inpatient encounters need to be included and suggested that they be included in a final rule.

Response. We have reviewed the comments regarding the Encounter Information data class and concerns around the lack of standards. The USCDI v3 data classes and data elements apply to inpatients and outpatients and define applicable vocabulary standards where appropriate. The Encounter Diagnosis data element references the SNOMED CT U.S. Edition and ICD–10–CM vocabulary standards. Regarding comments on privacy and security of Encounter Information and related services, we note the adoption of USCDI v3 sets a new baseline for the capability of Health IT Modules certified to particular certification criteria to capture and exchange data but does not dictate when and how either of those two actions occur.

vii. Health Insurance Information

USCDI v3 includes the Health Insurance Information data class, which provides an opportunity for health IT to capture and exchange key elements of healthcare insurance coverage. This is a new data class as compared to USCDI v1. This data class includes seven data elements: Coverage Status, Coverage Type, Relationship to Subscriber, Member Identifier, Subscriber Identifier, Group Identifier, and Payer Identifier.

Comments. A number of commenters expressed support for the Health Insurance Information data class. Comments included that it would be vital for emergency medical services (EMS) providers to receive reimbursement and that it will open opportunities for patients and providers to use beneficial apps, such as those related to cost barriers and administrative transactions.

Response. We thank commenters for their support of the Health Insurance Information data class and for recognizing the potential benefits.

Comments. A number of commenters expressed concern or did not support the Health Insurance Information data class. Several commenters stated that the data elements needed more standardization before they should be required, and that it was unreasonable to include this data class because there are no related standards yet. One commenter stated that the Health Insurance Information data class is problematic because there is no guidance about how to align this proposed standard with the proposed US Core IG v5.0.1 that payers would be required to adopt via the Interoperability and Prior Authorization Proposed Rule (87 FR 76238). The commenter stated that ONC's proposal does not align with the changes proposed in the Interoperability and Prior Authorization Proposed Rule. Commenters also stated that prior authorization standards were needed for payers to see value in this data class. Additionally, commenters expressed concern that most health IT systems seeking certification would need to rely on third-party systems to support documentation and storage of health insurance data. Commenters also stated that ONC should not add data elements to the USCDI that duplicate processes housed in practice management systems. Several commenters stated that USCDI v3 should not be required until the Health Insurance Information data class is revised, or that USCDI v3 should be adopted without the Health Insurance Information data class included. Commenters also stated that the Health Insurance Information data class should not have to be shared until CMS clarifies which data elements do not have to be shared through the Payer-to-Payer API to avoid the exchange of competitively sensitive information.

Response. We have considered the comments expressing concern about the Health Insurance Information data class. We do not agree that there are no related standards for these data elements, as HL7 FHIR US Core and the C–CDA Companion Guide support the Health Insurance Information data elements and include references to standard vocabulary where available and in use. Regarding alignment with requirements proposed by CMS in the Interoperability and Prior Authorization Proposed Rule, we refer readers to CMS' proposals in the Interoperability and Prior Authorization Proposed Rule to allow payers to use updated versions of standards in § 170.215, subject to certain conditions including approval for use by the National Coordinator (87 FR 76315). We also note that in the Interoperability and Prior Authorization Proposed Rule, CMS has proposed to allow flexibility for use of a version of the USCDI standard in § 170.213 (87 FR 76250) where proposed payer API requirements reference the USCDI, which will include USCDI v3 under our finalized policy. We further disagree

with the concerns reflected in the comments about the burden that would be associated with sharing this data and believe these comments may not accurately reflect what is expected from the USCDI v3 data elements. The data elements in this data class are to exchange information about whether a patient has insurance coverage, and the type of coverage. Also included are elements that provide information about the plan. The Health Insurance Information data elements do not include any claims specific information. Additionally, we recognize that this information may or may not originate in an EHR, however Health IT Modules certified to certification criteria that reference § 170.213 must be able to capture and exchange the values when available.

Regarding the comment about this data only being valuable with respect to prior authorization standards, we note that such standards may be adopted in the future and believe that this information can provide substantial value at present by supporting the availability of data about coverage that is important for health care providers to understand a patient's situation. We recently sought comment through an RFI titled ''Electronic Prior Authorization Standards, Implementation Specifications, and Certification Criteria'' (87 FR 3475), which appeared in the January 24, 2022 issue of the **Federal Register**, on how updates to the Program could support electronic prior authorization. We have reviewed comments, and this information may be used to inform a future rulemaking related to the ONC Health IT Certification Program and electronic prior authorization. We will continue to work with CMS to ensure alignment with our rules.

Comments. Several commenters also expressed privacy concerns regarding the Health Insurance Information data class. Commenters suggested that ONC revise the data class to protect patient privacy and that ONC should remove data elements that provide personally identifiable information not supportive of patient care, such as ''group identifier.'' Commenters also expressed concern about the inclusion of financial data in the USCDI, the sharing of claim-level payment information and the disclosure of confidentially negotiated rates.

Response. As we have noted in similarly themed comments, the adoption of USCDI v3 sets a new baseline for the capability of Health IT Modules certified to particular certification criteria to capture and exchange data but does not dictate when and how either of those two actions occur. Further, the concerns expressed related to financial data including claim-level payment and negotiated rates are not within scope of the HTI–1 Proposed Rule because USCDI v3 does not include any financial, claim level, or negotiated rate data elements.

Comments. Commenters suggested that the data class should focus on data elements related to whether a person has insurance coverage, the type of coverage, and which payers are covering the patient. Other commenters suggested that the data class should be revised to focus on sharing information that can be collected based on national standards. Commenters also stated that vendors use different health insurance payer identification numbers, making it challenging to match records, and that ONC should work with the industry to adopt a single source for payer identification. One commenter recommended including both medical insurance and prescription insurance as part of the data elements, and another comment recommended that ONC adopt the data elements included in the CARIN IG for Blue Button.

Response. We appreciate the additional suggestions. The data elements in the Health Insurance Information class are to exchange information about whether a patient has insurance coverage, and the type of coverage. Also included are elements that provide information about the plan.

The USCDI v3 is a published standard at *www.healthit.gov/uscdi* and thus it is not possible to add new data elements to USCDI v3 through the rulemaking process or other means at this time. We direct commenters to the USCDI website available at *www.healthit.gov/uscdi* where the public is invited to enter comments on leveled data elements or submit new data elements for consideration in future versions of USCDI.

Comments. Commenters sought clarification regarding the Coverage Status data element and if it should indicate whether and which type of health insurance a patient has, rather than if specific services are covered. One commenter sought clarification for why the value set for Coverage Type data element was not a required standard in USCDI v3. Commenters also sought clarification regarding whether health insurance includes both medical and prescription insurance.

Response. The Health Insurance data class is intended to capture data related to an individual's insurance coverage for healthcare including medical and prescription insurance. Coverage Status is defined in USCDI v3 as the presence or absence of healthcare insurance, whereas Coverage Type is designed to communicate the category of healthcare payer (*e.g.,* Medicare, Commercial, Managed Care—PPO). ONC refers implementers to the US Core and C–CDA implementation guides for guidance on specific value sets. For future versions of USCDI, we encourage interested parties to provide feedback for applicable vocabulary standards, for the Coverage Type and Coverage Status data elements during an open comment period at *https://www.healthit.gov/uscdi.*

viii. Health Status Assessments

USCDI v3 includes a data class called Health Status Assessments, which contains four new data elements: Disability Status, Mental/Cognitive Status, Functional Status, and Pregnancy Status. This is a new data class as compared to USCDI v1. In USCDI v3, the Health Status Assessments data class also includes two data elements that have been recategorized, Health Concerns and Smoking Status, which were previously part of different data classes in USCDI.

Comments. Several commenters expressed concerns about the Health Status Assessment data class. One commenter noted that Health Status Assessments often vary from provider to provider and that requiring these data elements from non-standardized forms by the proposed deadline is not possible. One commenter noted that it is not clear how the USCDI data elements apply to mental/behavioral health and substance use treatment data.

Response. We thank commenters and acknowledge that assessments often vary from provider to provider. The USCDI data elements in this data class reference applicable vocabulary standards, including LOINC and SNOMED CT U.S. Edition, to identify the assessment and related questions which may identify not only the assessment or survey instrument, but may also allow for understanding the semantics of the assessment data. The USCDI v3 includes a Mental/Cognitive Status data element to support the exchange of mental/behavioral health data. There are new data elements in USCDI v4 that capture Alcohol Use and Substance Use assessments. We clarify that USCDI v4 is not being adopted as a standard in this final rule. Additionally, USCDI v4 is not available through SVAP at this time. Generally, approved SVAP versions of standards are announced in June each year and

become effective for Program use after a 60-day period.[44]

Comments. The majority of the comments on the Health Status Assessment data class were related to the Pregnancy Status data element. One commenter expressed support for including Pregnancy Status as a data element, but most comments expressed concerns about Pregnancy Status, including regarding legal implications for providers and that sharing this information in patients' records without their express consent could create real dangers. Some commenters recommended reconsidering this data element given the increased criminalization of reproductive health and pregnancy-related care. Commenters suggested delaying the inclusion of this data element until patient requested restrictions could be fully operationalized. Commenters also noted a lack of standards around this data element and stated that without standards, incompatible data could be entered for Pregnancy Status, and recommended against including it as a data element until there is a defined standard. One commenter recommended also including Pregnancy Intention Screening as a data element.

Response. We appreciate the comments regarding privacy concerns expressed above. The adoption of USCDI v3 sets a new baseline for the capability of Health IT Modules certified to particular certification criteria to capture and exchange data but does not dictate when and how either of those two actions occur. For more on patient requested restrictions on sharing of their health information, we refer readers to section III.C.10 on modifications to the ''view, download, and transmit to 3rd party'' certification criterion in § 170.315(e)(1), stating patients (and their authorized representatives) must be able to use an internet-based method to request a restriction to be applied for any data expressed in the standards in § 170.213.

The USCDI v3 is a published standard at *www.healthit.gov/uscdi* and thus it is not possible to add new data elements to USCDI v3 through the rulemaking process or other means at this time. We direct commenters to the USCDI website available at *www.healthit.gov/uscdi* where the public is invited to enter comments on leveled data elements or submit new data elements for consideration in future versions of USCDI. Commenters are directed to the FHIR US Core 6.1.0 and C–CDA Companion Guide R4.1 for guidance on how to implement the Pregnancy Status data element.

ix. Laboratory

USCDI v3 includes Specimen Type and Result Status data elements, which have been added to the USCDI Laboratory data class to address public health reporting priorities.

We did not receive comments to specifically respond to with clarifications.

x. Medications

USCDI v3 includes Dose, Dose Unit of Measure, Indication, and Fill Status data elements, which have been added to the Medications data class in response to public feedback. These data elements are necessary for certain CMS reporting programs and are also critical to certain ONC certification criteria (including the ''electronic prescribing certification'' criterion at § 170.315(b)(3)).

Comments. Several comments expressed concern about the lack of standards for data elements in the Medications data class, including Medications, Indication, and Fill Status. One comment noted that Fill Status data is generally maintained by pharmacy systems and many systems seeking certification would not natively support documentation and storage of this information. One comment stated that USCDI v3 is not clear regarding what must be included for the Medications data element and that more specificity could improve patient care and safety.

Response. The Medications data element includes both RxNorm and NDC as applicable vocabulary standards in USCDI v3. The HL7 FHIR US Core Implementation Guide and C–CDA Companion Guide for USCDI v3 have defined terminology bindings for Indication to include value sets drawn from both SNOMED CT U.S. Edition and ICD–10–CM. Regarding the utility of including Fill Status in the USCDI v3, we recognize that this information may or may not originate in an EHR, however certified health IT with Health IT Modules certified to particular certification criteria that reference § 170.213 must be able to capture and exchange the value when it is available.

xi. Patient Demographics/Information

Based on submissions and comments during the USCDI update processes described above, we changed or added data elements in the Patient Demographics/Information data class. USCDI v3 includes data elements Sexual Orientation and Gender Identity, which have been added to the USCDI Patient Demographics/Information data class. As described in the HTI–1 Proposed Rule, we previously adopted standards for Sexual Orientation in the demographics criterion in § 170.315(a)(5)(i)(D) and for Gender Identity in the demographics criterion in § 170.315(a)(5)(i)(E) that included requirements to code Sexual Orientation and Gender Identity according to the adopted SNOMED CT® U.S. Edition codes and HL7 Version 3 Standard, Value Sets for AdministrativeGender and NullFlavor, as referenced § 170.207(o)(1) and § 170.207(o)(2), respectively (88 FR 23766). We proposed to remove the requirement to use specific codes for representing Sexual Orientation and Gender Identity and have removed the codes as applicable vocabulary standards from USCDI v3. We proposed that certified health IT with Health IT Modules certified to particular certification criteria that reference § 170.213 would be required to be capable of representing Sexual Orientation and Gender Identity in SNOMED CT® U.S. Edition when such information is exchanged as part of USCDI. We stated in the HTI–1 Proposed Rule that we believe it is best to let the health IT community develop the list of appropriate values for Sexual Orientation and Gender Identity, whether through implementation specifications or developing additional codes in SNOMED CT® U.S. Edition (88 FR 23766).

As described in the HTI–1 Proposed Rule, we have recharacterized the USCDI data element Sex (Assigned at Birth) to Sex (88 FR 23766). We proposed to remove the requirement in § 170.315(a)(5)(i)(C) and § 170.315(b)(1)(iii)(G)(*3*) to code Sex according to the adopted value sets of HL7 Version 3 Value Sets for AdministrativeGender and NullFlavor as referenced in the value sets in § 170.207(n)(1). We proposed instead to permit coding according to either the adopted value sets of HL7 Version 3 Value Sets for AdministrativeGender and NullFlavor as referenced in the value sets in § 170.207(n)(1) until December 31, 2025, or in accordance with the standard in proposed § 170.207(n)(2). We also proposed to no longer require the use of specific code sets for representing Sex and have removed the codes from USCDI v3. We proposed that certified health IT with Health IT Modules certified to certification criteria that reference § 170.213 would be required to be capable of representing Sex in SNOMED CT when such information is exchanged as part of USCDI. We proposed to adopt the same changes for relevant certification criteria that reference these

[44] *https://www.healthit.gov/sites/default/files/2023-07/2023_SVAP_Fact_Sheet.pdf.*

standards (see sections III.C.8 and III.C.9).

In the HTI–1 Proposed Rule, we noted efforts to develop a clinically meaningful way for identifying a patient's sex from observable information that may be suitable for clinical care, including the development of a new data element Sex for Clinical Use, and sought public comment on this concept and approach (88 FR 23766). In addition, as noted in our proposals to the ''patient demographics and observations'' certification criterion in § 170.315(a)(5), we proposed to adopt the same changes for relevant certification criteria that reference these standards (see sections III.C.8 and III.C.9).

As discussed in the HTI–1 Proposed Rule, a new standard for patient addresses, the Unified Specification for Address in Health Care (US@),[45] emerged and was released in 2022 (88 FR 23767). After receiving broad support from the public, ONC has incorporated the Project US@ Technical Specification version 1 as the applicable standard for Current Address and Previous Address in USCDI v3.

Also as discussed in the HTI–1 Proposed Rule, USCDI v3 includes six data elements added to the USCDI Patient Demographics/Information data class: Related Person's Name, Related Person's Relationship, Date of Death, Occupation, Occupation Industry, and Tribal Affiliation.

Comments. Several commenters explicitly expressed support for the Patient Demographics/Information data class, noting that this will improve healthcare quality, enhance communication, bolster cultural competency, and support the ability of providers to gather and exchange the information needed to make the best care plans for their patients.

Response. We thank commenters for their support of the Patient Demographics/Information data class and for noting the potential benefits.

Comments. Some commenters had concerns about the Patient Demographics/Information data class, including that it was not reasonable to require the full data class. Additionally, comments included recommendations for ONC with respect to the Patient Demographics/Information data class. Comments recommended aligning deadlines with the availability of FHIR-based APIs to ensure consistency across interested parties and aligning the USCDI Patient Demographics/Information data class with CMS definitions of the included data elements.

Response. We receive submissions and comments from federal partners, including CMS, on the USCDI and will continue to work towards alignment where appropriate with these partners. With respect to the suggestions regarding flexibility in supporting USCDI v3 data classes and data elements for purposes of the Program, we decline to allow developers to be selective in which USCDI v3 data classes and data elements they support for purposes of the Program. Because the USCDI standard is intended to provide a common set of data classes and data elements in support of nationwide health information exchange, partial adoption of the USCDI standard would impact the effectiveness of the standard and impede interoperability.

Comments. Specific comments about data elements stated that standards should be included to restrict date formats for Date of Birth and Date of Death data elements, and that Previous Name and Tribal Affiliation data elements should not be included in USCDI v3 until there are standards for them. One commenter asked for clarification on whether detailed race standards or free text fields should be used for Tribal Affiliation.

Response. We thank commenters for the feedback on the lack of standards for the Date of Birth and Date of Death data elements. We direct commenters to the HL7 FHIR US Core Implementation Guide and the C–CDA Companion Guide when an applicable standard is not identified in USCDI. In addition, these implementation guides provide guidance for exchanging Previous Name and Tribal Affiliation, the latter of which includes a vocabulary binding to a harmonized value set.

Comments. A number of commenters addressed the Sexual Orientation and Gender Identity (SOGI) and Sex data elements. Many of those commenters expressed support for including SOGI data elements, for removal of the requirement to use specific codes for representing SOGI, and for updating SOGI codes with SNOMED CT. Some of these commenters noted that this would reduce burden and would facilitate identifying disparities and improving outcomes for the LGBTQ+ population.

Response. We thank commenters for the feedback in support of the Sexual Orientation, Gender Identity, and Sex data elements and related requirements and standards, and for recognizing the potential benefits.

Comments. Several commenters expressed concerns related to the SOGI data elements, including that best practices around SOGI data are not well established and that there could be unintended confusion around the terms. Commenters also stressed the need for standardized codes related to SOGI, the importance of industry collaboration, and the value of education on SOGI data elements and use cases. One commenter noted that patients are historically reluctant to answer questions on sexual identity and this may lead to lower accuracy. One commenter stated that the health IT industry will not coalesce around value sets for Sex, Sexual Orientation and Gender Identity data elements and urged ONC to create them. Commenters also noted that several existing definitions within the proposed standards for SOGI expire on December 31, 2025, and recommended aligning deadlines.

Response. We appreciate the detailed comments. We defined SNOMED CT, U.S. Edition as the vocabulary standard for Sex, Sexual Orientation, and Gender Identity in USCDI v3. We collaborated with HL7, and the HL7 Gender Harmony Project team to update the US Core Implementation Guide and C–CDA Companion Guide with references to value sets with specific SNOMED CT U.S. Edition concepts. We work closely with federal partners to promote quality data capture and storage practices using standard terminology. We encourage providers to work with their patients to understand how and when this data is valuable for patient care and to address the situation where a patient may be reluctant to share information.

Comments. One commenter stated that changing Sex (assigned at birth) to Sex would lead to inconsistency and that it would be preferable to define a series of specific data elements with clear definitions related to this data class. One commenter sought clarification that under USCDI v3 developers should continue exchanging the same data from their systems that is currently being exchanged as the Sex (assigned at birth) data element to comply with requirements for the Sex data element.

Response. We thank commenters for the input regarding the Sex data element in USCDI v3 and concerns regarding the update from Sex (Assigned at Birth) in USCDI v2 to Sex in USCDI v3. We, along with the HL7 community recognized that Sex (Assigned at Birth) has been used to represent different concepts not always associated with the value assigned at time of birth such as clinically relevant sex for laboratory tests or diagnostic imaging, and administrative sex recorded on birth certificates and health forms. The values

[45] *https://oncprojectracking.healthit.gov/wiki/pages/viewpage.action?pageId=180486153.*

used for each instance may not be the same for a given patient. Furthermore, the value set referenced in earlier versions of USCDI for Sex (Assigned at Birth) does not include all possible values that represent sex. We therefore removed the reference to the limited value set previously used and expanded the applicable vocabulary standard to the SNOMED CT U.S. Edition code set. ONC worked closely with HL7 Structured Documents and US Core teams to update the US Core Implementation Guide and the C–CDA Companion Guide to distinguish between Sex (Assigned at Birth) and Sex as separate data elements. It is ONC's intent that developers continue exchanging the same data from their systems that is currently being exchanged as Sex (Assigned at Birth) and additionally exchange the USCDI v3 Sex data element.

Comments. In the HTI–1 Proposed Rule, we stated that we welcomed public comment on the development and inclusion in future standards of a new data element Sex for Clinical Use (88 FR 23766). We received several comments in support of including a Sex for Clinical Use data element in future versions of USCDI, generally because of the perceived benefits. One commenter opposed inclusion of Sex for Clinical Use as a data element in USCDI without further consultation with transgender and intersex communities. However, most of the comments about Sex for Clinical Use related to proposals regarding the Sex for Clinical Use data element in the ''patient demographics and observations'' criterion.

Response. We thank commenters for these suggestions. Sex for Clinical Use may be considered for inclusion as a data element in a future version of USCDI. We received comments related to Sex for Clinical Use as it relates to the ''patient demographics and observations'' certification criterion, and we discuss those comments in section III.C.8 of this final rule concerning the ''patient demographics and observations'' certification criterion in § 170.315(a)(5).

Comments. There were several comments related to the Race and Ethnicity data elements. Commenters expressed concerns about upgrading to the 2022 version of the Centers for Disease Control and Prevention (CDC) Race and Ethnicity code sets because this would add burden to the industry and recommended only adding codes and not changing existing ones. Commenters requested clarification on why this change was needed and the benefits. Commenters also noted that ONC should follow efforts by the Office of Management and Budget (OMB) regarding adoption of new race and ethnicity data standards.

Response. We thank commenters for the input regarding the Race and Ethnicity data elements. We did not propose updating to the 2022 version of the Centers for Disease Control and Prevention (CDC) Race and Ethnicity code set at this time as the 2022 version of CDC Race and Ethnicity code set has not been released. We assure commenters that we follow efforts by OMB regarding adoption of new race and ethnicity standards.

Comments. Several commenters asked for additional guidance, including on how data for the Patient Demographics/Information data class is collected and used, and on terminology related to SOGI. One commenter requested that ONC clarify how interested parties should address conflicting information among SOGI data elements due to disparities in elements and collection. One comment stated that ONC should encourage healthcare organizations to offer the term ''nonbinary'' as a Gender Identity data element field.

Response. We thank commenters for the feedback. We do not dictate when and how capture and exchange of USCDI data elements occur, nor how conflicting information may be reconciled. We also do not require specific concepts, such as ''nonbinary,'' from the applicable vocabulary standard, SNOMED CT U.S. Edition for Gender Identity, and instead defer to the HL7 FHIR US Core Implementation Guide, HL7 v2 and C–CDA Companion Guide to declare value sets appropriate for use.

xii. Problems

As discussed in sub-section i of this section, USCDI v3 includes the SDOH Problems/Health Concerns data element added to the prior USCDI Problems data class. In addition, USCDI v3 includes Date of Diagnosis and Date of Resolution data elements added to the prior USCDI Problems data class to include timing elements for recorded and maintained problem lists within electronic health records.

Comments. A couple of commenters noted a lack of standards for the Date of Diagnosis, Date of Resolution, and Problems data elements. Commenters stated that the lack of standards constricting date formats impacts interoperability, and that the Problems data element should be able to indicate a degree of importance.

Response. We thank commenters for the input regarding the lack of standards for Date of Diagnosis, Date of Resolution, and Problems data elements. While the USCDI v3 does not identify applicable vocabulary standards for the data elements, the HL7 FHIR US Core Implementation Guide and C–CDA Companion Guide define the allowable date formats.

Addressing the comment about indicating a degree of importance for a Problem, the USCDI v3 is a published standard at *www.healthit.gov/uscdi* and thus it is not possible to add new data elements to USCDI v3 through the rulemaking process or other means at this time. We direct commenters to the USCDI website available at *www.healthit.gov/uscdi* where the public is invited to enter comments on leveled data elements or submit new data elements for consideration in future versions of USCDI.

xiii. Procedures

USCDI v3 includes the Reason for Referral data element added to the prior USCDI Procedures data class. As discussed in sub-section i of this section, the USCDI v3 also includes the SDOH Interventions data element added to the prior USCDI Procedures data class.

Comments. One commenter on the Procedures data class recommended that USCDI v3 specify that CDT is the applicable standard for technology developed to record dental procedures.

Response. We thank the commenter for the comment and note that the Code on Dental Procedures and Nomenclature (CDT) is included in USCDI v3 as an applicable standard in the USCDI v3 Procedures data element in the Procedures Data Class and may be used when exchanging dental procedures.

xiv. Updated Versions of Vocabulary Standard Code Sets

In the 2015 Edition Final Rule, we established a policy for minimum standards code sets that update frequently throughout a calendar year at 80 FR 62612, and we have listed several standards as minimum standards code sets in 45 CFR part 170 subpart B. As with all adopted minimum standards code sets, health IT can be certified to newer versions of the adopted baseline version minimum standards code sets for purposes of certification, unless the Secretary specifically prohibits the use of a newer version (see § 170.555 and 77 FR 54268). In USCDI v3, we included the versions of the minimum standards code sets available when we published USCDI v3. We have adopted the minimum standards code sets we proposed in the HTI–1 Proposed Rule.

Comments. Commenters recommended that HL7, LOINC, SNOMED CT U.S. Edition, and RxNorm

vocabulary bindings be added to the USCDI criteria in the final rule.

Response. We thank commenters for the comments related to vocabulary and vocabulary bindings in USCDI. USCDI v3 includes required and optional applicable vocabulary standards with references to code sets for data elements where an encoded value is expected and where a code set has been identified and is in use. This general binding to a code system may be further refined in the HL7 implementation guides.

xv. Unique Device Identifier(s) for a Patient's Implantable Device(s)

Comments. Several commenters specifically supported Unique Device Identifier(s) for a Patient's Implantable Device(s) as a data class and data element in USCDI v3. One commenter encouraged ONC to include this data element in all information exchanges and to work with CMS to tie Unique Device Identifier codes to payment for devices.

Response. We thank commenters for the comments regarding Unique Device Identifier(s) for a Patient's Implantable Device(s). Regarding requests that ONC work with CMS on alignment, we assure commenters that we work closely with CMS across multiple programs and initiatives to align program requirements and deadlines and will continue to do so in the future.

xvi. Vital Signs

Comments. One commenter expressed concern that without dates and times, vital signs information is not meaningful and potentially dangerous.

Response. We thank commenters for the comments and understand the concern. The HL7 FHIR US Core Implementation Guide (both the prior and updated versions) adopted in § 170.215(b)(1) and incorporated by reference in § 170.299 and the HL7 C–CDA R2.1 base standard adopted in § 170.205(a)(4) and incorporated by reference in § 170.299 require dates and times when exchanging vital signs.

After consideration of all comments regarding the data classes and data elements in USCDI v3, we have finalized our adoption of USCDI v3 in § 170.213(b) as proposed. We have extended the date USCDI v1 expires as a standard for use in the Program to January 1, 2026.

2. C–CDA Companion Guide Updates

We proposed to adopt the HL7® CDA® R2 Implementation Guide: C–CDA Templates for Clinical Notes STU Companion Guide, Release 3—US Realm in § 170.205(a)(6) (''C–CDA Companion Guide R3''). The C–CDA Companion Guide R3 provides supplemental guidance and additional technical clarification for specifying data in the C–CDA Release 2.1 for USCDI v2. We stated that if the C–CDA Companion Guide Release 4 (C–CDA Companion Guide R4) is published before the date of publication of this final rule, it would be our intention to consider adopting the updated C–CDA Companion Guide R4 that provides guidance and clarifications for specifying data in USCDI v3 in § 170.205(a)(6), since we proposed to adopt USCDI v3 as the baseline (88 FR 23767).

As mentioned above, HL7® has been updating the C–CDA Companion Guide to accommodate the new data classes and data elements in each USCDI version. To allow developers to voluntarily update to USCDI v2, ONC included the C–CDA Companion Guide R3 in the SVAP Approved Standards List for 2022. ONC released the SVAP Approved Standards List for 2022 in June 2022. We stated in the HTI–1 Proposed Rule that we anticipated that the C–CDA Companion Guide R4 would support updates included in the proposed USCDI v3 and that the adoption of the C–CDA Companion Guide R4 would align with our goal to increase the use of consistently implemented standards among health IT developers and improve interoperability. We proposed to adopt the C–CDA Companion Guide R3 as a standard in § 170.205(a)(6) and incorporate it by reference in § 170.299. We stated that if the C–CDA Companion Guide R4 is available at the time of publication of this final rule, we would consider adopting the C–CDA Companion Guide R4 in § 170.205(a)(6), which would support the updates included in proposed USCDI v3 (88 FR 23767).

Consistent with our proposals in sections III.A and III.C.11, we proposed to revise § 170.205(a)(5) to add that the adoption of the standard in § 170.205(a)(5) expires on January 1, 2025. Developers of certified health IT with Health IT Modules certified to particular certification criteria that reference § 170.205(a)(5) would have to update those Health IT Modules to § 170.205(a)(6) and provide them to customers by January 1, 2025. We clarified that under this proposal, for the time period up to and including December 31, 2024, HL7 CDA® R2 Implementation Guide: C–CDA Templates for Clinical Notes R2.1 Companion Guide, Release 2 would remain applicable as the minimum version required in the Program.

Further, we proposed that Health IT Modules certified to the particular certification criteria below would need to update to the HL7 CDA® R2 IG: C–CDA Templates for Clinical Notes R2.1 Companion Guide, Release 3 in § 170.205(a)(6) by January 1, 2025:

- ''transitions of care'' (§ 170.315(b)(1)(iii)(A));
- ''clinical information reconciliation and incorporation'' (§ 170.315(b)(2)(i), (ii), and (iv));
- ''care plan'' (§ 170.315(b)(9)(ii));
- ''view, download, and transmit to 3rd party'' (§ 170.315(e)(1)(i)(A) and (B));
- ''consolidated CDA creation performance'' (§ 170.315(g)(6)(i)); and
- ''application access—all data request'' (§ 170.315(g)(9)(i)).

For the purposes of meeting that compliance date, we stated that we expected health IT developers to update their certified health IT without new mandatory testing and notify their ONC–ACB on the date at which they have reached compliance. Developers would also need to factor these updates into their next real world testing plan (88 FR 23767 through 23768).

Comments. The majority of commenters supported the adoption of the HL7 CDA® R2 IG: C–CDA Templates for Clinical Notes R2.1 Companion Guide, Release 3 as proposed in § 170.205(a)(6). Many of the comments also noted support for the adoption of C–CDA Companion Guide Release that aligns with USCDI v3 if published before the date of publication of this final rule. Comments supporting this proposal noted that incorporating newer versions of the C–CDA standard will improve interoperability of clinical data.

Response. We thank commenters for support of our proposals and for recognizing potential benefits expand interoperability for clinical information shared via structured clinical notes. We also appreciate commenters who recommended adoption of the most recent version of C–CDA Companion Guide. After the publication of C–CDA Companion Guide R4, HL7 found errors with how the guide implemented data elements in USCDI v3 and had to make updates to the specification to align with USCDI v3 and ensure that USCDI v3 can be implemented in certified Health IT Modules. We note that C–CDA Companion Guide R4.1 has not added any substantial functionality or requirements beyond C–CDA Companion Guide R4. Therefore, we do not believe adoption of C–CDA Companion Guide R4.1 would contribute to a greater implementation burden, and C–CDA Companion Guide R4.1 is the only version of the C–CDA

Companion Guide that fully aligns with and supports the complete USCDI v3. Given the support of the commenters to adopt the most recent version of the C–CDA Companion Guide that aligns with USCDI v3, we have finalized adoption of C–CDA Companion Guide R4.1, which was published in June 2023, in § 170.205(a)(6).

Adopting the C–CDA Companion Guide R4.1 is necessary for developers of certified health IT to have appropriate implementation guidance to meet the criteria adopted in this final rule that reference USCDI v3. Based on public comments on this and prior rulemakings, we believe that the health IT industry, healthcare standards developers, and health care providers expect and support ONC making such determinations so that the adopted version of standards are the most up-to-date available and are feasible for real world implementation (see, for example, 85 FR 25677 and 25708).

Comments. Some commenters expressed concern about the deadline for this proposal and requested to extend the implementation deadline. Some suggested deadline extensions included to 24 months post-effective date of this final rule and December 31, 2025.

Response. We thank commenters for expressing a desire for an extension on proposed deadlines. We have finalized a January 1, 2026 date for the expiration of the standard in § 170.205(a)(5). We believe that this deadline provides adequate time for developers and industry to support C–CDA Companion Guide R4.1, which we have finalized in § 170.205(a)(6).

Comments. A minority of commenters cautioned us about the real-world needs of physicians and patients and added complexities of implementing additional health IT standards. One commenter appreciated the flexibility and reduced burden of confirming conformance via a notification to their ONC–ACB and noted concern that certification to a new requirement may involve proof of conformance to ensure that there is clear and consistent understanding and application of requirements across developers of certified health IT.

Response. We thank commenters for the comments regarding the potential burden placed on providers and developers by our proposal. We do not believe that the burden on providers or developers for the adoption of a new version of the C–CDA Companion Guide is excessive. ONC has worked closely with the implementer community to help alleviate burden, and we are confident that the addition of USCDI v3 data elements will provide significant benefit.

3. ''Minimum Standards'' Code Sets Updates

We established a policy in the 2015 Edition Final Rule for minimum standards code sets that update frequently (80 FR 62612). In prior rulemaking, we discussed the benefits of adopting newer versions of minimum standards code sets, including the improved interoperability and implementation of health IT with minimal additional burden (77 FR 54170). When determining whether to propose newer versions of minimum standards code sets, we consider the impact on interoperability and whether a newer version would require substantive effort for developers of certified health IT to implement. If adopted, newer versions of minimum standards code sets would serve as the baseline for certification and developers of certified health IT would be able to use newer versions of these adopted standards on a voluntary basis. We reiterate that while minimum standard code sets update frequently, perhaps several times in a single year, these updates are confined to concepts within the code system, not substantive changes to the standards themselves. In the HTI–1 Proposed Rule, we proposed to adopt the following versions of the minimum standards code sets listed below (88 FR 23768 through 23769).

- § 170.207(a)—Problems

We proposed to remove and reserve § 170.207(a)(3), IHTSDO SNOMED CT® International Release July 2012 and US Extension to SNOMED CT® March 2012 Release. We proposed to revise § 170.207(a)(1), which is currently reserved, to reference SNOMED CT US Edition March 2022 and incorporate it by reference in § 170.299.

- § 170.207(c)—Laboratory tests

We proposed to remove and reserve § 170.207(c)(2), Logical Observation Identifiers Names and Codes (LOINC®) Database version 2.40. We proposed to revise § 170.207(c)(1), which is currently reserved, to reference LOINC Database version 2.72, February 16, 2022, and incorporate it by reference in § 170.299.

- § 170.207(d)—Medications

We proposed to revise § 170.207(d)(1), which is currently reserved, to reference RxNorm July 5, 2022, Full Monthly Release and incorporate it by reference in § 170.299. We proposed in § 170.207(d)(4) to reference the code set specified in 45 CFR 162.1002(c)(1) which includes International Classification of Diseases, 10th Revision, Clinical Modification (ICD–10–CM); International Classification of Diseases, 10th Revision, Procedure Coding System (ICD–10–PCS) (including The Official ICD–10–PCS Guidelines for Coding and Reporting); National Drug Codes (NDC); the combination of Health Care Financing Administration Common Procedure Coding System (HCPCS), as maintained and distributed by HHS, and Current Procedural Terminology, Fourth Edition (CPT–4), as maintained and distributed by the American Medical Association, for physician services and other healthcare services; Health Care Financing Administration Common Procedure Coding System (HCPCS) as maintained and distributed by HHS, for all other substances, equipment, supplies, or other items used in healthcare services; and Code on Dental Procedures and Nomenclature.

We have not finalized this proposal and explain the update later in this section in response to a comment in support of our proposal to update the standards for Medications in § 170.207(d).

- § 170.207(e)—Immunizations

We proposed to revise § 170.207(e)(1), which is currently reserved, to reference CVX—VaccinesAdministered, updates through June 15, 2022, and incorporate it by reference in § 170.299. We also proposed to revise § 170.207(e)(2), which is currently reserved, to reference National Drug Code Directory (NDC)—Vaccine NDC Linker, updates through July 19, 2022, and incorporate it by reference in § 170.299.

- § 170.207(f)—Race and ethnicity

We proposed to add § 170.207(f)(3) to reference CDC Race and Ethnicity Code Set Version 1.2 (July 15, 2021) and incorporate it by reference in § 170.299.

- § 170.207(m)—Numerical references

We proposed to revise § 170.207(m)(2), which is currently reserved, to reference the Unified Code for Units of Measure, Revision 2.1, November 21, 2017, and incorporate it by reference in § 170.299.

- § 170.207(n)—Sex

We proposed to revise § 170.207(n)(2), which is currently reserved, to reference the version of SNOMED CT ® U.S. Edition codes specified in § 170.207(a)(1). We also proposed to add § 170.207(n)(3) to reference the version of LOINC ® codes specified in § 170.207(c)(1).

- § 170.207(o)—Sexual orientation and gender information

We proposed to change the heading of § 170.207(o) from ''sexual orientation and gender identity'' to ''sexual orientation and gender information'' to acknowledge that § 170.207(o) includes

standard code sets to support other gender related data items. We proposed to add § 170.207(o)(3) to reference the version of SNOMED CT ® U.S. Edition codes specified in § 170.207(a)(1) and to add § 170.207(o)(4) to reference the version of LOINC ® codes specified in § 170.207(c)(1) for Pronouns.

• § 170.207(p)—Social, psychological, and behavioral data

We proposed to revise § 170.207(p)(1) through (8) to reference the version of LOINC® codes specified in proposed § 170.207(c)(1) instead of § 170.207(c)(3). We proposed to revise § 170.207(p)(4), (5) and (7) and (8) to reference the version of the Unified Code of Units of Measure in proposed § 170.207(m)(2), instead of § 170.207(m)(1). We also proposed to revise § 170.207(p)(6) to include a reference to the version of the Unified Code of Units of Measure in proposed § 170.207(m)(2).

• § 170.207(r)—Provider type

We proposed to revise § 170.207(r)(2), which is currently reserved, to reference Medicare Provider and Supplier Taxonomy Crosswalk, October 29, 2021, and incorporate it by reference in § 170.299.

• § 170.207(s)—Patient insurance

We proposed to revise § 170.207(s)(2), which is currently reserved, to reference Public Health Data Standards Consortium Source of Payment Typology Code Set December 2020 Version 9.2 and incorporate it by reference in § 170.299.

In addition to updating the minimum standards code sets listed above, we proposed to update some of the certification criteria that reference those minimum standards. We proposed to update some of the certification criteria that reference § 170.207(a) Problems by replacing the reference to § 170.207(a)(4) in those criteria that reference it with a reference to the new proposed § 170.207(a)(1). These criteria include § 170.315(a)(12), (b)(1)(iii)(B)(*2*), (b)(6)(ii)(B)(*2*), (c)(4)(iii)(I), and (f)(4)(ii). We also proposed to update § 170.315(f)(3)(ii) by replacing the reference to § 170.207(a)(3) with a reference to the new proposed § 170.207(a)(1).

We proposed to update the certification criteria that reference § 170.207(c) Laboratory Tests by replacing the references to § 170.207(c)(2) and (c)(3) in those criteria with a reference to the new proposed § 170.207(c)(1). These criteria include § 170.315(f)(3)(ii) and (f)(4)(ii).

We proposed to update two certification criteria that reference § 170.207(e) Immunizations. We proposed to update the certification criterion § 170.315(f)(1)(i)(B), which references § 170.207(e)(3), to instead reference the new proposed § 170.207(e)(1). We also proposed to update the certification criterion § 170.315(f)(1)(i)(C), which references § 170.207(e)(4), by replacing the reference to § 170.207(e)(4) in that criterion with a reference to the new proposed § 170.207(e)(2).

We proposed to update several certification criteria that reference § 170.207(f) Race and Ethnicity. We proposed to update certification criteria that reference § 170.207(f)(2) to instead reference the new proposed § 170.207(f)(3). These criteria include § 170.315(a)(5)(i)(A)(*1*) and (*2*) and § 170.315(c)(4)(iii)(H).

As described in sections III.C.1 and III.C.8 of this final rule, we proposed to update criteria that reference § 170.207(n) Sex by updating criteria that reference § 170.207(n)(1) to reference the new proposed § 170.207(n)(2). More specifically, we proposed to update § 170.315(a)(5)(i)(C) to reference § 170.207(n)(1) for the time period up to and including December 31, 2025, or to reference § 170.207(n)(2). We also proposed to update § 170.315(c)(4)(iii)(G) and § 170.315(b)(1)(iii)(G)(*3*) to reference § 170.207(n)(2). We note that, in the HTI–1 Proposed Rule regulation text in § 170.315(b)(1)(iii)(G)(*3*), we inadvertently included a reference to § 170.213 (88 FR 23909) instead of including § 170.207(n)(2) as discussed in our proposal (88 FR 23821). ONC has finalized § 170.315(b)(1)(iii)(G)(*3*) without the proposed reference to § 170.213. We have finalized § 170.315(b)(1)(iii)(G)(*3*) to include a reference to § 170.207(n)(2) to correct this error and to reference the most recent version of SNOMED CT U.S. Edition available at the time of this rule. Health IT developers may update to a newer version if one exists at effective date of the criterion.

Additionally, as described in sections III.C.1 and III.C.8 of this final rule, we proposed to update the criteria that reference § 170.207(o) Sexual orientation and gender information (as we proposed to rename the criterion) by updating criteria that reference § 170.207(o)(1) and (2). We proposed to replace the reference to § 170.207(o)(1) in § 170.315(a)(5)(i)(D) with a reference to the new proposed § 170.207(o)(3) and proposed to replace the reference to § 170.207(o)(2) in § 170.315(a)(5)(i)(E) with a reference to the new proposed § 170.207(o)(3). More specifically, we proposed to update § 170.315(a)(5)(i)(D) to reference § 170.207(o)(1) for the time period up to and including December 31, 2025, or to reference § 170.207(o)(3), as well as whether a patient declines to specify sexual orientation. We proposed to update § 170.315(a)(5)(i)(E) to reference § 170.207(o)(2) for the time period up to and including December 31, 2025, or to reference § 170.207(o)(3), as well as whether a patient declines to specify gender identity.

We also proposed to update § 170.315(c)(4)(iii)(C), which references § 170.207(r) Provider Type. Specifically, we proposed to replace the reference to § 170.207(r)(1) in that criterion with a reference to the new proposed § 170.207(r)(2). We also proposed to update § 170.315(c)(4)(iii)(E), which references § 170.207(s) Patient insurance. Specifically, we proposed to replace the reference to § 170.207(s)(1) in that criterion with a reference to the new proposed § 170.207(s)(2).

Comments. Most commenters were supportive of ONC's proposal to adopt updated minimum code set versions. Meanwhile other commenters had recommendations pertinent to specific standards considered a ''minimum standard'' code set.

Response. We thank commenters for their support of our proposal to adopt updated minimum code set versions. We have finalized the adoption of updated minimum standard code set versions as proposed. We note that newer versions of the codes sets may have become available since we published the HTI–1 Proposed Rule and this does not preclude developers of certified health IT from updating minimum code sets to newer versions in their Health IT Modules.

Comments. Several commenters suggested different naming conventions for different standards and data concepts included as part of the Program's minimum standard code sets, including the name of Patient Demographics, Sexual Orientation, and Gender Identity.

Response. We appreciate these comments. However, we have finalized the title of § 170.207(o) to reflect the inclusion of the minimum standard code set for Pronouns in that section, and we have finalized our proposal to update the Sexual Orientation and Gender Identity title in § 170.207(o) to ''Sexual orientation and gender information'' to provide clarity on the standard code sets related to data elements in that section. We have also finalized our proposal to update the ''demographics'' title in § 170.315(a)(5) to ''patient demographics and observations'' to acknowledge that not all data described in that section are understood to be demographics.

Comments. We received multiple comments encouraging ONC to continue to work with the HL7 Gender Harmony project team and federal partners to update terminology definitions over time.

Response. We thank commenters for their support of our working with the HL7 Gender Harmony project team and federal partners to update terminology definitions. We anticipate ongoing collaboration with these parties to promote collection and exchange of data elements related to health equity and support for underserved populations.

Comments. We received a comment in support of the proposal to update the standards for Medications at § 170.207(d); however, the commenter noted that the reference to 45 CFR 162.1002(c)(1) for NDC includes references to medical code sets that are not appropriate for medications and the reference should be changed to 162.1002(b)(2), which is specific to NDC.

Response. We thank the commenter for their support of our proposed updates. We note that our reference to 45 CFR 162.1002(c)(1) in the proposal was intended to be consistent with the timeframes identified in the referenced regulation—*i.e.,* ''For the period on and after October 1, 2015'' as opposed to 45 CFR 162.1002(b)(2) which is referenced as ''For the period on and after October 16, 2003 through September 30, 2015.'' However, we agree with the commenter that the reference should include only NDC, and we have finalized § 170.207(d)(4) to reference 45 CFR 162.1002(b)(2) as referenced in 45 CFR 162.1002(c)(1) for the period on and after October 1, 2015.'' We did not intend to cross-reference code sets no longer in effect, and we believe that commenters would have anticipated us to correct this.

Comments. We received several comments related to the OMB Initial Proposals For Updating OMB's Race and Ethnicity Statistical Standards and the 2022 proposed updates to the CDC Race and Ethnicity code set. Some commenters suggest that ONC prioritize and prepare for any changes that may be necessary should the proposed changes be finalized. Other commenters expressed concern that the proposed changes will have a significant impact on health IT. Some commenters provided suggestions for ONC to develop data collection guidelines and provided suggestions for code set content updates.

Response. We thank commenters for their input regarding the proposed updates to the CDC race and ethnicity code set and OMB race and ethnicity collection; however, these comments are out of scope for this rulemaking. We will continue to work with federal partners to promote alignment for these data concepts.

Comments. We received comments regarding the effective dates for the new minimum code set versions. Some comments suggested that ONC specify the time health IT developers must incorporate the new code set versions once they have been published to allow time for health IT developers and providers to incorporate the new versions. Other commenters recommended that ONC align code set version update timelines to the base program requirements.

Response. We thank commenters for their input regarding the effective dates for new minimum code set version and to align code set version updates timelines to the base Program requirements. We have finalized the adoption of § 170.207 with a compliance date of January 1, 2026.

We have adopted the proposed version of code sets. Again, we note that we have adopted minimum code set versions and this does not preclude developers of certified health IT from updating minimum code sets to newer versions in their Health IT Modules.

4. Electronic Case Reporting

As discussed in the HTI–1 Proposed Rule, case reporting serves as early notification to Public Health Agencies (PHAs) for potential disease outbreaks and includes information that enables PHAs to start contact tracing and other prevention measures. (88 FR 23769)

Since ONC adopted 45 CFR 170.315(f)(5) as a functional requirement for Health IT Modules in the 2015 Edition, standards development organizations (SDOs), public health, and interested parties within the healthcare industry have balloted several standards related to electronic case reporting. The standards were produced and developed through a collaborative effort among many partners, including CDC, the Council of State and Territorial Epidemiologists (CSTE), the Association of State and Territorial Health Officials (ASTHO), the Association of Public Health Laboratories (APHL), EHR developers, and the HL7 Public Health (PH) Work Group.[46] These standards pertain to both HL7® FHIR and HL7® CDA and include multiple Implementation Guides (IGs).

Recognizing advancement of standards development in this area, ONC analyzed the currently balloted standards for potential inclusion in the existing 45 CFR 170.315(f)(5) criterion. As discussed in detail in the HTI–1 Proposed Rule, ONC examined the standards for potential inclusion as a part of this criterion (88 FR 23770–23771).

In the HTI–1 Proposed Rule (88 FR 23771–23772), we proposed to adopt standards for electronic case reporting in § 170.315(f)(5)(ii). This included a proposal in § 170.315(f)(5)(ii)(A) that a Health IT Module certified to § 170.315(f)(5) support the consumption and processing of electronic case report trigger codes and parameters based on a match from Reportable Conditions Trigger Code value set in § 170.205(t)(4) received from the eRSD profiles as specified in the HL7 FHIR eCR IG in § 170.205(t)(1). We clarified that a Health IT Module need only support parsing and consuming the eRSD Specification Library and eRSD Supplemental Library because we understand that health IT developers may choose to either manually encode the electronic case reporting trigger logic into Health IT Modules or may support a more automated process for encoding the trigger logic into Health IT Modules. We requested comment on this approach and on whether there is general support of the eRSD Specification Library and eRSD Supplemental Library for electronic case reporting triggering (88 FR 23773).

Additionally, we proposed in § 170.315(f)(5)(ii)(B) to require a Health IT Module to create a case report for electronic transmission according to at least one of the following two HL7® standards: in accordance with the electronic initial case report (eICR) profiles specified in the HL7 FHIR eCR IG in § 170.205(t)(1) or in accordance with the HL7 CDA eICR IG in § 170.205(t)(2). Finally, we proposed in § 170.315(f)(5)(ii)(C) to require that Health IT Modules certified to § 170.315(f)(5) support the receipt, consumption, and processing of reportability responses (RR) formatted according to the RR profiles defined in the HL7 FHIR eCR IG or the HL7 CDA RR IG.

Comments. We received numerous comments and broad support for updating the ''electronic case reporting'' criterion to reference standards-based requirements. Commenters stated that the current functional certification criteria in the Program do not meet eCR program needs and that requiring use of a standard would improve interoperability and implementation

[46] See work group membership at: *https://confluence.hl7.org/display/PHWG/Public+Health+Work+Group.*

consistency to further enable the transmission of timely, granular, and accurate case data between health providers and public health agencies. Commenters stated that moving from functional electronic case reporting requirements to standards-based requirements is an important step toward ensuring that public health programs have access to critical data. Commenters also stated there is substantial opportunity to empower public health, improve public health surveillance, and more efficiently monitor and manage public health concerns through standardization of electronic case reporting. Others wrote that the standards would improve consistency and increase real-time communication between healthcare and public health.

Several commenters supported the requirements as proposed, including the requirements for Health IT Modules to support either HL7 FHIR or HL7 CDA standards for case reporting. Some commenters stated the need for EHRs to support the HL7 CDA standard since many public health agencies only accept HL7 CDA documents. Several commenters stated that both the HL7 CDA and the HL7 FHIR standards should be required to allow Public Health Agencies (PHAs) time and the appropriate resources to be able to receive incoming electronic case reports. Other commenters stated they would prefer a single standard be included in the criterion rather than including multiple options for certification. Commenters noted that existing health information conversion tools could help with the translation between HL7 CDA and HL7 FHIR formats. Additionally, commenters advocated that the electronic case report and the reportability response should adhere to the same standard (CDA or FHIR) and noted that it would be burdensome if the reportability response from public health was based on a different standard than the initial case report.

Response. We appreciate these comments and agree with the importance of including standards to improve interoperability and public health agencies' access to critical information. Taking into consideration feedback from commenters, we have finalized our proposal in § 170.315(f)(5)(ii)(B) to require Health IT Modules to enable a user to create a case report consistent with at least the eICR profile of the HL7 FHIR eCR IG in § 170.205(t)(1) or the HL7 CDA eICR IG § 170.205(t)(2). Additionally, we have finalized in § 170.315(f)(5)(ii)(C) to require Health IT Modules to receive, consume, and process a case report response according to the reportability response profile of the HL7 FHIR eCR IG in § 170.205(t)(1) or the HL7 CDA RR IG in § 170.205(t)(3) as determined by the standard used in (f)(5)(ii)(B) of this section. We have finalized this requirement to ensure that a Health IT Module that creates a case report according to the eICR profile of HL7 FHIR eCR IG can receive, consume, and process a case report response using the same HL7 FHIR eCR IG. The same would be true for a Health IT Module that creates a case report according to the HL7 CDA eICR IG; this Health IT Module must be capable of receiving a reportability response according the HL7 CDA RR IG. We believe requiring support for creating a case report based on either the HL7 FHIR eCR IG or the HL7 CDA eICR IG while requiring support for receipt, consumption, and processing of a case report response according to either the HL7 FHIR eCR IG or the HL7 CDA RR IG provides technical design flexibility while supporting the HL7 CDA-based landscape for case reporting that exists today. Additionally, we have finalized our proposal in § 170.315(f)(5)(ii)(D) for Health IT Modules to support transmission of a case report electronically to a system capable of receiving a case report.

As with most consensus-based standards, we recognize that additional improvements can be made to the HL7 FHIR and HL7 CDA IGs for case reporting. We encourage interested parties, including the CDC, the appropriate HL7 working groups, and public health associations to update and improve the IGs, as well as collaborate on solutions that facilitate the ability of PHAs to parse, filter, and consume case reports. We plan to continue monitoring the development of standards for case reporting and foundational standards that facilitate interoperability for various public health use cases. As the HL7 FHIR-based certification criteria in the Program continue to grow and industry more broadly supports HL7 FHIR-based IGs, we intend to transition to solely an HL7 FHIR-based approach for case reporting in future rulemaking.

Comments. One commenter suggested that the adoption of HL7® standards was unnecessary to advance interoperability for EHI because EHR systems are capable of effectively and securely communicating using multiple standards and messaging formats. This commenter stated that the adoption of HL7 standards would prevent health care providers from using other standards that could better serve different situations and communities.

Response. We disagree that adoption of standards for case reporting is unnecessary to advance interoperability. We note that for nearly a decade, Program requirements for electronic case reporting have not been standards-based, and numerous examples cited in this preamble and in the HTI–1 Proposed Rule reveal deficiencies in nationwide electronic case reporting due to misaligned technical standards and implementations. We believe that consensus has emerged for adoption of HL7 standards, which we have finalized in § 170.315(f)(5)(ii), and we believe that such standards can be enhanced over time to address the emergent needs of health care providers and the communities they serve.

Comments. We received multiple comments supporting our proposal relating to the consumption and processing of case report trigger codes based on the Reportable Conditions Trigger Code value set in § 170.205(t)(4). Many public health agency commenters expressed support to require certified Health IT Modules to support the ability to consume and process the eRSD profiles, which include the RCTC value set, regardless of whether such a Health IT Module supports a FHIR-based or CDA-based approach to certification, stating that it would support interoperability. One hospital-based commenter suggested that in addition to the mandated proposed RCTC value sets, ONC should require support for the adjunct 'eRSD Supplemental Library' as part of the certification criterion at § 170.315(f)(5) as we proposed. Several health IT developer commenters stated that the eRSD profiles should not be required, including the reference to the eRSD Supplemental Library or the eRSD Specification Library, stating that the underlying standards are too immature and not sufficient for broad use. Commenters further stated concerns about the burdensome and manual updates and maintenance required to support the eRSD profiles and noted that the specification is mainly in use today by the eCR Now FHIR App, a solution developed specifically for case reporting. One commenter suggested that Health IT Modules should be required to use updated reportable condition trigger codes, stating that during an emergency, new trigger codes are almost always needed and are necessary in effectiveness of use in an emergency response. One commenter emphasized coordination with the CDC to not only make eRSD-based sharing of reportable events available, but also the Reportable Conditions Knowledge Management System (RCKMS) to enable

efficient sharing of PHA requirements in terms of reportable events, content, format, and transport.

Response. We thank the commenters for their perspectives. We agree that consuming and processing reportable condition trigger codes is a necessary first step in electronic case reporting, and we have finalized in § 170.315(f)(5)(ii)(A) our proposal that Health IT Modules certified to § 170.315(f)(5) must, beginning January 1, 2026, support the consumption and processing of case reporting trigger codes and must identify a reportable patient visit or encounter based on a match from the RCTC value set in § 170.2015(t)(4). However, after additional examination of the HL7 FHIR eCR specification, and in response to comments received, we have not adopted our proposal to require that such Health IT Modules receive the RCTC value set from the eRSD profiles as specified in the HL7 FHIR eCR IG in § 170.205(t)(1). This means that Health IT Modules do not need to support the eRSD profiles, including the eRSD PlanDefinition, Supplemental Library, and Specification Library, in order to be certified to § 170.315(f)(5).

We have finalized this approach to allow developers of certified health IT flexibility to support the consumption of the RCTC value set in the way that best suits their technology and in a way that does not constrain how the RCTC value set is consumed as the underlying standards mature. We share concerns with commenters who noted that the triggering logic within the eRSD profiles of the FHIR IG are complex, not supported across the industry, and remain largely untested outside their use in the eCR Now FHIR App. We believe requiring that a Health IT Module certified to § 170.315(f)(5) support the consumption and processing of case reporting trigger codes and identify a reportable patient visit or encounter based on a match from the RCTC value set in § 170.205(t)(4), without further constraining how the RCTC value set is received, will simplify Program conformance and responds to concerns raised by commenters and raised through our own analysis.

For purposes of Program conformance, we reiterate from the HTI–1 Proposed Rule that the RCTC value set in § 170.205(t)(4) is a minimum standard code set, and that Health IT Modules certifying to § 170.315(f)(5) by way of § 170.315(f)(5)(ii) may voluntarily support an updated version (*e.g.,* a subsequent release) of the RCTC value set. We anticipate that health IT developers would be incentivized by their customers to take advantage of this opportunity to voluntarily support updated versions of the RCTC value set because updated versions will likely include new codes reflecting new or emerging infectious diseases (88 FR 23773). We urge developers with Health IT Modules certified to § 170.315(f)(5)(ii) to support all the reportable condition trigger codes in the RCTC value set as it updates so that emerging infectious diseases may be reported electronically to public health authorities as those infectious diseases emerge.

We note that the RCTC value set is not currently hosted on the National Library of Medicine Value Set Authority Center, like many other value sets. Instead, the RCTC value set is currently available for distribution by the Association of Public Health Laboratories.[47] We plan to work with CDC and the industry to align the availability of the RCTC value set with other, similar value sets in the future.

Finally, we note that the CDA IG cross-references the RCTC value set specified in the HL7 FHIR eCR IG.[48] Therefore, Health IT Modules certified to § 170.315(f)(5) using the HL7 CDA IG as described in § 170.315(f)(5)(i), must also support the requirement to trigger a case report based on a match from the RCTC value set in § 170.205(t)(4) at a minimum. We encourage implementers to reference the HL7 CDA eICR IG for additional guidance regarding the use of the RCTC value set for identifying reportable cases.

Comments. Commenters suggested requiring a longer compliance date than December 31, 2024, for health IT developers to certify to the proposed updated criterion to allow the industry to widely implement the standards-based requirements in production. One commenter expressed support, stating that allowing current standards requirements to remain until December 31, 2024, is reasonable, while another commenter recommended an implementation deadline of December 31, 2025. Several commenters stated that more time should be given for compliance, such as a minimum of 24 months post-final rule effective date for such deadlines or postponing the requirement for electronic case reporting until public health jurisdictions can adequately adapt to the technology needed to ingest the data. One commenter expressed that more time is needed to develop, test, and deliver new capabilities, stating that the proposed timeframe is insufficient.

Response. We appreciate commenters' concerns about the timelines for conformance to new standards for the Program. We have finalized in § 170.315(f)(5) that Health IT Modules must enable a user to create a case report for electronic transmission meeting requirements in § 170.315(f)(5)(i) for the time period up to and including December 31, 2025, or meet the requirements in § 170.315(f)(5)(ii). This approach will allow developers to continue to certify to functional requirements for case reporting according to § 170.315(f)(5)(i) while allowing developers to certify to the standards-based approach to case reporting in § 170.315(f)(5)(ii). After December 31, 2025, developers will only be able to certify to case reporting using the standards-based approach described § 170.315(f)(5)(ii). In addition, previously certified products will need to update their certification to the standards-based approach described in § 170.315(f)(5)(ii) by December 31, 2025. We believe this date will provide adequate time for developers of certified health IT with Health IT Modules certified to § 170.315(f)(5) to comply with the requirements we have finalized, while also ensuring timely implementation of the requirements for public health agencies.

Comments. Many commenters suggested that systems receiving electronic case reports should also have to certify to capabilities that align with the requirements in § 170.315(f)(5). Another commenter stated that there is little value in requiring the capability to transmit electronic case reporting if public health partners do not have the capabilities to receive data electronically. Some commenters stated that they are prepared to support electronic case reporting but have not been able to do so due to lack of public health capacity to receive it, and recommended ONC work with other agencies to support public health partners with funding to bolster electronic case reporting capacity. Several commenters suggested ONC provide support for the transition to eCR reporting, such as ONC collaborating with other agencies and public health entities to provide financial resources/incentives and support, as well as publishing and maintaining a master list of U.S. public health data standards, and work with state and local public health agencies to ensure technical readiness for their adoption and implementation. One commenter

[47] Electronic Reporting and Surveillance Distribution page managed by the Association of Public Health Laboratories: *https://ersd.aimsplatform.org/#/home.*

[48] See section 1.11.2 of the CDA eICR IG titled, ''Using the eRSD (from the FHIR eCR IG).'' *https://www.hl7.org/implement/standards/product_brief.cfm?product_id=436.*

recommended ONC encourage and enforce public health agencies to move away from manual reporting. The same commenter also urged coordination to promote the reduction and elimination of variances in format and transport mechanisms.

One commenter expressed support and requested clarification if the intent is to require support based on the standards ONC specifies, and not to require support for jurisdiction-specific communication methods. Another commenter stated that state and local variations create burden on the sender to meet specific requests and needs of jurisdictions. One commenter requested further guidance through a companion guide on how to comply with differing federal and state regulations related to electronic case reporting requirements, such as what additional data elements are needed by state PHAs and beyond those that are defined in the standards. Multiple commenters expressed concern regarding variability in implementation of standards, and the jurisdictional distinctions that required customizations and manual burden to maintain. We received a few comments stating that the proposed requirements are too broad and urged a more tempered approach to permit maturation as integrations increase. One commenter stated that the proposal does not describe likely performance parameters or offer an architecture that would support true disease surveillance. Some commenters expressed concern with public health agencies' lack of readiness for electronic case reporting, stating that, in their experience, production use of electronic case reporting is limited for conditions beyond COVID–19 and Mpox.

Response. We understand that gaps remain in practice regarding the ability of public health agencies to receive electronic case reports, particularly with parsing, filtering, and consuming incoming electronic case reports, and that manual reporting mechanisms remain in place for many reportable conditions. We appreciate the commenters that suggested we create an aligned requirement for systems receiving electronic case reports and will consider these comments for future rulemaking. We are supportive of CDC-led efforts to build public health capacity to accept electronic case report information, and the electronic receipt and ingestion of electronic case reports are a core component of the CDC Public Health Data Strategy.[49] We believe the timeline for requiring standards-based electronic case reporting for Health IT Modules certified to § 170.315(f)(5) will allow both healthcare organizations and public health agencies to develop and implement the capability for receipt and exchange of electronic case reports and associated information. We recognize the need for ONC to continue to collaborate and coordinate with CDC and national public health associations, as well as with public health jurisdictions. Further, there are tools and intermediary options available, like HL7 CDA to HL7 FHIR conversion tools, that PHAs could leverage to accept incoming HL7 FHIR-based case reports and convert them into a format they can receive and process.

We acknowledge that variations between state and federal requirements and local requirements and needs add burden for reporters. However, we are unable to holistically solve this challenge through the Program. The Program is voluntary, and developers that elect to participate are only required to adhere to the requirements in applicable certification criteria. The Program does not directly address case reporting requirements imposed by state or local bodies. Furthermore, we believe these issues could be addressed through the standards development processes, including through the Public Health Workgroup for HL7, and through working with PHAs and appropriate public health associations to align on the use of a national standard and reduce state and local variation in requirements where possible. Regarding comments that the proposals are too broad, we believe requiring standards-based support for electronically reporting case reports and receiving reportability responses, including using standard triggers, will allow for implementation flexibility while improving interoperability. Further, standards-based requirements can help to reduce variation and fragmentation that may otherwise cause interoperability issues for implementers and users. We understand that PHAs expressed concerns related to technology used by PHAs being able to accept incoming reports that adhere to the FHIR standard. We believe that the longer timeline can help with this transition, as well as allow the industry time to pursue different approaches to implementing the required components of the eCR FHIR IG. We understand concerns related to performance, scalability, and maintenance, and will monitor standards development and implementation to inform future rulemaking.

Comments. Some commenters stated that public health-specific approaches for data exchange should not be the way of the future, and that existing solutions, such as FHIR capabilities including subscriptions and patient-level queries, should instead be leveraged for the purposes of public health data exchange. Several commenters believe common data infrastructure and standards, such as HL7 FHIR-based APIs and the SMART Backend Services, would better serve electronic case reporting than the current standards, which they stated are brittle and require consistent updating and manual support. Several commenters offered suggestions of additional functionality. One commenter suggested that health IT developers must provide functionality to users to send on-discharge summary updates for patients admitted to hospital, and interfaces to allow their users to adjust timing of triggering, document build, send, and other parameters. One commenter suggested that ONC incorporate the language and data elements of specialty records into its standards to increase effectiveness for interoperability initiatives across the spectrum of patient care. Another commenter suggested requiring functionality related to high-risk and immediate reporting for provider-initiated (or 'manually triggered') electronic reporting stating that provider-triggered 'manual' eCRs are critical for emergency preparedness and reducing the burden on healthcare staff and public health staff of manual reporting and data entry in future outbreaks, novel conditions, and early in confirmed outbreak scenarios. One commenter stated that healthcare facility IDs and address formatting cause serious impacts for public health because they cannot be verified for eCRs sent. The commenter, therefore, suggested more standards conformance and health IT functionality to allow users to easily edit, update, and maintain correct facility IDs, as well as consistent formatting of address and rational facility naming, will ease processing burden on PHAs and other data receivers. Several comments mentioned specific challenges within the proposed specifications, including challenges with certain data elements.

Response. We acknowledge the importance of reusable and scalable standards for health information interoperability including standards-based APIs. The Standardized API for ''patient and population services'' criterion at § 170.315(g)(10) has provided a baseline for reusable services to advance interoperability nationwide.

[49] *https://www.cdc.gov/ophdst/public-health-data-strategy/Public_Health_Data_Strategy-final-P.pdf.*

Like many other HL7 FHIR IGs in the US Realm, the HL7 FHIR profiles defined in the eCR FHIR IG were built using the profiles defined in the US Core IG as part of the HL7 FHIR profiling model.[50] Notably, the US Core IG is part of the certification criterion at § 170.315(g)(10), adopted in § 170.215(b)(1) and incorporated by reference in § 170.299. While we recognize the potential of these foundational APIs, implementation guides, and services to generally support public health, we believe it is helpful to provide further specificity for use cases like electronic case reporting. We will consider ways to align the public health certification criteria in the Program to promote reuse of common standards to support various public health reporting and interoperability use cases in future rulemaking. We appreciate that challenges and additional potential uses and applications of the electronic case reporting standard remain. However, the Program is not the venue through which the specification can be updated or changed. We encourage commenters to participate in standards development processes, including in the HL7 Public Health Workgroup. Further, we are aware that tools exist for PHAs that can translate incoming FHIR to CDA and/or other formats that public health surveillance systems can currently accept, which can aid with data receipt in the interim period as surveillance systems are updated to be able to receive FHIR and as additional FHIR-based tools and solutions are developed and implemented.

For concerns related to triggering and adjusting triggers based on timing and the occurrence of certain events, we believe this can be addressed through healthcare organizations and other reporters working with public health jurisdictions to determine the timing and triggers that work for all involved participants and that do not place undue burden on health IT and public health systems. We also encourage triggering and timing approaches to be discussed through standards development processes to develop, pilot, and share approaches that meet the needs of both reporters and public health agencies.

Comments. One commenter requested clarification on whether the Health IT Module being certified needs to identify any intermediaries involved in the transmission of electronic case reports or RR messages as part of certification, or if these intermediaries need to also be certified for these eCR criteria. Another commenter requested clarification on how a ''system capable of receiving an electronic case report'' would be identified or validated, and whether this system would need to be certified against specific criteria. A few commenters recommended recognition, or new certification processes using the eCR Now FHIR application with a companion guide, as well as a different set of data than the USCDI v1 data set cited as standard for the criterion to ensure health IT systems can meet the new certification criteria. One commenter suggested that the eCR Now FHIR App should be accepted for certification. Some commenters expressed a belief that continued success in case reporting relies on a reasonable expectation of a routing and decision support intermediary such as AIMS (APHL Informatics Messaging Services). One commenter suggested that the AIMS network should support the submission (and response to submission) of any public health reporting using RESTful (or Representational State Transfer) application programming interfaces. One commenter recommended that ONC work closely with the CDC and the AIMS Platform team to ensure requirements do not exceed or violate the AIMS requirements, stating that many of the proposals are beyond the current allowed features on the AIMS network application programming interfaces. One commenter recommended that ONC work closely with the CDC and the AIMS Platform team to ensure requirements do not exceed or violate the AIMS requirements, stating that many of the proposals are beyond the current allowed features on the AIMS network.

Response. We appreciate the questions we received related to intermediaries, the use of specific tools or systems, and the applicability of the Program to intermediaries. Our Program is voluntary, and health IT developer participation in the Program has traditionally been incentivized through connections to CMS payment programs. While we do not have the authority to enforce or provide incentives for adoption of certified Health IT Modules, other entities could choose to do so. Should other federal entities choose to require certain systems or technologies to certify to the criterion at § 170.315(f)(5) via other mechanisms, the applicability of the requirements could extend beyond health IT that is traditionally presented for certification. Additionally, developers of intermediary software may also voluntarily certify their technology through the Program without incentives or requirements.

As part of the Program, we do not require the use of specific systems or solutions, such as the eCR Now FHIR App, which several commenters raised. Rather, we specify standards-based requirements based on standards and implementation specifications that have been developed through consensus by the health IT industry and functional requirements to allow for flexibility and innovation. We are aware that the eCR Now FHIR App is an option for transmitting electronic case reports using either the HL7 CDA IG or the HL7 FHIR eCR IG. We also are aware of the CDC-supported data ingestion building blocks that can aid PHAs in converting incoming information from HL7 FHIR to HL7 CDA so that surveillance systems are able to process reports in the standards with which they can currently receive data. Developers of certified health IT have the flexibility to leverage the eCR Now FHIR App or other solutions to meet the requirements under our Program under existing requirements for § 170.315(f)(5). Further, as developers of certified health IT work to implement either the CDA or FHIR standards as part of their Health IT Modules, they can use ''relied upon software'' to demonstrate certification criteria compliance (see 84 FR 7433 and 76 FR 1276–1277).[51] This encompasses third-party software or products that are not developed by the health IT developer but are being used to meet a portion of (or the entirety of) certain certification criteria. Such third-party products must be reported to the Certified Health IT Product List. We are aware that there are several technical options that meet our required functional criteria adhering to the FHIR standard. Intermediaries, such as the AIMS platform supported by APHL, as well as other intermediaries such as HIEs or HINs, are used by healthcare organizations to assist with routing, transport, and, in some cases, conversion before submitting electronic case reports to PHAs. However, we do not dictate the mechanism through which vendors or organizations choose to accomplish the electronic case reporting workflow—only the functional expectations and the accompanying standard(s). At this time, ONC is not requiring Health IT Modules certified to § 170.315(f)(5) to specifically connect to AIMS or support RCKMS[52] to meet the proposed requirements in § 170.315(f)(5)(ii)(D). While we

[50] *https://hl7.org/fhir/R4/profiling.html#reslicing.*

[51] *https://www.healthit.gov/sites/default/files/relieduponsoftwareguidance.pdf.*

[52] *https://www.rckms.org/.*

understand the role AIMS and RCKMS play in a centralized, hub-and-spoke model for electronic case reporting, we proposed that the functional requirements for § 170.315(f)(5)(ii)(D) remain agnostic as to which reporting platform and which decision support tool(s) are used. Further, the use of HL7 FHIR supports the use of RESTful APIs. We will continue to coordinate and work with CDC on ensuring support is available as Health IT Modules work toward Certification of the ''electronic case reporting'' criterion, regardless of their approach. Given public comments and our desire to support providers reporting electronic case reports to any PHA that may be authorized to receive case reports, we have finalized our requirements in § 170.315(f)(5)(ii)(D) to ''transmit a case report electronically to a system capable of receiving an electronic case report,'' as proposed.

Comments. One commenter recommended that systems be tested with ''live'' public health information systems, or systems specified by the public health community instead of self-certifying that real world testing has been completed. The same commenter also recommended that if a Health IT Module is certified only for CDA or FHIR exchange of RR data, the Health IT Module must also successfully complete real world testing with a commercially available service to transform the data into the format not implemented as part of the Health IT Module to ensure the provider can receive RR messages regardless of the format utilized. One commenter recommended that timely and or automated eRSD updates should be considered for inclusion in real world testing. One commenter expressed that they appreciate the requirement to ensure Health IT Modules continue to demonstrate conformance through real world testing.

Response. We appreciate the comments and note that electronic case reporting is subject to the Real World Testing Condition and Maintenance of Certification requirements at § 170.405(a). However, we note that developers of certified Health IT Modules subject to real world testing have extensive flexibility to design real world testing approaches that meet requirements established in § 170.405(b)(1)(iii). We decline to establish specific requirements for real world testing plans beyond what is established in § 170.405(b)(1)(iii) for electronic case reporting currently. We also note that our requirement for Health IT Modules certifying to § 170.315(f)(5)(ii) to use either the FHIR-based or CDA-based IG is intended to facilitate interoperability and should not necessitate support for multiple formats to receive RR messages. Several commenters were concerned about receiving RRs in a different standard than the sent eICR, and we encourage the reporters to work with PHAs and intermediaries to limit the potential differentiation in standards used for eICR and RR, and to consider the use of potential solutions that could convert the eICR or RR into the corresponding standard.

We have finalized the revised criterion for electronic case reporting in § 170.315(f)(5) with modifications. First, we have finalized a modification of the proposed description in § 170.315(f)(5) from ''an electronic case report'' to ''a case report for electronic transmission'' consistent with the prior functional criterion in § 170.315(f)(5). Second, we have modified the date from December 31, 2024 to December 31, 2025 for certification to the existing functional criterion, which is now specified in § 170.315(f)(5)(i) *Functional electronic case reporting.* For the standards-based version of the criterion in § 170.315(f)(5) and specified in § 170.315(f)(5)(ii) *Standards-based electronic case reporting,* we have finalized a modification to the proposed regulation text to reference the Reportable Conditions Trigger Code value set in § 170.205(t)(4) without including the reference to the HL7 FHIR eCR IG in § 170.315(f)(5)(ii)(A). We have finalized a modification to the proposed regulation text as described above to reference only the HL7® CDA® eICR IG in § 170.315(f)(5)(ii)(B)(2). We have finalized a modification to the proposed regulation text for the capabilities described in § 170.315(f)(5)(ii)(C) by adding ''as determined by the standard used in (f)(5)(ii)(B) of this section.'' Finally, we have finalized a modification to § 170.315(f)(5)(ii)(D) to modify ''capable of receiving an electronic case report'' as follows: ''Transmit a case report electronically to a system capable of receiving a case report.''

5. Decision Support Interventions and Predictive Models

Since 2010, the Program has maintained a CDS certification criterion, consistent with the *qualified electronic health record* definition in section 3000(13) of the PHSA, which defines a qualified EHR as an electronic record of health-related information on an individual that has the capacity to ''provide clinical decision support'' (42 U.S.C. 300jj(13)(B)(i)). The initial requirements for the CDS certification criterion were intended to ensure that Health IT Modules would support broad categories of CDS while being agnostic toward the intended use of the CDS beyond drug-drug and drug-allergy interaction checks (75 FR 2046).

In 2012, ONC established a new set of requirements for Health IT Modules to support CDS. These requirements included capabilities to support evidence-based CDS based on a defined set of data elements; CDS configuration for both inpatient and ambulatory settings; and the display of source attribute or bibliographic citation of CDS (77 FR 54212). These requirements were largely based on recommendations made by ONC's Health Information Technology Policy Committee (HITPC) [53] from 2011 recommending ONC require Health IT Modules support CDS, including: (1) display source or citation of CDS; (2) be configurable based on patient context (*e.g.,* inpatient, outpatient, problems, meds, allergies, lab results); (3) be presented at a relevant point in clinical workflow; (4) include alerts presented to users who can act on alerts (*e.g.,* licensed professionals); and (5) be integrated with the EHR (*i.e.,* not standalone). In the 2015 Edition Final Rule, ONC finalized an updated CDS criterion in § 170.315(a)(9) (80 FR 62622).

Since the CDS criterion was first adopted in § 170.315(a)(9), health IT implementation and technology resources used to support clinical decision-making have continued to evolve and expand across the health IT ecosystem. Within healthcare today, predictive models are increasingly being used and relied upon to inform an array of decision-makers, including clinicians, payers, researchers, and individuals, and to aid decision-making through CDS.[54] In many cases, Health IT Modules are key components of these predictive models, often providing the data used to build and train algorithms and serving as the vehicle to influence day-to-day decision-making.[55] Both

[53] Health Informational Technology Policy Committee (HITPC) Transmittal Letter to the National Coordinator. June 2011. *https://www.healthit.gov/sites/default/files/facas/hitpc-stage-2-mu-recommendations.pdf#page=4.*

[54] See, *e.g.,* American Hospital Association. ''Surveying the AI Health Care Landscape'' 2019. *https://www.aha.org/system/files/media/file/2019/10/Market_Insights_AI-Landscape.pdf;* Darshali A Vyas, et al., Hidden in plain sight—reconsidering the use of race correction in clinical algorithms § 383 (Mass Medical Soc 2020); Fact Versus Fiction: Clinical Decision Support Tools and the (Mis)use of Race. (2021); Goldhill, Olivia. Artificial intelligence can now predict suicide with remarkable accuracy, Quartz, (July 2022), *https://qz.com/1001968/artificial-intelligence-can-now-predict-suicide-with-remarkable-accuracy/* (discussing the use of ML algorithms to predict and prevent suicide).

[55] See, *e.g.,* Burdick, Hoyt, et al. ''Effect of a sepsis prediction algorithm on patient mortality, length of

Continued

structured and unstructured data generated by, and subsequently made available through, certified Health IT Modules power the training and real-world use of predictive models. Developers of certified health IT also create and deploy predictive algorithms or models for use in production environments through their Health IT Modules and, increasingly, such developers also enable *other parties,* including third-party developers and the developer of certified health IT's customers, to create and deploy predictive models through the developer's Health IT Modules.[56] [57] In turn, certified Health IT Modules are often the vehicle or delivery mechanism for predictive model outputs to reach users, such as clinicians, through clinical decision support.[58] [59]

The National Academy of Medicine (NAM) described in a 2019 report how predictive models and other forms of artificial intelligence (AI) have the potential to represent the ''payback'' of using health IT ''by facilitating tasks that every clinician, patient, and family would want, but are impossible without electronic assistance.'' [60] The NAM report also identified a crucial ''need to present each health care AI tool along with the spectrum of transparency related to the potential harms and context of its use. Evaluating and addressing appropriate transparency, in each sub-domain of data, algorithms, and performance, and systematically reporting it, must be a priority.'' [61]

In November 2020, the Office of Management and Budget released a Memorandum for the Heads of Executive Departments and Agencies on *Guidance for Regulation of Artificial Intelligence Applications,* which directed that ''[w]hen considering regulations or policies related to AI applications, agencies should continue to promote advancements in technology and innovation, while protecting American technology, economic and national security, privacy, civil liberties, and other American values, including the principles of freedom, human rights, the rule of law, and respect for intellectual property.'' [62] This was followed by an executive order in December 2020, E.O. 13960 Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government.[63] The executive order stated: ''The ongoing adoption and acceptance of AI will depend significantly on public trust. Agencies must therefore design, develop, acquire, and use AI in a manner that fosters public trust and confidence while protecting privacy, civil rights, [and] civil liberties[.]'' (85 FR 78939).

In June 2021, the Government Accountability Office (GAO) published *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities,* which specifically outlined key principles and actions ''[t]o help entities promote accountability and responsible use of AI systems.'' This included outlining four principles for the framework, including governance, data, performance, and monitoring.[64]

In September 2022, the Biden-Harris Administration published *Principles for Enhancing Competition and Tech Platform Accountability,* which included a principle related to stopping discriminatory algorithmic decision-making.[65] In October 2022, the Biden-Harris Administration published a *Blueprint for an AI Bill of Rights,* which outlines five principles, informed by public input, that should guide the design, use, and deployment of automated systems to protect the American public in the age of AI. These principles are safe and effective systems; algorithmic discrimination protections; data privacy; notice and explanation; and human alternatives, consideration, and fallback.[66]

On February 16, 2023, E.O. 14091, Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government, was issued (88 FR 10825–10833).[67] E.O. 14091 builds upon previous equity-related executive orders, including E.O. 13985.[68] Section 1 of E.O. 14091 requires the Federal Government to ''promote equity in science and root out bias in the design and use of new technologies, such as artificial intelligence.'' Section 8, subsection (f) of E.O. 14091 requires agencies to consider opportunities to ''prevent and remedy discrimination, including by protecting the public from algorithmic discrimination.''

Finally, on October 30, 2023, E.O. 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, was issued to ensure that America leads the way in seizing the promise and managing the risks of AI.[69] This E.O. established directives and priorities for this emerging technology, including, standards for AI safety and security. E.O. 14110 supports responsible AI development and use in healthcare, specifically, and directs HHS to issue a strategic plan on responsible deployment and use of AI and AI-enabled technologies in the health and human services sector that includes ''development, maintenance, and availability of documentation to help users determine appropriate and safe uses of AI in local settings in the health and human services sector;'' (Section 8, subsection (b)(i)(E)). It likewise directs the Secretary of HHS to develop a strategy to ''determine

---

stay and readmission: a prospective multicentre clinical outcomes evaluation of real-world patient data from US hospitals.'' *BMJ health & care informatics* 27.1 (2020).

[56] Landi, H. Epic taps Microsoft to accelerate generative AI-powered 'copilot' tools to help clinicians save time. Fierce Healthcare. August 22, 2023 *https://www.fiercehealthcare.com/ai-and-machine-learning/epic-expands-ai-partnership-microsoft-rolls-out-copilot-tools-help.*

[57] See 88 FR 23860 where we discuss that a production environment is generally understood as being the setting where health IT is implemented, run, and relied on by end users in day-to-day conduct of their profession (such as medicine, nursing, or pharmacy) or other business (such as a payer processing healthcare reimbursement claims or a patient managing their health and care).

[58] Fox, A. NextGen introduces AI-enabled ambient listening that syncs with EHR. Healthcare IT News. October 11, 2023. *https://www.healthcareitnews.com/news/nextgen-introduces-ai-enabled-ambient-listening-syncs-ehr.*

[59] Miliard, M. Oracle Cerner adds generative AI to its EHR platforms. September 19, 2023. *https://www.healthcareitnews.com/news/oracle-cerner-adds-generative-ai-its-ehr-platforms.*

[60] Michael Matheny, et al., Artificial intelligence in health care: the hope, the hype, the promise, the peril, Washington, DC: National Academy of Medicine (2019).

[61] *Id.*

[62] OMB—EOP—Memorandum for the Heads of Executive Departments and Agencies on Guidance for Regulation of Artificial Intelligence M–21–06, p. 6 (Nov. 17, 2020).

[63] E.O. No. 13960, 85 FR 78939: *https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government.*

[64] GAO, Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities: (June 2021), *https://www.gao.gov/assets/gao-21-519sp.pdf.* See generally *Artificial Intelligence in Health Care: Benefits and Challenges of Technologies to Augment Patient Care,* (Nov. 2020), *https://www.gao.gov/products/gao-21-7sp.*

[65] See White House, *Principles for Enhancing Competition and Tech Platform Accountability,* Sept. 8, 2022, *https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/08/readout-of-white-house-listening-session-on-tech-platform-accountability/.*

[66] See White House, *Blueprint for an AI Bill of Rights* (October 4, 2022), *https://www.whitehouse.gov/ostp/ai-bill-of-rights/.*

[67] E.O. 14091, 88 FR 10825–10833: *https://www.federalregister.gov/documents/2023/02/22/2023-03779/further-advancing-racial-equity-and-support-for-underserved-communities-through-the-federal.* See *https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/.*

[68] E.O. 13985, 88 FR 7009: *https://www.federalregister.gov/documents/2021/01/25/2021-01753/advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government.*

[69] E.O. 14110. 88 FR 75191: *https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.*

whether AI-enabled technologies in the health and human services sector maintain appropriate levels of quality, including, as appropriate, in the areas described in subsection (i) of this section. This work shall include the development of AI assurance policy—to evaluate important aspects of the performance of AI-enabled healthcare tools—and infrastructure needs for enabling premarket assessment and post-market oversight of AI-enabled healthcare-technology algorithmic system performance against real-world data (Section 8, subsection (b)(ii)). In addition, E.O. 14110 directs HHS to establish a safety program to receive reports of—and act to remedy—harms or unsafe healthcare practices involving AI (Section 8, subsection (b)(iv)).[70]

A growing body of peer-reviewed evidence, technical and socio-technical expert analyses, and government activities and reports focus on ensuring that the promise of AI and machine learning can equitably accelerate advancements in healthcare to improve the health and well-being of the American public.[71] The Department has a longstanding interest in understanding and addressing concerns about negative, adverse, or harmful consequences that may result from the use of digital data or information about individuals' health (including data analytics), including historically, their use in computerized decision-making.[72] As such, we proposed in the HTI–1 Proposed Rule (88 FR 23774–23811) to incorporate new requirements into the Program for Health IT Modules that support the execution of AI or machine learning-based technology in support of decision-making as part of the revised CDS criterion in § 170.315(b)(11). These requirements align with the Federal Government's efforts to promote trustworthy AI and the Department's stated policies on advancing equity in the delivery of health and human services.[73]

We believe that the continued evolution of decision support software, especially as it relates to AI or machine learning-driven Predictive DSIs, necessitates new requirements for the Program's CDS criterion. We therefore proposed requirements for new sets of information that are necessary to guide decision-making based on outputs (*e.g.,* recommendations) from Predictive DSIs, such as an expanded set of ''source attributes'' and information related to how risk is managed by developers of certified health IT (88 FR 23775). We believe that these new sets of information will provide appropriate information to help guide decisions at the time and place of care, consistent with 42 U.S.C. 300jj–11(b)(4).

In the HTI–1 Proposed Rule (88 FR 23746), we provided an overview of the history, current uses, and risks associated with predictive algorithms and models in healthcare. We refer readers to section III.C.5 of the HTI–1 Proposed Rule for the details of those discussions (88 FR 23776 through 23781). We noted our goal with the proposals, described herein and as aligned with our authority, was to assist in addressing the gaps between the promise and peril of AI in health articulated in the National Academy of Medicine report[74] discussed in the HTI–1 Proposed Rule (88 FR 23780).

Objectives of the Policies To Address Predictive Modeling in DSI

In the HTI–1 Proposed Rule at 88 FR 23780–23781, we noted that the proposals for § 170.315(b)(11) were intended to introduce much-needed information transparency to address uncertainty regarding the quality of Predictive DSIs that Health IT Modules certified to the criterion in § 170.315(b)(11) support. We noted that doing so would equip potential users with sufficient information about how a Predictive DSI was designed, developed, trained, and evaluated to determine whether it was trustworthy (88 FR 23780). We proposed a dual emphasis for transparency on (1) the technical and performance aspects of Predictive DSIs and (2) the organizational competencies employed to manage risks for Predictive DSIs. Together, this information would support potential users in making better informed decisions about whether and how to use Predictive DSIs in their decision-making given the specifics of their context, patients, and needs. We noted that we considered the information included in these proposed requirements as a prerequisite to determine the quality of predictive models. We explained that our proposals were not aimed at approving or guaranteeing the quality of Predictive DSIs or the models on which they are based. Instead, the proposals were intended to provide users and the public with greater information, available in a consistent manner, on whether a Predictive DSI is fair, appropriate, valid, effective, and safe (FAVES). We anticipated that a long-term outcome of such transparency would be increased public trust and confidence in Predictive DSIs. As a result of new transparency, we anticipated that users, including healthcare systems, clinicians, and patients, would be able to expand the use of these technologies in safer, more appropriate, and more equitable ways.

We did not propose to establish or define regulatory baselines, measures, or thresholds for FAVES (88 FR 23780). Instead, we proposed to establish requirements in § 170.315(b)(11) to make information available that would enable users, based on their own judgment, to determine if a Predictive DSI, that is supported by a Health IT Module, is acceptably fair, appropriate, valid, effective, and safe. We conveyed our understanding that numerous and parallel efforts led by industry groups and academia were developing methods to evaluate Predictive DSIs for fairness, appropriateness, validity, effectiveness, and safety, among other kinds of evaluations. Moreover, we noted that we understood that these efforts were also identifying means to communicate measures of FAVES through model cards,[75] model nutrition labels,[76] datasheets,[77] data cards,[78] or algorithmic audits.[79] However, we also

[70] In addition to the E.O., on November 1, the Office of Management and Budget (OMB) released draft guidance for federal agencies, ''Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence'' available at: *https://ai.gov/wp-content/uploads/2023/11/AI-in-Government-Memo-Public-Comment.pdf.*

[71] We discuss additional federal and HHS activities—including activities resulting from the executive orders—in the subsection below entitled ''Relationship to Other Federal Agencies' Relevant Activities, Interests, and Regulatory Authority.''

[72] See *e.g.,* U.S. Dep't. of Health, Education, & Welfare (HEW), Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of citizens viii (1973) *https://aspe.hhs.gov/report/records-computers-and-rights-citizens https://aspe.hhs.gov/report/records-computers-and-rights-citizens* (The origination of the code of fair information practices, more commonly known as the fair information practice principles (FIPPs)).

[73] HHS, Statements on New Plan to Advance Equity in the Delivery of Health and Human Services, April 14, 2022, *https://www.hhs.gov/about/news/2022/04/14/hhs-statements-on-new-plan-advance-equity-delivery-health-human-services.html.*

[74] Michael Matheny, et al., Artificial intelligence in health care: the hope, the hype, the promise, the peril, Washington, DC: National Academy of Medicine (2019).

[75] Mitchell, Margaret, et al. ''Model cards for model reporting.'' Proceedings of the conference on fairness, accountability, and transparency. 2019.

[76] Sendak MP, Gao M, Brajer N, Balu S. Presenting machine learning model information to clinical end users with model facts labels. NPJ Digit Med. 2020 Mar 23;3:41. Doi: 10.1038/s41746–020–0253–3.

[77] Gebru, Morgenstern, Vecchione, et al, Datasheets for Datasets, *https://arxiv.org/abs/1803.09010.*

[78] FaccT '22: 2022 ACM Conference on Fairness, Accountability, and Transparency (June 2022) Pages 1776–1826, *https://dl.acm.org/doi/proceedings/10.1145/3531146.*

[79] See Iag Guszcza, et al., Why We Need to Audit Algorithms. Harvard Business Review. Nov. 28,

Continued

noted that these efforts lacked consensus and have not been widely or consistently implemented to date. We described that we thought it would be premature to propose requirements for specific measures or thresholds for FAVES. Rather, we stated that the proposed requirements would enable consistent and routine access to technical and performance information specifically relevant to FAVES, which would support users in making informed decisions about whether and how to use Predictive DSIs. While we stressed that transparency regarding the technical and performance dimensions of Predictive DSIs was needed, we also believed that transparency regarding the organizational and socio-technical competencies employed by those who develop Predictive DSIs was foundational for users to determine whether their Predictive DSI is FAVES. Therefore, in addition to the proposed requirements for Predictive DSI-specific source attributes, we also proposed that developers of certified health IT with Health IT Modules that enable or interface with Predictive DSIs employ or engage in intervention risk management practices, subsequently making summary information about these practices publicly available.[80] We proposed three intervention risk management practices: (1) risk analysis, (2) risk mitigation, and (3) governance (88 FR 23780). Overall, we identified these as practices that promote transparency regarding how the developer of certified health IT analyzes and mitigates risks at the organization level, including proposals that would have such developers establish policies and implement controls for governance, inclusive of how data are acquired, managed, and used in Predictive DSIs. Together, transparency regarding the technical and performance details of a Predictive, as well as the organizational competencies of the developer of certified health IT to manage risks for a Predictive DSI, were intended to contribute to the trustworthiness of these emerging and important technologies.

We noted at 88 FR 23780–23781 that the proposed requirements for the certification criterion in § 170.315(b)(11) also supported health equity by design,[81] for example, (1) emphasizing transparency regarding the use of specific data elements relevant to health equity [82] in Predictive DSIs; (2) enabling users to review whether and how the Predictive DSI was tested for fairness; and (3) enabling transparency about how developers of certified health IT manage risks related to fairness for the Predictive DSIs their Health IT Modules enable or interface with.

At 88 FR 23781, we noted our belief that the existing scope and structure of the Program were fit for these purposes because the Program has existing requirements to make information transparent regarding the authorship, bibliography, and other kinds of ''source attribute'' information for evidence-based decision support and linked referential intervention types (at § 170.315(a)(9)(v)(A) and (B), respectively). We proposed to build on these requirements so that developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) would need to enable user review of evidence-based and Predictive DSIs within their certified products, and to disclose approach(es) to intervention risk management in a publicly accessible manner. Together, we said these requirements would have an important impact on the Department's efforts to address disparities and bias that may be propagated through DSIs. Consequently, we hoped to enhance market transparency and encourage trust across the software development life cycle (SDLC) of DSIs in healthcare. We said this transparency would serve as a foundation for establishing consistency in information availability, improving overall data stewardship, and guiding the appropriate use of data derived from health information about individuals.

At 88 FR 23781, we noted that we were intentional regarding the level of prescriptiveness in our proposals because these are nascent technologies with enormous potential benefit. Thus, we sought to establish appropriate guardrails for information transparency about Predictive DSIs that do not undercut the value that could be offered to patients and clinicians from such promising technologies.

Comments. Commenters were largely supportive of our DSI proposals but mixed in their support of the specifics of the DSI certification criterion we proposed in § 170.315(b)(11). Most commenters stated that our proposals would increase transparency and accountability, enhance trustworthiness in AI and machine learning-driven decision support tools, and promote risk management by developers of certified health IT. Several commenters stated that these benefits would lead to equitable access to healthcare, contribute to reducing health disparities during provider-patient encounters, increase user and patient trust, and enhance patient experience. Commenters commended ONC's efforts to prevent bias and discriminatory outcomes driven by DSIs and noted that a regulatory framework must be created whereby tools are appropriately tested and vetted during their development, and products are labeled to provide users with essential information.

Several commenters applauded our effort to address transparency of rapidly evolving AI in healthcare. Commenters noted that adding new requirements for transparency around DSI applications' technical information, risk management processes, and real-world testing are all foundational steps in establishing these tools' safe and effective use. Several commenters agreed with our proposal that biases in the data and algorithms underlying AI or machine learning could negatively impact certain subpopulations and supported more rigorous evaluation of such tools to ensure that they are fair, effective, and support improved outcomes for patient populations. Specifically, commenters remarked that greater transparency, including about the datasets used to train a Predictive DSI, would help avoid embedding bias in the system and help improve efficiency. Several commenters noted that the HTI–1 Proposed Rule would help lay the foundations for responsible, ethical AI development in healthcare and for enhanced federal AI transparency and will promote establishing necessary assurances for greater trust in AI use. Commenters acknowledged that due to the leaps in technological innovations, especially as it relates to predictive models, it is necessary to have new requirements for the Program's CDS criterion. Several commenters agreed that it is critical for the end user to understand how a Predictive DSI is designed, developed, trained, and evaluated; and how it should be used by the end-user.

2018. *https://hbr.org/2018/11/why-we-need-to-audit-algorithms;* Xiaoxuan Liu, et al., *The medical algorithmic audit,* The Lancet Digital Health (2022). See generally Outsider Oversight: Designing a Third-Party Audit Ecosystem for AI Governance, ID Raji, P Xu, C Honigsberg, D Ho—Proceedings of the 2022 AAAI/ACM Conference on AI, 2022, *https://dl.acm.org/doi/pdf/10.1145/3514094.3534181.*

[80] Public availability and transparency aims align with the OSTP Memorandum to federal departments and agencies (August 2022): ''Ensuring Free, Immediate, and Equitable Access to Federally Funded Research'' *https://www.whitehouse.gov/wp-content/uploads/2022/08/08-2022-OSTP-Public-access-Memo.pdf.*

[81] See ''Embracing Health Equity by Design'' ONC, February 2022: *https://www.healthit.gov/buzz-blog/health-it/embracing-health-equity-by-design.*

[82] See HHS's Strategic Approach to Addressing Social Determinants of Health to Advance Health Equity—At a Glance (April 2022), *https://aspe.hhs.gov/sites/default/files/documents/aabf48cbd391be21e5186eeae728ccd7/SDOH-Action-Plan-At-a-Glance.pdf.*

Commenters approved of the proposal separately looking at risk analysis, risk mitigation, and governance as essential tasks in ensuring proper DSI development, management, and use. Commenters observed that the proposal, if adopted, would provide the opportunity for transparent, thoughtful decision-making by enabling users, including medical practitioners, health care providers, and other interested parties of AI and algorithmic tools to evaluate, disclose, and mitigate risks that could impact patients. Lastly, commenters urged ONC to be mindful that regulations on AI should not stifle innovation or have a chilling effect on beneficial uses of this emerging tool, and that we should seek to balance the risks and benefits to consumers of the public availability of information with the need to protect certain data to comply with the HIPAA Privacy Rule and limit adverse effects from a clinical standpoint.

Response. We thank commenters for their broad support of our proposals. We appreciate that many commenters understood our policy objectives and agreed with our proposals to improve trustworthiness through transparency in support of decision-making using AI machine learning-driven tools. We agree with and thank commenters who noted that greater transparency, including about the datasets used to train Predictive DSI, would help avoid embedding bias in the system and help improve efficiency. We are also mindful of the need to balance prescriptiveness and flexibility in our requirements for developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) and have made several modifications to our proposals, described in detail in subsequent responses, to achieve this balance.

Comments. Several commenters expressed concern that the proposed requirements were not strong enough to ensure DSIs are designed with equity in mind and fully validated for all patient populations when deployed and believed the HTI–1 Proposed Rule did not ensure developer accountability. One commenter was concerned that the proposal did not address or require equity testing across patient populations to limit potential biases.

Response. We appreciate commenters concerns. We have finalized several requirements that will help promote DSIs to be designed with health equity in mind, and we have finalized specific requirements related to performance measures of validity and fairness.[83] Our proposal sought to ensure that information would be available for users to easily review whether a given model has been adequately validated and tested for fairness before using it, as well as enable users to understand if a DSI used data elements relevant to health equity, such as race, ethnicity, and sexual orientation, among other data elements.[84] We clarify that nothing from our proposals nor our finalized criterion would require a user of a Health IT Module certified to § 170.315(b)(11) to review source attributes, though we also note that certain users may already have an existing obligation to ensure compliance with non-discrimination requirements and comply with applicable law.[85]

Comments. A minority of commenters did not support the proposed revised DSI certification criterion, noting that it was premature for ONC to adopt policies related to AI or machine learning. Some commenters expressed a belief that ONC's proposed revised DSI certification criterion's requirements would exceed ONC's authority, questioned whether ONC had the authority to impose non-quality or efficacy criteria on Predictive DSI, and believed there was not sufficient statutory support for the proposed revisions to DSI or authority over non-certified software that is enabled by or interfaces with certified health IT. In particular, commenters noted that ONC's authority to adopt certification criteria is provided by section 3001(c)(5)(D) of the PHSA and that the HTI–1 Proposed Rule would make changes to the architecture of health software used by thousands of hospitals and health providers across the country, including software that would not be directly part of the Program. Commenters also requested that ONC address how each of its proposed changes fit within the subcategories permitted by section 3001(c)(5)(D) of the PHSA.

Response. We disagree with commenters who believe that requirements for AI or machine learning-driven decision support is premature. Given the proliferation of such tools used in healthcare and supplied by developers of certified health IT, we believe now is an opportune time to help optimize the use and improve the quality of AI and machine learning-driven decision support tools. Moreover, our statutory authority to promulgate regulations to define certification criteria for the Program is established in 42 U.S.C. 300jj–11(c)(5)(A) and 300jj–14(b). The authority in 42 U.S.C. 300jj–11(c)(5)(D) of the PHSA was added by section 4002(a) of the Cures Act and is specific to conditions of certification under the Program, which does not limit the scope of the Program and, in fact, expanded the scope and applicability of the Program with respect to developers of certified health IT. Moreover, since 2010, the Program has included a certification criterion related to decision support in response to the definition established by Congress for *qualified electronic health record,* in 42 U.S.C. 300jj(13)(B)(i).[86] At the time Congress included this specific capability within the *qualified electronic health record* definition, it did so without specific limits and in the context of the broader HITECH Act, and subsequently the Cures Act, with the understanding that technology changes over time and so too would certification criteria. Finally, we note that our authority to propose and finalize revisions to the Program's DSI criterion is consistent with 42 U.S.C. 300jj–(c)(5) and fulfills several purposes enumerated by Congress in 42 U.S.C. 300jj–(b). The finalized requirements in § 170.315(b)(11), consistent with our authority, substantially focus on the responsibilities of developers of certified health IT and the products these developers bring forward for certification. Specifically, the updated criterion includes new sets of information that are necessary to guide

[83] See § 170.315(b)(11)(iv)(B)(v)(*5*)–(*9*).

[84] See § 170.315(b)(11)(iv)(A)(*5*)–(*13*).

[85] See U.S. Dept of Health & Human Servs., Office for Civil Rights, Notice of Proposed Rulemaking, Nondiscrimination in Health Programs and Activities, 87 FR 47824, 47880 (Aug. 4, 2022), *https://www.federalregister.gov/documents/2022/08/04/2022-16217/nondiscrimination-in-health-programs-and-activities* (prohibiting discrimination on the basis of race, color, national origin (including limited English proficiency), sex (including sexual orientation and gender identity), age, or disability in certain health programs or activities *through the use of clinical algorithms in their decision-making*); Title VI of the Civil Rights Act of 1964, 42 U.S.C. 2000d *et seq.* (prohibiting discrimination on the basis of race, color, or national origin (including limited English proficiency) in federally funded programs or activities); Title IX of the Education Amendments of 1972, 20 U.S.C. 1681 *et seq.* (prohibiting sex discrimination in federally funded education programs or activities); the Age Discrimination Act of 1975, 42 U.S.C. 6101 *et seq.* (prohibiting age discrimination in federally funded programs or activities); Section 504 of the Rehabilitation Act of 1973, 29 U.S.C. 794 (prohibiting disability discrimination in federally funded or federally conducted programs or activities); and the Americans with Disabilities Act, 42 U.S.C. 12101 *et seq.* (prohibiting disability discrimination by employers, state and local government entities, and businesses that are open to the public, among others).

[86] ONC finalized in § 170.304(e) the ''clinical decision support'' certification criteria in the interim final rule, ''Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology,'' January 13, 2010 (75 FR 2014).

decision-making based on outputs (*e.g.,* recommendations) from Predictive DSIs, including:

- An expanded set of ''source attributes'' in § 170.315(b)(11)(iv);
- Requirements for Health IT Modules to enable a limited set of identified users to access complete and up-to-date plain language descriptions of source attribute information in § 170.315(b)(11)(v);
- Requirements for intervention risk management practices to be applied for each Predictive DSI supplied by the health IT developer as part of its Health IT Module in § 170.315(b)(11)(vi); and
- Requirements for summary information related to how intervention risk is managed to be publicly accessible in § 170.523(f)(1)(xxi).

We believe that these new sets of information will provide appropriate information to help guide decisions at the time and place of care, consistent with 42 U.S.C. 300jj–11(b)(4). Additionally, our finalized policies in §§ 170.315(b)(11), 170.402(b)(4), and 170.523(f)(1)(xxi) will support several other Congressionally-identified purposes that inform the National Coordinator's work in carrying out their duties, including the duty identified in 42 U.S.C. 300jj–11(c)(5)(A). These additional purposes include 42 U.S.C. 300jj–11(b)(2), ''improves health care quality, reduces medical errors, reduces health disparities, and advances the delivery of patient-centered medical care''; 42 U.S.C. 300jj–11(b)(8), ''facilitates health and clinical research and health care quality''; 42 U.S.C. 300jj–11(b)(10), ''promotes a more effective marketplace, greater competition, greater systems analysis, increased consumer choice, and improved outcomes in health care services''; and 42 U.S.C. 300jj–11(b)(11), ''improves efforts to reduce health disparities.''

In consideration of all the public comments received, and aligned with both the authorities granted by Congress and directives established by several Executive Orders, we have finalized most of our proposals for § 170.315(b)(11) with modifications intended to align and simplify technical requirements between evidence-based DSIs and Predictive DSIs as well as to clarify: (1) the definition of Predictive DSI in § 170.102; (2) the scope of technologies considered to be an evidence-based DSI for purposes of the Program; and (3) the scope of source attribute information that must be accessible to users. Specifically, we have finalized our proposals by significantly narrowing the scope of requirements for Predictive DSI-related source attributes and intervention risk management (IRM) practices to apply only to Predictive DSIs supplied by the health IT developer as part of its Health IT Module. In addition to the detailed section-by-section final rule discussions, the following paragraphs summarize some of the key policy determinations included in this final rule.

Additionally, in consideration of comments received and the scope reductions we have made to this final certification criterion, we determined that a supportive Maintenance of Certification requirement as part of the Assurances Condition of Certification is necessary to fully implement our policy objectives and proposals. Specifically, we have finalized in this final rule an ''Assurances'' Maintenance of Certification requirement at 45 CFR 170.402(b)(4) that starting January 1, 2025, and on an ongoing basis thereafter, health IT developers with Health IT Modules certified to § 170.315(b)(11) review and update as necessary, source attribute information in § 170.315(b)(11)(v)(A) and (B), risk management practices described in § 170.315(b)(11)(vi), and summary information provided through § 170.523(f)(1)(xxi). This reinforces a health IT developer's ongoing responsibility to enable users to access complete and up-to-date descriptions of DSI source attribute information at § 170.315(b)(11)(v)(A) and (B) to review and update as necessary IRM practices for all Predictive DSIs it supplies as part of its Health IT Module, and to ensure the ongoing public availability of summary IRM practice information as submitted to their ONC–ACB via hyperlink in § 170.523(f)(1)(xxi). We have finalized that developers with Health IT Modules certified to § 170.315(b)(11) will need to comply with this Maintenance of Certification requirement starting January 1, 2025. We added this Maintenance of Certification requirement to serve as a discrete connection for developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) to ensure that their Health IT Modules have complete and up-to-date descriptions of source attribute information and other required information, both at the time of certification and on an ongoing basis while their Health IT Modules are certified to § 170.315(b)(11).

We have *not* finalized proposals related to the proposed Predictive DSI attestation statement, and we will *not* require Health IT Modules certified to § 170.315(b)(11) to support linked referential DSIs or related source attributes under the Program. Further, we have finalized modifications to our proposal for IRM practices in § 170.315(b)(11)(vi) and did *not* adopt the requirement for detailed documentation we proposed in § 170.315(b)(11)(vi)(B). The finalized § 170.315(b)(11)(vi) requires that IRM practices must be applied for each Predictive DSI supplied by the health IT developer as part of its Health IT Module, which is similar to how we described the proposal in § 170.315(b)(11)(vii)(A) in the HTI–1 Proposed Rule (88 FR 23798).

We have also finalized in § 170.102, as proposed, the date for which the requirements of § 170.315(b)(11) must be satisfied for Health IT Modules to meet the definition of Base EHR. This means that proposed changes to the Base EHR definition in § 170.102 that would allow a Health IT Module to meet said definition if it has been certified to § 170.315(a)(9) or (b)(11) for the period up to and including December 31, 2024, and § 170.315(b)(11) on and after January 1, 2025, have been finalized as proposed. This also means that a developer of certified health IT with a Health IT Module certified to § 170.315(b)(11) must apply IRM practices for each Predictive DSI supplied by the health IT developer as described in § 170.315(b)(11)(vi) and submit summary information of their IRM practices to its ONC–ACB via publicly accessible hyperlink according to § 170.523(f)(1)(xxi) before December 31, 2024. We note that we have finalized, as discussed in section III.C.5.a.xiv, that the adoption of the criterion at § 170.315(a)(9) for purposes of the ONC Health IT Certification Program expires on January 1, 2025.

Together, these modifications reflect feedback received from numerous interested parties and are in response to both their support and opposition to our proposals. They are also intended to simplify Program requirements and support practical implementation of the certification criterion by developers of certified health IT. We elaborate on the details of these and other finalized policies more fully in subsequent responses of this final rule.

a. Requirements for Decision Support Interventions (DSI) Certification Criterion

i. Structural Revisions and New Criterion Categorization

We proposed at 88 FR 23782 through 23783 to adopt the certification criterion ''decision support interventions,'' (DSI) in § 170.315(b)(11) as a ''revised certification criterion'' according to the

proposed definition in § 170.102. The proposed criterion in § 170.315(b)(11) was a revised version of 45 CFR 170.315(a)(9), ''clinical decision support (CDS).'' In § 170.315(b)(11), we proposed to adopt a substantially similar structure as is currently in § 170.315(a)(9). In the revised certification criterion at § 170.315(b)(11), we proposed to modify the existing requirements in § 170.315(a)(9) to reflect an array of contemporary functionalities, data elements, and software applications that certified Health IT Modules support to aid decision-making in healthcare. We proposed that the policies established in § 170.315(a)(9)(i) through (iv) would be included as § 170.315(b)(11)(i) through (iv) with modifications. We proposed to introduce a new intervention type in § 170.315(b)(11), Predictive DSIs, with a corresponding definition in § 170.102 for the term.

At 88 FR 23782, we discussed our rationale for these proposals and stated our view that proposed § 170.315(b)(11) reflected functionality that is better categorized as part of the ''care coordination certification criteria,'' as opposed to the ''clinical certification criteria,'' supported by the Program. Hence, we proposed to adopt the ''decision support intervention'' certification criterion in the ''care coordination criteria'' section adopted within § 170.315(b).

At 88 FR 23783, we proposed modifications to the Base EHR definition in § 170.102 to identify the dates when § 170.315(b)(11) would replace § 170.315(a)(9) in the Base EHR definition. In keeping with the proposal to modify the Base EHR definition in § 170.102, we proposed that the adoption of § 170.315(a)(9) as part of the Program would expire on January 1, 2025. We noted that if we finalized these proposals, developers of certified health IT with Health IT Modules certified to § 170.315(a)(9) would need to certify those Health IT Modules to § 170.315(b)(11) in order for those Health IT Modules to continue to meet the Base EHR definition. Lastly, as a consequence of the proposed adoption of this criterion in § 170.315(b), we noted that developers of certified health IT with Health IT Module(s) certified to § 170.315(b)(11) would be required to submit real world testing plans and corresponding real world testing results, consistent with § 170.405.

Comments. Commenters' support was split with respect to the proposal to adopt the certification criterion naming update of ''decision support interventions,'' or DSI, for § 170.315(b)(11) as a ''revised certification criterion'' of 45 CFR 170.315(a)(9), ''clinical decision support'' (CDS). Commenters in support noted that the proposal would promote greater trust in DSI and predictive models through the Program. Commenters stated that distinguishing between CDS and DSI was warranted and that with the technological advancements in predictive analytics, AI, and machine learning, the certification criterion needed to be updated to better reflect the market, and our proposal reflected contemporary and emerging functions, uses, and data elements. Commenters who did not support the proposal recommended against renaming clinical decision support to decision support interventions because they stated the term ''intervention'' has other meanings within healthcare. Commenters suggested that retaining the name ''clinical decision support'' aligns better with the clinical decision support included in the legislative definition of a *qualified electronic health record.*

Response. We appreciate commenters' support for our proposal and agree that revising the existing CDS criterion in § 170.315(a)(9) as the DSI criterion in § 170.315(b)(11) is reflective of how decision support relies on increasing technological advancements in predictive analytics, AI, and machine learning. We agree the Program should be updated to reflect these advancements. While we appreciate the concerns raised regarding renaming the criterion from Clinical Decision Support to Decision Support Interventions, we note that the term ''evidence-based decision support intervention,'' has been part of the Program for nearly a decade, and we believe that removing ''clinical'' reflects the reality that Health IT Modules already support a broad array of decision support beyond what has been traditionally considered CDS. We also believe that the DSI criterion will continue to support the legislative definition of a *qualified electronic health record* as it has since the inception of the Program. We note our discussion of the term ''intervention'' was described in 88 FR 23786 and that the Program's use of the term ''intervention'' is different from ''clinical intervention'' as defined under FDA regulation that includes a range of regulated products, such as a medication or medical device. We discuss the term ''intervention'' in more detail in subsequent responses.

Comments. Several commenters suggested that ONC make Predictive DSI support a separate certification criterion from the existing ''clinical decision support'' criterion to better facilitate it being on a more extended timeframe for implementation and potentially impacting different products, whereas other commenters were supportive of revising the criterion to account for the rapid changes in this area of health IT.

Response. We appreciate the comments, but we decline to create a separate certification criterion for Predictive DSIs. We believe that the current structure of the CDS criterion in § 170.315(a)(9) is suitable to be implemented in a revised version in § 170.315(b)(11) and that this approach is more straight-forward than having substantially similar yet separate criteria. We have not extended the timeframe for implementation from what we proposed because many of the capabilities we have finalized in § 170.315(b)(11) are substantially similar to what already exists in § 170.315(a)(9) and because we have made other corresponding scope adjustments to the finalized certification criterion. We agree with commenters who note that technology is changing rapidly and there is a need for these policies to be implemented on a more accelerated timeline from other requirements in the HTI–1 Proposed Rule.

After consideration of these comments, we have finalized our proposal to adopt the ''DSI certification criterion'' in § 170.315(b)(11) as a ''revised certification criterion'' according to the proposed definition in § 170.102 and as part of the ''care coordination certification criteria,'' in § 170.315(b), including paragraph (b)(11)(i), which remains unchanged from paragraph (a)(9)(i). We have also finalized inclusion of the certification criterion at § 170.315(b)(11) as part of the Base EHR definition in § 170.102, and that beginning January 1, 2025, the certification criterion at § 170.315(a)(9) would not be included in that definition. Among the numerous standards and certification criteria proposed for revision by the end of 2024, the certification criterion in § 170.315(b)(11) has been prioritized and finalized on the proposed timeline. Based on public comment, we have lengthened the implementation timeline for nearly every other standard and certification criterion proposed in the HTI–1 Proposed Rule, as well as made other timing adjustments that could impact prioritization for § 170.315(b)(11). We believe these final rule updates will give developers of certified health IT time to focus on implementing the DSI criterion at § 170.315(b)(11).

Finally, as we noted in the HTI–1 Proposed Rule (88 FR 23783), as a consequence of adopting this revised

criterion in § 170.315(b), developers of certified health IT with Health IT Module(s) certified to § 170.315(b)(11) are required to submit real world testing plans and corresponding real world testing results, consistent with § 170.405, demonstrating the real world use of each type of DSI in § 170.315(b)(11), including evidence-based DSIs and Predictive DSIs. Finally, as we noted in the HTI–1 Proposed Rule (88 FR 23783), as a consequence of adopting this revised criterion in § 170.315(b), developers of certified health IT with Health IT Module(s) certified to § 170.315(b)(11) are required to submit real world testing plans and corresponding real world testing results, consistent with § 170.405, demonstrating the real-world use of each type of DSI in § 170.315(b)(11), including evidence-based DSIs and Predictive DSIs.

ii. Decision Support Configuration

At 88 FR 23783, we proposed in § 170.315(b)(11)(ii) to establish ''decision support configuration'' requirements based on what is currently in § 170.315(a)(9)(ii) with modifications and additional requirements. To reflect ONC's focus on the USCDI and to acknowledge the varied data for which DSIs may be enabled, we proposed that data elements listed in § 170.315(b)(11)(ii)(B)(*1*)(*i*) through (*iii*) and (*v*) through (*viii*) be expressed according to the standards expressed in § 170.213, including the proposed USCDI v3. We proposed to reference the USCDI in § 170.315(b)(11)(ii)(B)(*1*) to define the scope of the data ''at a minimum.'' We noted the intention was to establish baseline expectations that Health IT Modules certified to § 170.315(b)(11) must be capable of supporting DSIs that use those data elements listed in § 170.315(b)(11)(ii)(B)(*1*). We did not propose to establish requirements for specific interventions to be supported, only that Health IT Modules certified to § 170.315(b)(11) be capable of supporting interventions that use those listed data elements. This proposed requirement was framed to pertain to both evidence-based DSIs and Predictive DSIs that would be enabled by or interfaced with a certified Health IT Module, including any Predictive DSIs that were developed by users of the certified Health IT Module. We proposed to adopt in § 170.315(b)(11) the existing reference in § 170.315(a)(9)(ii)(B)(*1*)(*iv*) to demographic data in § 170.315(a)(5)(i).

Additionally, at 88 FR 23783 we proposed to include two USCDI data classes not currently found in § 170.315(a)(9)(ii)(B)(*1*). In § 170.315(b)(11)(ii)(B)(*1*)(*vii*)–(*viii*), we proposed to include the Unique Device Identifier(s) for a Patient's Implantable Device(s) and Procedures data classes, respectively, as expressed in the standards in § 170.213, including the proposed USCDI v3. We proposed to require that Health IT Modules would support data from the Procedures data class and the Unique Device Identifier(s) for a Patient's Implantable Device(s) data class as an input to DSIs. We invited comment on the additional data classes described in § 170.315(b)(11)(ii)(B)(*1*)(*vii*).

At 88 FR 23784, we proposed to adopt in § 170.315(b)(11)(ii)(C) a new functionality to enable users to provide electronic feedback data based on the information displayed through the DSI. We proposed that a Health IT Module certified to § 170.315(b)(11) must be able to export such feedback data, including but not limited to the intervention, action taken, user feedback provided (if applicable), user, date, and location, so that the exported data could be associated with other relevant data.

At 88 FR 23784, we proposed that such feedback data be available for export by users for analysis in a computable format, so that it could be associated with other relevant data. We noted that ''computable format,'' was consistent with current requirements in § 170.315(b)(10)(i)(D) for EHI Export, and we clarified that ''computable format'' is also referred to as ''machine readable,'' in other contexts, which is not synonymous with ''digitally accessible.'' [87] We did not propose to require specific formatting requirements for such feedback mechanisms.

Comments. The majority of commenters expressed support for the proposal to define the scope of data and supported the inclusion of USCDI v3 as the minimum set of data that should be included stating that defining data elements according to the USCDI v3 standard would have the benefit of improving transparency and increasing accuracy. Commenters recommended ONC support alignment efforts with standards development organizations (SDOs) and convene listening sessions with DSI developers to align reporting efforts and to understand the appropriate minimum base sets of data for DSI technology. One commenter expressed concern that the proposal to include USCDI v3 data elements was unclear and requested ONC clarify whether a Health IT Module must support these data elements so external DSI solutions can be integrated. One commenter expressed concern that the proposal for the data to be expressed in the standards in § 170.213 was unclear and recommended including USCDI data elements individually within the criterion for clarity on which elements would be required.

Response. We thank commenters for their support and feedback received during the public comment period, and we have finalized several proposals based on such feedback. We thank the commenter for expressing their concern regarding our proposals to include the USCDI v3. We did not propose to establish requirements for specific interventions to be supported, only that Health IT Modules certified to § 170.315(b)(11) be capable of supporting interventions that use those listed data elements (88 FR 23783). The criterion at § 170.315(a)(9)(ii)(B)(*1*) listed many of the same types of information, such as medications for example, but the criterion at § 170.315(a)(9) did so without specifying a standard. As the result of our finalizing references to the standards in § 170.213, we have provided clarity and better alignment with other certification criteria in the Program. We appreciate the suggestion that we work with SDOs and coordinate listening sessions with DSI developers. We will take these suggestions under consideration for future work, including potential future workshops, listening sessions, and advisory group task forces.

We have finalized § 170.315(b)(11)(ii)(A) with a minor modification to remove ''(*e.g.,* system administrator)'' from that provision (which is also in existing regulation text at § 170.315(a)(9)(ii)(A)), as this example is unnecessary. We have also finalized the list of data elements proposed at § 170.315(b)(11)(ii)(B)(*1*) with the following modifications in consideration of comments. We have moved the list from proposed § 170.315(b)(11)(ii)(B)(*1*) and finalized the list at § 170.315(b)(11)(iii)(A)(*1*) and finalized the list as proposed. We have finalized the list of data elements in § 170.315(b)(11)(iii)(A)(*1*) because they establish a scope for evidence-based DSIs that must be supported by Health IT Modules certified to § 170.315(b)(11) as well as scope the evidence-based DSIs that are subject to requirements in § 170.315(b)(11)(v). Including the list in § 170.315(b)(11)(iii)(A)(*1*) is intended to make this connection clearer.

We note that elsewhere in this final rule we have finalized an expiration date in § 170.213 for USCDI v1 to occur on January 1, 2026. Consistent with the applicable dates for the versions of the

[87] See also 85 FR 25879 discussion of machine readable.

USCDI in § 170.213, this means Health IT Modules certified to § 170.315(b)(11) need only support the listed data elements according to the USCDI v1 standard until this time. A Health IT Module certified to § 170.315(b)(11) may support the data elements according to the USCDI v3 standard adopted in § 170.213 as of the effective date of this final rule. On and after January 1, 2026, Health IT Modules certified to § 170.315(b)(11) must support those listed data elements according to the USCDI v3 standard consistent with § 170.213.

We have also finalized § 170.315(b)(11)(ii)(B)(*2*) as § 170.315(b)(11)(ii)(B) due to the corresponding shift of the list of evidence-based DSI-related data elements noted above. We did not propose any changes to § 170.315(b)(11)(ii)(B) in transposing the proposed regulatory text from the regulation text at § 170.315(a)(9)(ii)(B)(*2*), and we have finalized regulation text proposed at § 170.315(b)(11)(ii)(B)(*2*) using existing language found at § 170.315(a)(9)(ii)(B)(*2*) at § 170.315(b)(11)(ii)(B).

Comments. Commenters generally expressed support for the proposal at § 170.315(b)(11)(ii)(C) to enable users to provide electronic feedback based on the information displayed through the DSI and applauded including human-readable display. However, there was concern among many commenters regarding the details of this proposal, including requirements that Health IT Modules must be able to export feedback data, including but not limited to the intervention, action taken, user feedback provided (if applicable), user, date, and location, so that the exported data can be associated with other relevant data. These concerns were generally related to how these requirements would impact usability, user interfaces, and ongoing innovation of decision support tools. Specific commenters noted that capturing the ''action taken,'' by a user would be particularly problematic and would degrade DSI to simple ''yes/no'' designs.

Commenters suggested that we should limit the requirements to DSIs directly implemented by a developer of certified health IT and limit the requirements to interruptive alerts, because passive alerts cannot have associated user actions. Other commenters recommended the functionality to enable ''feedback loops'' be optional for users and that the requirement pertain to evidence-based DSIs exclusively.

Response. We appreciate the comments and thank commenters for their recommendations. We noted in the HTI–1 Proposed Rule that this is the second time we have proposed a functionality that would require a Health IT Module to enable a user to provide electronic feedback, also referred to as the capability to support ''feedback loops,'' on the performance of DSIs implemented at the point of care (88 FR 23783). We note that in our 2015 Edition Proposed Rule, we proposed to adopt new functionality that would require a Health IT Module certified to the CDS criterion in § 170.315(a)(9) to be able to record at least one action taken, and by whom it was taken, when a CDS intervention is provided to a user (*e.g.,* whether the user viewed, accepted, declined, ignored, overrode, provided a rationale or explanation for the action taken, took some other type of action not listed here, or otherwise commented on the CDS intervention) (80 FR 16821). At the time, many commenters stated that current systems already provided a wide range of functionality to enable providers to document decisions concerning CDS interventions and that such functionality was unnecessary to support providers participating in the EHR Incentive Programs (80 FR 62622). However, subsequent research over the last seven years indicates that ''feedback loop'' functionality is not widely available across Health IT Modules certified to the CDS criterion in § 170.315(a)(9), but that such functionality could be useful (88 FR 23784).

We appreciate the comments asking us to clarify to which DSI types our proposals would pertain. We agree with commenters who indicated that feedback loop functionality would be most appropriate for evidence-based DSIs. We have finalized § 170.315(b)(11)(ii)(C) to make clear that this functionality would only be required to apply to evidence-based decision support interventions. We decline to limit this functionality to interruptive alerts only, but we believe that interruptive alerts can be improved if user feedback data is applied to make such interruptions more meaningful.

While we are receptive to concerns regarding usability, we do not believe that the finalized requirements to enable a user to provide electronic feedback on evidence-based DSIs constrain or hinder usability or would lead to CDS degradation because this electronic feedback data can be gathered in ways that are non-disruptive to users and we believe our requirements are sufficiently flexible to enable a user to provide feedback in a manner appropriate to their workflow. Furthermore, we note that while Health IT Modules must support the capability at § 170.315(b)(11)(ii)(C) in order to demonstrate conformance to the certification criterion, a user still needs to choose to implement such functionality. A user would not be required to provide feedback; rather, the capability to enable a user to provide electronic feedback is what must be included within the Health IT Module.

We clarify that only evidence-based DSIs that are actively presented to users in clinical workflow to enhance, inform, or influence decision-making related to the care a patient receives must be supported by the ''feedback loop'' functionality described in § 170.315(b)(11)(ii)(C). We believe that scoping the requirement for feedback loops to these kinds of evidence-based DSIs would be both appropriate to the goal of enabling ongoing quality improvement of DSIs, as discussed on 88 FR 23784–23785, and feasible for Health IT Modules to support. We also clarify that a Health IT Module must be able to make available feedback data to a limited set of identified users for export in a computable format. This clarifies that while the Health IT Module must enable any user to provide electronic feedback, the Health IT Module is not required to export this feedback data to any user; rather, such an export of feedback data must be available to a limited set of identified users.

As it relates to concerns regarding the ''action taken,'' requirement, we note that the action taken will be specific to the intended use of the evidence-based DSI. Actions could include whether the user viewed, accepted, declined, ignored, overrode, or modified the DSI in some way. At this time, we decline to require an enumerated list of ''actions taken'' be supported. We believe that developers of certified health IT and their customers are better positioned to determine the range of actions that are appropriate as part of feedback data.

iii. Evidence-Based Decision Support Interventions

In the HTI–1 Proposed Rule, we proposed at 88 FR 23784 to establish ''evidence-based decision support interventions'' at § 170.315(b)(11)(iii), with a minor revision to current requirements that are part of the CDS criterion in § 170.315(a)(9)(iii). We explained that this proposal would replace the current construct in § 170.315(a)(9)(iii), which states a Health IT Module must enable evidence-based decision support interventions ''based on each one and at least one combination of'' the data referenced in paragraphs

§ 170.315(a)(9)(ii)(B)(*1*)(*i*) through (*vi*). We proposed that Health IT Modules supporting evidence-based DSIs must have the ability to support ''any,'' meaning all, of the revised data referenced in paragraphs of proposed § 170.315(b)(11)(ii)(B)(*1*)(*i*) through (*viii*). We noted this proposal would broaden the scope of data elements that Health IT Modules must support when enabling evidence-based DSIs to include 15 data elements expressed by the standards in § 170.213, including USCDI v3, which we proposed to adopt in § 170.213(b) elsewhere in the HTI–1 Proposed Rule. The HTI–1 Proposed Rule did not prescribe the intended use of the evidence-based DSI. Rather, the proposed subparagraph at § 170.315(b)(11)(iii), in combination with the data referenced in § 170.315(b)(11)(ii)(B)(*1*), represented the scope of evidence-based DSIs and scope of data that Health IT Modules certified to § 170.315(b)(11) should enable for purposes of certification under our Program.

Comments. Commenters were generally evenly split on their support for the proposal to establish ''evidence-based decision support interventions,'' with a minor revision to current requirements that are part of the CDS criterion in § 170.315(a)(9)(iii), with those in support noting that it would ensure that decision support systems are founded on the latest scientific research and clinical guidelines and assist healthcare professionals in making informed and effective choices that are supported by robust evidence. One commenter appreciated that we differentiated between predictive and evidence-based DSIs to support decision-making. One commenter noted that they believed it is critical that ONC account for the needs of clinical guideline developers so that undue burdens are not placed on the guideline development process as DSI tools are developed and implemented in part based on clinical guidelines.

Response. We appreciate these comments. We have finalized § 170.315(b)(11)(iii) with accompanying modifications and clarifications. As articulated in more detail in subsequent responses, we clarify that evidence-based DSIs, for purposes of requirements in § 170.315(b)(11), are limited to only those DSIs that are actively presented to users in clinical workflow to enhance, inform, or influence decision-making related to the care a patient receives and that do not meet the definition for Predictive Decision Support Intervention at § 170.102. Actively presented stands in contrast to decision support that initiates an action without a user's knowledge or occurs outside a user's normal workflow. We believe this clarification will help interested parties differentiate between evidence-based DSIs and Predictive DSIs and delineate which requirements in § 170.315(b)(11) pertain to these DSI types. We also note that some data elements in § 170.315(b)(11)(iii)(A) are not part of USCDI v1 and are only in USCDI v3. For the time period before the expiration date of USCDI v1, Health IT Modules are not required to support evidence-based DSIs that are based solely on data elements included in USCDI v3. However, beginning January 1, 2026, Health IT Modules must support DSIs based on all—meaning each—USCDI v3 data element listed in § 170.315(b)(11)(iii)(A).

Comments. Commenters not in support of the proposal expressed concern that the definition of *evidence-based DSI* was too broad and would encompass a large number of baseline functionality and capabilities within an EHR including passive and active alerts, order sets, care plans and protocols, simple rules and calculations, references ranges, age and weight based dosing and reminders for preventative care. Commenters sought more clarity related to how evidence-based and Predictive DSIs were defined and should be supported. Specifically, commenters noted concerns related to consistently determining what types of functionalities qualify as an evidence-based DSI, a Predictive DSI, or neither. Commenters also noted that EHRs support a vast number of financial and reimbursement rules to support medical necessity and reimbursement. The commenters recommended that the definition of evidence-based DSI align with the current § 170.315(a)(9) definition of clinical decision support and that the § 170.315(a)(9) certification criterion remain unchanged until future rulemaking can more clearly define the criterion and specific priority use cases beyond clinical.

Response. We thank commenters for their concerns and understand there is substantial confusion regarding the scope of what constitutes an evidence-based DSI as well as corresponding requirements for evidence-based DSIs in § 170.315(b)(11). In the HTI–1 Proposed Rule we included background information indicating that the initial CDS criterion, established in 2010, required that a Health IT Module could: (1) implement rules, ''according to specialty or clinical priorities;'' (2) ''automatically and electronically generate and indicate in real-time, alerts and care suggestions based upon clinical decision support rules and evidence grade;'' and (3) track, record, and generate reports on the number of alerts responded to by a user (75 FR 2046).'' (88 FR 23774). Since this time, the CDS criterion has remained agnostic to use case, except for drug-drug and drug-allergy contraindication checking, requiring Health IT Modules to enable the use of a variety of tools based on a specified set of data, including problems, medications, demographics, and laboratory data. While this framing has ensured that users have access to a broad range of tools, for a wide array of purposes, related to decision support through Health IT Modules certified to the CDS criterion, we now believe some clarity is needed to refine the scope of evidence-based DSIs for the purposes of requirements in § 170.315(b)(11).

We noted in the HTI–1 Proposed Rule that we were not establishing requirements for specific interventions to be supported, only that Health IT Modules certified to § 170.315(b)(11) be capable of supporting interventions based on specified data (as proposed in § 170.315(b)(11)(ii)(B)(*1*)(*i*) through (*viii*) (88 FR 23783)). We also noted in the HTI–1 Proposed Rule that the term ''intervention,'' [88] is specific to ''an intervention occurring within a workstream, including but not limited to alerts, order sets, flowsheets, dashboards, patient lists, documentation forms, relevant data presentations, protocol or pathway support, reference information or guidance, and reminder messages,'' (88 FR 23786).

Given the confusion conveyed through comments received from many interested parties regarding the scope of what decision support is considered evidence-based decision support, we clarify that for purposes of requirements in § 170.315(b)(11), evidence-based DSIs are limited to only those DSIs that are actively presented to users in clinical workflow to enhance, inform, or influence decision-making related to the care a patient receives and that do not meet the definition for Predictive DSI at § 170.102.[89] In the context of Program

[88] The ONC Program's use of the term ''intervention'' is different from ''clinical intervention'' as defined under FDA regulation that includes a range of regulated products, such as a medication or medical device. We note that there may be a software-as-a-medical device (SaMD) that is considered a ''clinical intervention'' and subject to FDA authority.

[89] We note that this clarification is aligned with FDA's Clinical Decision Support Software Guidance, specifically the software functionalities described under Criterion 3, which refers to condition-, disease-, or patient-specific recommendations to a health care professional to enhance, inform, or influence a health care decision. Note that we reference the FDA CDS Guidance only to clarify the scope of which kinds

requirements, this means that if a developer of certified health IT with a Health IT Module certified to § 170.315(b)(11) enables a user to select an evidence-based DSI that is actively presented in clinical workflow to enhance, inform, or influence decision-making related to the care a patient receives that evidence-based DSI would be subject to the requirements that apply to evidence-based DSIs within § 170.315(b)(11). We note that if the DSI in question meets the definition of Predictive DSI at § 170.102, then requirements that apply to those types of interventions within § 170.315(b)(11) would be applicable. Additionally, we clarify that ''actively presented,'' is inclusive of, but not limited to, ''interruptive alerts,'' and we clarify that ''related to the care a patient receives,'' would include use cases related to direct patient care as well as use cases that impact care a patient receives. For example, a decision support rule that recommends a follow-up appointment within 12 weeks according to United States Preventive Services Taskforce (USPSTF) recommendations would be considered an evidence-based DSI for purposes of Program requirements. These clarifications stand in contrast to back-end systems rules that are not presented to users and are not related to care an individual patient receives, such as those used for resource management or back-end logic that may support an organization's business rules but are not part of a user's workflow. Such rules and tools would not be considered an evidence-based DSI for the purposes of this certification criterion.

Beyond this clarification, we have finalized § 170.315(b)(11)(iii) by changing the title of the paragraph from proposed ''*Evidence-based decision support interventions,*'' to ''*Decision support intervention selection*'' and included explicit instruction for Health IT Modules to enable a limited set of identified users to select (*i.e.,* activate) decision support interventions (in addition to drug-drug and drug-allergy contraindication checking) that are evidence-based DSIs and Predictive DSIs. We have finalized the same requirement for all DSI types recognized in the Program, be they evidence-based DSIs or Predictive DSIs, because the technical capability to enable a user to select (*i.e.,* activate) is the same regardless of the type of DSI being activated. As described in more detail below, Program requirements to enable a user to select a DSI is contingent only on the data elements in § 170.315(b)(11)(iii)(A) (for evidence-based DSIs) and § 170.213 (for Predictive DSIs) and supportive of various use cases.

As discussed in more detail in the section III.C.5.v. ''Predictive Decision Support Interventions, Attestation for Predictive Decision Support Interventions,'' we did not adopt the Predictive DSI attestation statement proposed at § 170.315(b)(11)(v) in this final rule and we have narrowed the overall scope of technologies impacted by finalized requirements in § 170.315(b)(11). Given these changes, certain adjustments to the certification criterion were necessary to simplify, clarify, and align technical requirements that could be shared between evidence-based DSIs and Predictive DSIs. We believe these adjustments directly respond to commenter confusion and help reduce the technical updates that developers will need to complete in response to final requirements in § 170.315(b)(11) as they will be able to build on and extend existing capabilities to support Predictive DSIs. This is particularly true with respect to the capability expressed at final § 170.315(b)(11)(iii). Further, the alignment of evidence-based DSI and Predictive DSI capabilities will help provide for a consistent experience for those users identified to select DSIs pursuant to final § 170.315(b)(11)(iii).

While we specifically discussed evidenced-based DSIs in the HTI–1 Proposed Rule (88 FR 23784) with respect to proposed § 170.315(b)(11)(iii), we did not (aside from the paragraph title) expressly limit the scope of the proposed regulation text to evidenced-based DSIs—instead focusing on ''electronic decision support interventions.'' Moreover, at 88 FR 23783, we noted that requirements proposed at § 170.315(b)(11)(ii) for DSI configuration ''would pertain to both evidence-based DSIs and predictive DSIs that are enabled by or interfaced with a certified health IT Module, including any predictive DSIs that are developed by users of the certified Health IT Model.'' We have addressed these ambiguities in finalized regulation text at § 170.315(b)(11)(iii) and appreciate the comments that sought more clarity related to the shared uses expected for certification for evidence-based and Predictive DSIs.

We note that the capability in § 170.315(b)(11)(iii) is consistent with the historic and current expectation for evidence-based DSIs in § 170.315(a)(9)(iii) and we reiterate that this capability does not require a developer of certified health IT with a Health IT Module certified to § 170.315(b)(11) to author, develop, or otherwise support a specific evidence-based DSI or Predictive DSI.

Comments. One commenter suggested that ONC reconsider including Unique Device Identifier(s) for a Patient's Implanted Devices as a required element, or alternatively recognize that any DSI around Unique Device Identifier(s) is likely to only use certain elements of the Unique Device Identifier, not the full Unique Device Identifier—particularly the Device Identifier—and suggested that adoption as a required element for support via evidence-based DSIs is unnecessary at this stage.

Response. We appreciate the comment. We noted in the HTI–1 Proposed Rule that we believed that data regarding a patient's procedures and whether a patient has an implantable medical device, as indicated by a unique device identifier (UDI), can play a significant role in contemporary DSIs (88 FR 23783). As a result, we proposed to require that Health IT Modules would support data from the Procedures data class and the Unique Device Identifier(s) for a Patient's Implantable Device(s) data class as an input to DSIs. The addition of UDI complements medications and proposed procedures as an important focal point for various decision support interventions, including those related to MRIs, post-implant clinical care, among other care scenarios (88 FR 23783). We note that under this requirement, a Health IT Module would be required to enable an evidence-based DSI that included a UDI as expressed in the standards in § 170.213, and we clarify this requirement is affirmed regardless of whether the full UDI is part of the intervention or a component of the full UDI, such as the device identifier or the production identifier. Both identifiers are required to be supported as a part of USCDI v1 (§ 170.213(a)) and v3 (§ 170.213(b)).[90]

Comments. One commenter requested clarification on whether algorithms that use patient medical/demographic information to provide patient-specific screening, counseling, and preventive recommendations by mapping to well-known and established authorities are considered evidence-based DSI unless there is a ''predicted value.'' The commenter questioned if scenarios where the algorithm is calculating a risk

of evidence-based DSIs are subject to applicable requirements in § 170.315(b)(11). See *https://www.fda.gov/regulatory-information/search-fda-guidance-documents/clinical-decision-support-software.*

[90] *https://www.healthit.gov/isa/uscdi-data-class/unique-device-identifiers-a-patients-implantable-devices#uscdi-v1.*

value based on a pre-defined deterministic clinical guideline are included.

Response. We appreciate the opportunity to clarify this point. We note that to be considered a Predictive DSI, a function or technology must meet all parts of the definition in § 170.102. Namely, it must support decision-making based on algorithms or models that derive relationships from training data and then produce an output that results in prediction, classification, recommendation, evaluation, or analysis. Based on the information presented by this commenter, we do not believe a risk score based on a deterministic clinical guideline would be considered a Predictive DSI. Rather, this would be considered an evidence-based DSI. However, we note that whether a technology meets the definition of Predictive DSI is fact based, and this response should not be understood as determinative.

Comments. One commenter noted that for non-predictive CDS certified to existing ONC standards, the new transparency requirements related to patient demographics, social determinants of health, and health status assessments would be difficult to implement as such information is often not available to the CDS developer and recommended that ONC not require this for certified CDS but encourage it when such information is available.

Response. We appreciate the comment and we note that our requirements for evidence-based DSIs related to source attributes is substantially unchanged from the existing requirements. We describe in more detail our final policy for source attributes in the section ''vi. Source Attributes.'' However, we will require that users can review whether and which patient demographics, social determinants of health, and health status assessments data are used as part of an evidence-based DSI.

iv. Linked Referential CDS

At 88 FR 23784, we proposed to replicate what is currently in § 170.315(a)(9)(iv) as § 170.315(b)(11)(iv) with a modification to reference the criterion in § 170.315(b)(11) wherever the current reference is to § 170.315(a)(9). We welcomed comment regarding the functionalities and standards listed in § 170.315(a)(9)(iv), the HL7 Context Aware Knowledge Retrieval Application (''Infobutton'') standards, including whether linked referential CDS were commonly used with, or without, the named standards in § 170.315(a)(9)(iv)(A)(*1*) and (*2*) and whether we should continue to require use of these standards.

Comments. The majority of commenters were in support of removing the linked referential CDS provisions from the scope of the criterion, noting that it emphasizes the shift in focus to AI and machine learning-based DSI technology and removes a requirement that has been of little value for health care providers. In particular, commenters were supportive of removing the HL7 Context Aware Knowledge Retrieval Application (''Infobutton'') standards from the scope of the criterion, noting that removal is appropriate because there is low utilization for this standard, there is significant expansion of the proposed criterion in the areas of evidence-based and Predictive DSI, it would help streamline the certification process, and that customers perceive it as lacking value to clinical workflow in favor of traditional evidence-based CDS interventions. However, one commenter strongly supported retention of the ''Infobutton'' standard for linked referential DSIs but did not provide a rationale.

Response. We thank commenters for their recommendations. We agree with commenters that ''infobuttons,'' while helpful and useful in some contexts, no longer need to be mandated as part of the revised criterion at § 170.315(b)(11). We also note that the ''infobutton'' standard has not been updated for several years (since 2014). As part of an effort to streamline and update the historic criterion at § 170.315(a)(9), we have finalized § 170.315(b)(11) without proposed paragraph (b)(11)(iv) Linked referential DSI and associated subparagraphs. We anticipate that ''infobuttons'' and other linked referential DSIs will continue to be used where they provide value without a requirement in the Program. We believe that removal of this requirement as part of the revised certification criteria at § 170.315(b)(11) will reduce overall burden and focus requirements on evidence-based and Predictive DSIs.

Comments. One commenter was supportive of our proposal to include ''linked referential DSIs'' in the Program, noting that it has the advantage of equipping health care providers with comprehensive and up-to-date resources, thus empowering them to make well-informed decisions by drawing upon a wealth of knowledge and clinical expertise, ultimately improving patient outcomes.

Response. We appreciate the commenter's support for the requirement. However, we have finalized § 170.315(b)(11) without requiring ''Linked referential DSIs.'' We reiterate that in circumstances where linked referential DSIs and ''infobuttons'' are providing value, nothing in this final rule would inhibit their use. Furthermore, nothing in this final rule should be used to inhibit the use of diagnostic and therapeutic reference information or any associated bibliographic information that is part of the linked referential DSI.

v. Predictive Decision Support Interventions

We proposed at 88 FR 23784 to reference a new intervention type, ''predictive decision support intervention,'' in § 170.315(b)(11)(v), and we proposed a corresponding definition in § 170.102. We also proposed in § 170.315(b)(11)(v)(A) that developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) attest ''yes'' or ''no'' as to whether their Health IT Module enables or interfaces with one or more Predictive DSIs based on any of the data expressed in the standards in § 170.213, including USCDI v3, which we also proposed at 88 FR 23746.

Definition of Predictive Decision Support Intervention

We proposed at 88 FR 23784–23785 a definition of ''predictive decision support intervention,'' (again hereafter referenced as Predictive DSI) in § 170.102 to mean ''technology intended to support decision-making based on algorithms or models that derive relationships from training or example data and then are used to produce an output or outputs related to, but not limited to, prediction, classification, recommendation, evaluation, or analysis.'' We explained that such Predictive DSIs are based on the use of predictive model(s), and that ''model'' refers to a quantitative method, system, or approach that applies statistical, economic, bioinformatic, mathematical, or other techniques (*e.g.,* algorithm or equations) to process input data into quantitative estimates. We also discussed our use of the phrase ''intended to support decision-making'' to be interpreted broadly and to encompass technologies that require users' interpretation and action to implement as well as those that initiate patient management without user action and require action to contest. We also noted that our use of Predictive DSI was not tied to who developed it, the level of risk or degree to which the Predictive DSI informs or drives treatment, is relied upon by the user, relates to time sensitive action, or whether the Predictive DSI is augmentative or

autonomous.[91] We differentiated Predictive DSIs as those that support decision-making by learning or deriving relationships to produce an output, rather than those that rely on pre-defined rules based on expert consensus, such as computable clinical guidelines, to support decision-making.

We noted in the HTI–1 Proposed Rule that our definition of Predictive DSI was intended to cover a wide variety of techniques from algebraic equations to machine learning and natural language processing (NLP) (88 FR 23785). We mentioned the Acute Physiology and Chronic Health Evaluation IV (APACHE IV) model, which predicts in-hospital mortality for patients in intensive care units and was initially trained and validated with data from 45 hospitals, including over 100,000 individuals in 2006 (88 FR 23785). We also mentioned that models designed to estimate risk of a first Atherosclerotic Cardiovascular Disease, trained and validated on pooled cohorts of large studies as examples of common and in-scope models for our definition of Predictive DSI. We also noted that more complex models, for instance ones developed by combining multiple algorithms or deep neural networks trained and validated on over ten thousand individuals, that can be applied to patients in operational contexts would meet the proposed definition. So too would our definition include models that were adaptive, online or unlocked, which continue to adapt when exposed to new data, as well as those that are locked to the relationships learned in training data.

As proposed in § 170.102, the definition of Predictive DSI would not include simulation models that use modeler-provided parameters rather than training data or unsupervised machine learning techniques that do not predict an unknown value (*i.e.,* are not labeled) (88 FR 23786). For instance, the use of an unsupervised learning model within decision support would not meet our definition of Predictive DSI, nor would the use of developer-supplied parameters to simulate operating-room usage and develop an effective scheduling strategy. We refer readers to 88 FR 23784–23786 for the discussion on the definition of Predictive DSI.

Comments. Commenters were mixed in their support for the proposed definition of Predictive DSI, with those in support noting that it provides broad flexibility, comprehensively encompasses AI, and accurately highlights its distinction from any other potential sources of decision support interventions that do not involve modeling. Some commenters expressed support particularly for including complex predictive models leveraging machine learning in the proposed definition, noting that this recognition serves as a necessary step to combat bias and promote equity amid the growing number and increased use of AI tools.

While many commenters broadly supported the intent and goals of the proposed definition for Predictive DSI, other commenters expressed concern that the proposed definition was too broad and should be narrowed in several ways to provide clarity on the scope of technologies covered to prevent burden on health IT developers and health care providers. Other commenters noted that a broad definition of Predictive DSI creates confusion for what technology must be scoped for certification. Notably, many commenters suggested revising the definition to clarify that Predictive DSI means technology intended to support *clinical* or *medical* decision-making to ensure organizational and administrative decision making are excluded from the definition to limit the documentation requirements to demonstrate compliance and limit the number of citations in the system to alleviate user burden. For instance, one commenter suggested that ONC add the term ''clinical'' so that Predictive DSI means ''Predictive decision support intervention means technology intended to support clinical decision-making based on algorithms or models that derive relationships from training or example data and then are used to produce an output or outputs related to, but not limited to, prediction, classification, recommendation, evaluation, or analysis.'' Commenters recommended that the definition be limited to high risk DSIs, and that it should exclude certain health care providers, such as those that develop their own DSI and do not make it commercially available. Commenters also requested that we reconsider the proposals to apply a more limited scope that centers on functionality that necessitates the granular transparency of source attributes and feedback capabilities for end-users that ONC proposed.

Response. We appreciate the support from those commenters that said our definition comprehensively encompasses AI, and accurately highlighted the definition's distinction from any other potential sources of decision support interventions that do not involve modeling. We sought to establish a definition that was both broad and appropriate. Consistent with our rationale to move from CDS to DSI in Program nomenclature, we sought to establish a definition that encompassed the broad forms that algorithm and model-based decision support interventions can take and for which transparency regarding the performance of that model would benefit users, and would help users determine whether the technology they are using is fair, appropriate, valid, effective, and safe. We also sought to establish a definition that did not include a range of simple alerts and functions that would not benefit from the sorts of transparency our requirements would portend. However, we note there are many recent examples[92] [93] [94] where the task of delineating between those predictive algorithms and models can have unintended consequences.

We thank commenters for their critiques of our definition. Many commenters said that our definition was too broad, and a small minority of these commenters offered specific suggestions on how to reduce the scope of our definition. We thank those commenters, especially. We understand that many algorithms not directly supporting medical decision making can nevertheless impact the delivery of healthcare (*e.g.,* algorithms supporting scheduling or the provision of supplies), and so have not sought to limit the definition to models specifically informing medical decision making. Overall, we found that many other commenters did not consider our definition for Predictive DSI as a whole; rather, these commenters chose to isolate certain phrases or aspects of the

[91] *See generally* IMDRF | Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations: *https://www.imdrf.org/documents/software-medical-device-possible-framework-risk-categorization-and-corresponding-considerations.*

See AMA | CPT® Appendix S: Artificial Intelligence Taxonomy for Medical Services and Procedures: *https://www.ama-assn.org/system/files/cpt-appendix-s.pdf* for definitions of ''augmentative'' and ''autonomous''; ANSI/CTA Standard, The Use of Artificial Intelligence in Health Care: Trustworthiness ANSI/CTA–2090: https://shop.cta.tech/collections/standards/products/the-use-of-artificial-intelligence-in-healthcare-trustworthiness-cta-2090?_ga=2.195226476.1947214965.1652722036-709349392.1645133306.

[92] Samorani M., Harris S.L., Blount L.G., et al (2021) Overbooked and Overlooked: Machine Learning and Racial Bias in Medical Appointment Scheduling. Manufacturing & Service Operations Management 24(6):2825–2842. *https://doi.org/10.1287/msom.2021.0999.*

[93] Vyas D.A., Eisenstein L.G., Jones D.S. Hidden in Plain Sight—Reconsidering the Use of Race Correction in Clinical Algorithms. Aug. 2020. N Engl J Med 2020; 383:874–882. DOI: 10.1056/NEJMms2004740.

[94] Ziad Obermeyer et al., Dissecting racial bias in an algorithm used to manage the health of populations. Science 366, 447–453 (2019). DOI:10.1126/science.aax2342.

definition to question its scope and its applicability to specific use cases. As stated, our intention with the definition of Predictive DSI is to be expansive beyond the traditional role of CDS, yet appropriate to the dynamic technology environment that Predictive DSIs may be applied. Toward these two intentions, we noted in the HTI–1 Proposed Rule that we differentiate Predictive DSIs as those that support decision-making by learning or deriving relationships to produce an output, rather than those that rely on pre-defined rules to support decision-making (88 FR 23785). Taken alongside the rest of the definition, this distinction is intended to preclude the vast number of alerts or reminders that are either based on consensus clinical guidelines or bespoke business processes and organizational policies that may or may not be based on any guideline.

We also noted in the HTI–1 Proposed Rule that our definition is not tied to the level of risk (88 FR 23785) and our certification criterion for CDS was established to ensure that Health IT Modules support broad categories of CDS while being agnostic toward the intended use of the CDS beyond drug-drug and drug-allergy interaction checks (88 FR 23774). We did not propose to alter that construct in our proposals. However, we are sensitive to defining Predictive DSIs in a way that makes clear which technologies are in scope for § 170.315(b)(11).

We also decline to limit the definition to a specific source or developer of the intervention, although additional facets of the final policy define the applicable scope of § 170.315(b)(11).

We have finalized our proposed definition for Predictive DSI with modification. Specifically, we have finalized the definition in § 170.102 as follows: ''Predictive decision support intervention or Predictive DSI means technology that supports decision-making based on algorithms or models that derive relationships from training data and then produce an output that results in prediction, classification, recommendation, evaluation, or analysis.'' We note that this version of the definition is not markedly different from the definition we proposed, but we intend it to be more exacting. Thus, the examples and discussion regarding scope in the HTI–1 Proposed Rule remain relevant to this definition (88 FR 23784–23786). To help interested parties better understand the scope of technologies included in this definition we reiterate the following: The development process whereby models under this definition ''learn'' relationships in training data and then are used to generate an unknown label or value (via prediction, classification, recommendation, evaluation, or analysis) that is based on the ''learned'' relationships is a fundamental differentiator from evidence-based DSIs. While we appreciate commenters' request to limit or constrain the scope of the Predictive DSI definition based on its intended purpose or use (*e.g.,* clinical and medical versus administrative), level of risk (*e.g.,* high versus low), and entity or party that developed the technology (*e.g.,* health care provider that self-develops versus technology company that sells Predictive DSIs), we do not believe such an approach would be appropriate. We believe that the transparency requirements within this criterion are appropriate to all Predictive DSIs used within the context of certified health IT, given the potential of these Predictive DSIs to impact the delivery of healthcare at vast scale. We believe that constraining the definition of Predictive DSI by intended purposes, level of risk, or developing entity would create multiple layers of complexity and lead to different requirements for technology that may have qualities that pertain to one or more of these dimensions or exist along a spectrum of these concepts. We believe that a broad and consistently applied definition will improve the likelihood of achieving our stated goals for transparency and trustworthiness.

We note that the definition of Predictive DSI is aligned with and within the scope of the definition of Artificial Intelligence at 15 U.S.C. 9401(3), as used in E.O. 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (88 FR 75191). Predictive DSIs perceive environments through the use of training data; abstract perceptions into models as they learn relationships in that data; and produce an output, often for an individual, through inference based on those learned relationships. We further note that evidence-based DSI likely represents another form of Artificial Intelligence, though that form is fundamentally based on rules-based models.

We also clarify that the exclusion of unsupervised learning models discussed at 88 FR 23786 was intended to focus on models trained in data without labels. This exclusion reflected our understanding that it is not feasible to produce descriptions for many of the source attributes we are requiring for Predictive DSI. For example, unsupervised models are generally based on data without labels, which often generate measures of similarity or closeness of observations rather than a predicted value. In these instances, assessing the accuracy, validity and fairness of a prediction would be difficult, if not impossible, because the outcome is not specified. The exclusion of unsupervised learning models is embedded in the definition because the definition focuses on ''relationships in training data,'' which generally refers to the relationship between some set of data (sometimes referred to as inputs, features, or predictors) and an outcome or label (such as a diagnosis or the next word in a string). In contrast, unsupervised learning models rely more generally on patterns in data. We further clarified this exclusion in the HTI–1 Proposed Rule at 88 FR 23786 and maintain the exclusion in the final definition.

These unsupervised models contrast with LLMs and other forms of generative AI, which often leverage self-supervised learning wherein the data itself provides a label (*e.g.,* the next word in a string of text) and the model returns a predicted value of that label as output, in which case the accuracy, validity and fairness of a prediction can readily be assessed (although additional use-case specific evaluation may also be beneficial). Self-supervised learning models would therefore generally be included within the definition of Predictive DSI. We also note that LLMs and other forms of generative AI often use a combination of unsupervised, self-supervised, supervised and reinforcement learning, and those that include a component of supervised learning, including semi-supervised approaches, would likely meet the definition of Predictive DSI.

Finally, we understood that models that solely rely on unsupervised learning techniques are not widely deployed in healthcare today.[95] We will continue to monitor development of methodologies and applications of unsupervised learning to health-related use cases and may consider future rulemaking for these models as the field develops.

Comments. Several commenters expressed concern about consistency, duplication, and redundant requirements across various federal

[95] Michael Matheny, et al., *Artificial intelligence in health care: the hope, the hype, the promise, the peril,* Washington, DC: National Academy of Medicine (2019).

Artificial Intelligence in Health Care: Benefits and Challenges of Technologies to Augment Patient Care, (Nov. 2020), *https://www.gao.gov/products/gao-21-7sp*. Deo, Rahul C. ''Machine learning in medicine.'' *Circulation* 132.20 (2015): 1920–1930.

American Hospital Association. ''Surveying the AI Health Care Landscape'' 2019. *https://www.aha.org/system/files/media/file/2019/10/Market_Insights_AI-Landscape.pdf.*

programs. Commenters recommended that ONC tailor the scope of the proposed term Predictive DSI, and the proposed definition at § 170.102, to exclude FDA-authorized AI and machine learning medical devices to mitigate their concerns mentioned above. Specifically, one commenter recommended tailoring the Predictive DSI requirements to explicitly exclude tools that are regulated medical devices, to exclude third-party tools that qualify as non-device per the statutory exemption for CDS software, and, to apply only to technology developed by vendors of certified Health IT Modules to avoid unnecessary burdens on regulated device manufacturers. Commenters noted that our proposal for Predictive DSI could implicate CDS software that falls within FDA regulated medical devices which may have already been cleared, approved, or otherwise authorized for marketing within the United States.

Response. We appreciate the concerns expressed by these commenters, which is why we worked closely with the FDA on development of our proposals in § 170.315(b)(11). This collaboration included consultation with the FDA on the inclusion or exclusion of devices within FDA's authority in the definition of Predictive DSI. Specifically, we sought alignment with the FDA's recent Clinical Decision Support Guidance for Industry (CDS Guidance), finalized in September 2022,[96] and we note that our requirements in § 170.315(b)(11) are complementary to FDA's Content of Premarket Submissions for Device Software Functions guidance, finalized in June 2023.[97] This high degree of coordination will reduce burden on device manufacturers by establishing the potential that a device manufacturer that also develops a Predictive DSI can fulfill two separate federal agency's requirements with substantially similar or the same information.

We noted in the HTI–1 Proposed Rule that our authority to regulate developers of certified health IT under the Program is separate and distinct from other federal agencies' regulatory authorities focused on the same or similar entities and technology (88 FR 23811).[98] For example, the safety and effectiveness of a software function, including clinical decision support or other kinds of decision support interventions, is within the purview of FDA regulatory oversight, if such software functionality meets the definition of a ''device.'' [99] In the area of predictive technology, ONC and FDA support a harmonized and complementary approach, independent of the platform on which the technology operates, in accordance with our existing intersecting regulatory oversight. We also noted in the HTI–1 Proposed Rule that questions of whether DSIs enabled by or interfaced with certified health IT are subject to FDA regulations, under the Federal Food, Drug, & Cosmetic Act, or are used by entities subject to the HIPAA Rules, are separate and distinct from the question of whether a developer or a particular technology is subject to regulatory oversight by our Program, to which our proposals pertain (88 FR 23811).

We also anticipate that in a scenario where a Device CDS (this is a CDS with software functions) has been cleared, approved, or otherwise authorized for marketing by the FDA, this device's manufacturer will have ready access to much of the information necessary for it to comply with requirements in § 170.315(b)(11) as a developer of certified health IT.

We appreciate the suggestions to exclude from our definition for Predictive DSI software that are regulated medical devices and to exclude third-party software that qualify as non-device software functions per the statutory exemption for CDS software. However, we decline to include any exclusionary criteria in our definition for Predictive DSI, such as exclusions for specific types of functions or specific types of Predictive DSI developers because the finalized definition is appropriate to reflect the wide variety of predictive tools that impact and intersect with the delivery of healthcare. Also, whether or not a given technology or tool is a Predictive DSI should be consistent regardless of the developer of the tool. We also note—as stated above and previously in the HTI–1 Proposed Rule—that the FDA and ONC have separate and distinct authorities and regulate for separate and distinct purposes with separate and distinct policy objectives (88 FR 23811). Moreover, we stress the benefits that such alignment and coordination brings to users. Because of our requirements for source attributes in § 170.315(b)(11), users of both CDS with device software functions and Non-Device CDS will have easy access to important information at the point-of-care.

Comments. Several commenters requested we clarify the proposed definition of Predictive DSI by providing examples of use cases to show the application of the policy. One commenter recommended that ONC include a clear standard or definition as to which entities the HTI–1 Proposed Rule applied to, and which applications and tools are in scope for Predictive DSIs.

Response. We understand commenters' desire to have ONC assess whether specific algorithms, models, and technologies would meet the definition for Predictive DSI. in § 170.102. Rather than make specific assessments to these commenters' questions, we provide the following examples of technologies that would likely meet our definition for Predictive DSI and examples of technologies that would likely not meet our definition for Predictive DSI:

1. Models that predict whether a given image contains a malignant tumor or that predict patient reported pain based on an image, trained based on relationships observed in large data sets often using neural networks, would likely be considered Predictive DSIs.[100]

2. Models that pre-selected or highlighted a default order from an order set based on relationships in training data indicating that order was most likely to be selected would likely be considered Predictive DSIs.

3. Models that predict risk of sepsis, readmission (*e.g.,* LACE+), estimated glomerular filtration rate (eGFR), or risk of suicide attempt, which have been trained based on relationships observed in large data sets, often using logistic

[96] See *https://www.fda.gov/regulatory-information/search-fda-guidance-documents/clinical-decision-support-software.*

[97] See *https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-device-software-functions.*

[98] See U.S. Dept of Health & Human Servs., Office for Civil Rights, Notice of Proposed Rulemaking, Nondiscrimination in Health Programs and Activities, 87 FR 47824, 47880 (Aug. 4, 2022), *https://www.federalregister.gov/documents/2022/08/04/2022-16217/nondiscrimination-in-health-programs-and-activities* (prohibiting discrimination on the basis of race, color, national origin (including limited English proficiency), sex (including sexual orientation and gender identity), age, or disability in certain health programs or activities *through the use of clinical algorithms in their decision-making*).

[99] A device, as defined in section 201(h) of the FD&C Act, can include an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is, among other criteria, intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease in man. The term ''device'' does not include software functions excluded pursuant to section 520(o) of the FD&C Act. For more information about determining whether a software function is potentially the focus of the FDA's oversight, please visit the FDA's Digital Health Policy Navigator Tool: *https://www.fda.gov/medical-devices/digital-health-center-excellence/digital-health-policy-navigator.*

[100] Pierson, Emma, et al. ''An algorithmic approach to reducing unexplained pain disparities in underserved populations.'' *Nature Medicine* 27.1 (2021): 136–140. Hosny, Ahmed, et al. ''Artificial intelligence in radiology.'' *Nature Reviews Cancer* 18.8 (2018): 500–510.

regression and machine learning techniques, and are used to support decision making, would likely be considered Predictive DSIs.[101]

4. Indices and classification systems developed by expert consensus rather than in empirical data, such as the SOFA index and NYHA Heart Failure classification, would likely not be considered Predictive DSIs but are likely evidence-based DSI because the score is based on pre-defined rules and not relationships learned in training data.[102]

5. Models that generate clinical notes or draft clinical notes and that were trained based on relationships in large data sets of free text, including large language models, and support decision making about what to document in the clinical note, would likely be considered Predictive DSIs.

6. Models that use natural language processing to route secure messages, which were trained based on the relationship between message contents and the individual who responded to similar messages in the past would likely be considered Predictive DSIs.

7. Rules-based algorithms for routing secure messages based on the type of message, rather than relationships in training data, would likely not be considered Predictive DSIs.

8. Growth charts, for instance percentile calculations based on a lambda-mu-sigma transformation of similar age children's weights, with parameters learned in training data from a national sample of children, would likely not be considered Predictive DSIs because the underlying model is based on the distribution of a single variable (*e.g.,* weight) rather than a prediction based on relationships between variables.

9. A calculation for BMI would likely not be considered a Predictive DSI because the calculation (weight divided by height squared) is not based on relationships in training data.

10. Patient matching algorithms based on indices of similarities, rather than by relationships in training data where an outcome is known, would likely not be Predictive DSIs. Many of these technologies are most similar to unsupervised machine learning, which we described previously in this section and in the HTI–1 Proposed Rule at 88 FR 23786 as out of scope of the current definition of Predictive DSI.

11. Optical character recognition, used simply to make a PDF readable or searchable to end users, would likely not be considered Predictive DSI because it does not support decision-making.

Comments. Commenters were generally mixed on our mention of LLMs and other generative AI as in scope for the proposed definition of Predictive DSI in the HTI–1 Proposed Rule. Some commenters in support agreed with our assessment that the use of predictive models, such as AI, invariably present model risk that can lead to patient harm, bias, widening health disparities, discrimination, inefficient resource allocation decisions, or ill-informed clinical decision-making. Commenters stated LLMs and generative AI tools could pose risks if they are not deployed appropriately and monitored carefully and viewed our proposals as a necessary step to combat bias and promote equity amid the growing number and increased use of AI tools.

Other commenters expressed concern that LLMs, such as ChatGPT, would be covered in the proposed Predictive DSI definition, noting the definition could sweep in developers of general-purpose AI applications that enable or interface with Health IT Modules. One commenter noted that these models are fundamentally different than other Predictive DSI models, thus including these models in the same category as Predictive DSIs would be an inaccurate classification. Commenters were concerned that including LLMs could potentially limit their effective application in non-clinical aspects of healthcare software intended to help users save time and organizations save money and urged ONC to revise the definition so that developers of general-purpose AI applications are not obligated by the proposed requirements and instead that applications be evaluated within the context of a specific use case.

Response. In the HTI–1 Proposed Rule, we were explicit in describing the scope of our Predictive DSI definition to include large language models, or LLMs, and other forms of generative AI that meet the definition of Predictive DSI. We do not believe that LLMs should be excluded from our definition for Predictive DSI if the LLMs are used to support decision-making, nor do we believe that LLMs are complete ''black-boxes'' about which no information can be made available to users that would be valuable. We agree with commenters that LLMs could pose a risk if they are not deployed appropriately. We believe that the source attribute- and risk management-related requirements in this rule could help to decrease the likelihood that a model is inappropriately deployed in a Health IT Module in a way that exacerbates bias or poses other risks. We note that we have finalized a fundamentally limited the scope in § 170.315(b)(11) to focus on transparency capabilities and instances where Predictive DSIs (such as LLMs or other generative AI) are supplied by a developer of certified health IT—and not generally on LLMs or generative AI that may be used in the healthcare ecosystem. If, as part of its Health IT Module, a health IT developer supplies an LLM or other generative AI that meets the definition of Predictive DSI, the finalized policy in § 170.315(b)(11) requires the health IT developer's Health IT Module certified to § 170.315(b)(11) to enable access to complete and up-to-date plain language descriptions of source attribute information related to that Predictive DSI. Our finalized policy also requires Health IT Modules certified to § 170.315(b)(11) to, at a minimum, have the technical capability for users and *other parties* to populate the source attributes listed in § 170.315(b)(11)(iv) themselves. We agree with commenters that LLMs should be evaluated within the context of specific use cases and believe that the scope of this final rule will not limit the effective application of LLMs.

Regarding commenters' concerns about LLMs being fundamentally different and requiring different kinds of source attributes that are more fit for transparency purposes, we note that our requirements for source attributes represent a minimum ''floor,'' and developers of certified health IT are encouraged to provide additional source attributes to users as appropriate. We also describe in more detail in subsequent responses that we have finalized a requirement for Health IT Modules to enable a limited set of identified users to record, change, and access additional source attribute information not specified in § 170.315(b)(11)(iv)(B) of this final rule. This will enable users to identify source

---

[101] van Walraven, Carl, Jenna Wong, and Alan J. Forster. ''LACE+ index: extension of a validated index to predict early death or urgent readmission after hospital discharge using administrative data.'' *Open Medicine* 6.3 (2012): e80.

Levey, Andrew S., et al. ''A more accurate method to estimate glomerular filtration rate from serum creatinine: a new prediction equation.'' *Annals of internal medicine* 130.6 (1999): 461–470.

Walsh, Colin G., Jessica D. Ribeiro, and Joseph C. Franklin. ''Predicting risk of suicide attempts over time through machine learning.'' *Clinical Psychological Science* 5.3 (2017): 457–469.

Fleuren, Lucas M., et al. ''Machine learning for the prediction of sepsis: a systematic review and meta-analysis of diagnostic test accuracy.'' *Intensive care medicine* 46 (2020): 383–400.

[102] Vincent, J -L., et al. ''The SOFA (Sepsis-related Organ Failure Assessment) score to describe organ dysfunction/failure: On behalf of the Working Group on Sepsis-Related Problems of the European Society of Intensive Care Medicine (see contributors to the project in the appendix).'' (1996): 707–710.

attributes and record, change, and access those source attributes based on local validation and enable users to access emerging transparency measures specific to emerging Predictive DSI types, such as those based on LLMs.

Comments. One commenter expressed concern with the proposed definition including the term ''derive relationships from training or example data,'' stating that it is overly broad and unclear as to what would be considered in scope, such as whether general system improvements learned from user behavior would fall into this definition. The commenter also expressed concern with our preamble description that ''Predictive models are those that have 'learned' relationships from a training or historic data source, generally using some form of statistical or machine learning approach'' stating that it is unclear whether commonly used predictions (*e.g.,* LACE+ for readmission or a SOFA score) [103] are included in the definition of Predictive DSI. The commenter requested that the definition should be clarified to focus only on models that are generated from machine learning techniques and for the types of clinical predictions that are not commonly used in medical practice and clarified to focus on a prediction of an unknown or future clinical event.

Response. We appreciate the comment and the questions. We note that ''derive relationships from training data'' is only a part of the overall definition we have finalized. If a technology is used to make ''general system improvements'' based on training data that consists of ''user behavior,'' it may meet the definition of a Predictive DSI in § 170.102 if it derived relationships (for instance, correlations) from that training data and then produced an output that results in prediction, classification, recommendation, evaluation, or analysis used to support decision-making. ''General system improvements'' based on other analysis, such as tracking the time required to perform a task, would likely not meet the definition because that technology does not ''derive relationships.'' If ''general system improvements learned from user behavior,'' were the outputs of the technology or the effect of the technology, but that output was not used to support decision-making or was not a prediction, classification, recommendation, evaluation or analysis, then this technology likely would not meet our finalized definition.

We noted above in examples that the LACE+ model for readmission would likely meet the definition of Predictive DSI at § 170.102 and because the SOFA score was defined by expert consensus, rather than training data, this would not likely meet the definition of Predictive DSI at § 170.102. We note that in our finalized definition, we have removed ''or example'' and now only refer to ''training data,'' for clarity and because we do not believe there is an appreciable or impactful difference between training and example data. We respectfully decline to include any exclusionary criteria in our definition for Predictive DSI, including exclusions for specific types of functions or specific types of Predictive DSI developers.

Comments. Several commenters recommended that we revise the definition to take a tiered approach to DSI requirements based on the type and level of meaningful risk to patients associated with the AI systems, suggesting that we should focus on ''high-risk'' DSIs, remarking that it would help alleviate public confusion and suggesting that this approach would better meet the intent of addressing the risks associated with DSI. One commenter recommended that Predictive DSI should not apply to consumer-facing devices and low risk tools, noting that the public interest would not be served by imposing regulatory compliance obligations on low-risk Predictive DSI use cases—even when applied in a clinical context. For example, Predictive DSI tools used for non-clinical purposes (*e.g.,* EHR integrations for administrative notes and billing) do not present the sorts of risks that the HTI–1 Proposed Rule is intended to address. Along with clarifying that low-risk Predictive DSI tools are exempt, the commenter suggested that ONC should also issue guidance clarifying the types of proposed uses that are considered ''low-risk.''

Response. We noted in the HTI–1 Proposed Rule that our definition is not tied to the level of risk (88 FR 23785), and we decline to focus on ''high-risk'' DSIs. Doing so would diverge from established approaches within the CDS criterion. The certification criterion for CDS was established to ensure that Health IT Modules certified to the criterion support broad categories of CDS, including by making information about the CDS available for user review, while being agnostic toward the intended use of the CDS beyond drug-drug and drug-allergy interaction checks (88 FR 23774). We did not propose to alter that construct in our proposals, and we respectfully decline to do so in this final rule. We do not agree with commenters that a focus on ''high-risk'' DSIs would alleviate public confusion because defining and determining levels of risk for Predictive DSIs that, in some cases indirectly, impact the healthcare of millions of individuals is complex and requires consideration of numerous factors. Instead, the information required for Predictive DSI will be beneficial for all Predictive DSI supplied by developers of certified health IT.

We also decline to include any exclusionary criteria in our definition for Predictive DSI, including exclusions for specific types of functions, such as consumer-facing tools or other ''low risk'' tools, or for specific types of Predictive DSI developers. We note that non-clinical Predictive DSIs and clinical Predictive DSIs that may be categorized as of relatively low risk have consequences for and impact the care individuals receive, and as we have noted elsewhere, demonstrably negative impacts beyond clinical safety have been well-documented in various studies and academic literature in recent years.[104] Together, we believe these factors warrant a broad and inclusive definition for Predictive DSI.

Comments. Some commenters were concerned that due to the breadth of the definition, non-certified health IT would be included in the definition and believed the HTI–1 Proposed Rule should be limited to software that an EHR vendor submits for certification under the Program, noting that ONC's authority under the Program is limited to oversight of certified Health IT Modules and developers of certified health IT.

[103] Vincent, J.L., et al. ''The SOFA (Sepsis-related Organ Failure Assessment) score to describe organ dysfunction/failure: On behalf of the Working Group on Sepsis-Related Problems of the European Society of Intensive Care Medicine (see contributors to the project in the appendix).'' (1996): 707–710.

van Walraven, Carl, Jenna Wong, and Alan J. Forster. ''LACE+ index: extension of a validated index to predict early death or urgent readmission after hospital discharge using administrative data.'' Open Medicine 6.3 (2012): e80.

[104] Samorani M., Harris S.L., Blount L.G., et al (2021) Overbooked and Overlooked: Machine Learning and Racial Bias in Medical Appointment Scheduling. Manufacturing & Service Operations Management 24(6):2825–2842. *https://doi.org/10.1287/msom.2021.0999.*

Vyas D.A., Eisenstein L.G., Jones D.S. Hidden in Plain Sight—Reconsidering the Use of Race Correction in Clinical Algorithms. Aug. 2020. *N Engl J Med* 2020; 383:874–882. DOI: 10.1056/NEJMms2004740.

Ziad Obermeyer et al.,Dissecting racial bias in an algorithm used to manage the health of populations. *Science* 366, 447–453 (2019). DOI: 10.1126/science.aax2342.

Delgado, Cynthia, et al. ''A unifying approach for GFR estimation: recommendations of the NKF–ASN task force on reassessing the inclusion of race in diagnosing kidney disease.'' *Journal of the American Society of Nephrology* 32.12 (2021): 2994–3015.

Response. We acknowledge that the definition of Predictive DSI itself may have broad applicability. As part of 45 CFR part 170, any application of the definition (and the related requirements in § 170.315(b)(11)) is limited to certified Health IT Modules and developers who develop them. We note that our definition does not depend on or reference the certification status of the entity that developed the technology that may or may not be considered a Predictive DSI. We established the definition to be agnostic to both use case and party that develops a Predictive DSI, and we and have not chosen to finalize a definition with any such caveats. As described elsewhere in the rule, and to address these and related commenters' concerns, we have focused the scope of Predictive DSIs to which our regulatory requirements apply to those supplied by the developer of certified health IT as part of its Health IT Module. We noted in the HTI–1 Proposed Rule that our authority to regulate developers of certified health IT and their Health IT Modules, ensuring that both conform to technical standards, certification criteria, implementation specifications, and adherence to Conditions and Maintenance of Certification requirements, is separate and distinct from other federal agencies' authorities to regulate for separate and distinct purposes with separate and distinct policy objectives that may be focused on the same or similar entities and technology (88 FR 23809–23810), that may pertain to the use of Predictive DSIs and technology, including AI and machine learning, in health and human services.[105] Outside of the Department of Health and Human Services, multiple federal agencies, within their unique authorities, are exploring policies pertaining AI and machine learning (88 FR 23810).[106]

Comments. A few commenters expressed concern that our proposed definition does not add clarity and offered other examples of definitions that ONC should consider. For example, one commenter recommended ONC use public definitions of AI and include a neural net component for an adopted definition of Predictive DSI. Another commenter suggested ONC narrow the definition of Predictive DSI to focus on outputs that are recommendations and to limit the definition by removing the proposed ''. . . prediction, classification, evaluation or analysis'' section of the proposed definition. One

[105] *See, e.g.,* See U.S. Dept of Health & Human Servs., Office for Civil Rights, Notice of Proposed Rulemaking, Nondiscrimination in Health Programs and Activities, 87 FR 47824, 47880 (Aug. 4, 2022), *https://www.federalregister.gov/documents/2022/08/04/2022-16217/nondiscrimination-in-health-programs-and-activities* (prohibiting discrimination on the basis of race, color, national origin (including limited English proficiency), sex (including sexual orientation and gender identity), age, or disability in certain health programs or activities *through the use of clinical algorithms in their decision-making*).

CMS Medicare Advantage Program Final Rule (April 2023), *https://www.federalregister.gov/documents/2023/04/12/2023-07115/medicare-program-contract-year-2024-policy-and-technical-changes-to-the-medicare-advantage-program* (The rule clarified coverage criteria for basic benefits and the use of prior authorization, added continuity of care requirements, and required an annual review of utilization management tools).

[106] The Federal Trade Commission (FTC) has addressed AI repeatedly in its work through a combination of law enforcement, business education and policy initiatives. For example, numerous FTC orders have required companies to delete data and algorithms. *See* ''Amazon/Alexa'' case, *https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever* (settling allegations that Amazon retained children's voice recordings indefinitely to feed its voice recognition algorithm in violation of a children's privacy law); ''Ring'' case, *https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users* (settling allegations that home security company allowed employees to access consumers' private videos); ''Weight Watchers/Kurbo'' case, *https://www.justice.gov/opa/pr/weight-management-companies-kurbo-inc-and-ww-international-inc-agree-15-million-civil-penalty* (settling allegations that weight loss app for use by children as young as eight collected their personal information without parental permission); ''Everalbum'' case, *https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3172-everalbum-inc-matter* (settling allegations that the company deceived consumers about the use of facial recognition to analyze users' private images, including in connection with training FRT models); the ''Mole Detective'' case, *https://www.ftc.gov/legal-library/browse/cases-proceedings/132-3210-new-consumer-solutions-llc-mole-detective* (alleging deceptive conduct, where app developers claimed in advertisements that their consumer-facing app could determine based on photographs whether a mole was cancerous). In May 2023, the FTC issued a Policy Statement discussing the application of Section 5 of the FTC Act to the collection and use of biometric information (such as finger or hand prints, facial images or geometry, voice recordings, or genetic information), including the use of biometric information technologies developed using machine learning and similar techniques. Fed. Trade Comm'n, *Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act* (May 18, 2023), *https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf.* In November 2023, the FTC filed a comment with the Copyright Office on Artificial Intelligence. *See https://www.ftc.gov/legal-library/browse/advocacy-filings/comment-federal-trade-commission-artificial-intelligence-copyright.* FTC staff guidance has warned companies about their obligation to use AI responsibly and identified concerns from consumers and about competition. *See, e.g., Consumers Are Voicing Concerns About AI, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/10/consumers-are-voicing-concerns-about-ai* (October 3, 2023); *Watching the detectives: Suspicious marketing claims for tools that spot AI-generated content* (July 6, 2023); *https://www.ftc.gov/business-guidance/blog/2023/07/watching-detectives-suspicious-marketing-claims-tools-spot-ai-generated-content; Generative AI Raises Competition Concerns, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/06/generative-ai-raises-competition-concerns* (June 29, 2023); *Hey, Alexa! What are you doing with my data?* (June 13, 2023), *https://www.ftc.gov/business-guidance/blog/2023/06/hey-alexa-what-are-you-doing-my-data; The Luring Test: AI and the engineering of consumer trust* (May 1, 2023), *https://www.ftc.gov/business-guidance/blog/2023/05/luring-test-ai-engineering-consumer-trust; Chatbots, deepfakes, and voice clones: AI deception for sale* (March 20, 2023), *https://www.ftc.gov/business-guidance/blog/2023/03/chatbots-deepfakes-voice-clones-ai-deception-sale;* and *Keep your AI claims in check* (February 27, 2023): *Keep your AI claims in check* (February 2, 2023), *https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check; Aiming for truth, fairness, and equity in your company's use of AI* (April 19, 2021), *https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai;* Artificial Intelligence and Algorithms (Apr. 8, 2020), *https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms;* The Commission has issued numerous reports related to algorithmic decision making. *See* FTC, Combatting Online Harms Through Innovation: A Report to Congress (June 2022), *https://www.ftc.gov/reports/combatting-online-harms-through-innovation;* FTC Report to Congress on Privacy and Security, September 2021, *https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf;* Fed. Trade Comm'n, Big Data: A Tool for Inclusion or Exclusion? (Jan. 2016), *https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.* For information on best practices to reduce bias and discrimination, *see generally* Rebecca Kelly Slaughter, Algorithms and Economic Justice, Yale J.L. & Tech. (Aug. 2021), *https://law.yale.edu/sites/default/files/area/center/isp/documents/algorithms_and_economic_justice_master_final.pdf.* The agency has also held several public events focused on AI issues, including a workshop on generative AI, workshops on dark patterns and voice cloning, sessions on AI and algorithmic bias at PrivacyCon 2020 and 2021, a hearing on competition and consumer protection issues with algorithms and AI, a FinTech Forum on AI and blockchain, and an early forum on facial recognition technology (resulting in a 2012 staff report). See *https://www.ftc.gov/news-events/events/2023/10/creative-economy-generative-ai; https://www.ftc.gov/news-events/events/2021/04/bringing-dark-patterns-light-ftc-workshop; https://www.ftc.gov/news-events/events-calendar/you-dont-say-ftc-workshop-voice-cloning-technologies; https://www.ftc.gov/news-events/events-calendar/privacycon-2021; https://www.ftc.gov/news-events/eventscalendar/privacycon-2020; https://www.ftc.gov/news-events/events-calendar/ftc-hearing-7-competition-consumerprotection-21st-century; https://www.ftc.gov/news-events/events-calendar/2017/03/fintech-forum-blockchainartificial-intelligence;* and *https://www.ftc.gov/news-events/events-calendar/2011/12/face-facts-forum-facialrecognition-technology.*The Commission has issued an advanced notice of proposed rulemaking that poses questions about the harms to consumers that may result from commercial surveillance, including as related to algorithmic decision making. *See* FTC, Advance Notice of Proposed Rulemaking regarding Commercial Surveillance and Data Security (August 11, 2022), *https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking.*

commenter urged ONC to survey the definitions of healthcare AI currently in use, including the American Medical Association Current Procedural Terminology (CPT®) Appendix S: AI taxonomy for medical services and procedures because it outlines the range of AI tools from those performing purely assistive functions to fully autonomous technologies.

Response. We appreciate the comments, and we are aware of the American Medical Association Current Procedural Terminology (CPT®) Appendix S: AI taxonomy for medical services and procedures. We think this taxonomy has value but decline to include specific purposes or kinds of machine learning in our Predictive DSI definition. We believe such constraints may unintentionally exclude relevant technology as it evolves and is applied to more use cases, humans interact with technology in more diverse ways, and societal views on the line between assistive and autonomous technologies shift. We, again, decline to modify our definition to exclude specific use cases, purpose of uses or intended uses and decline to modify our definition to include specific types of algorithms, such as neural networks, because we suspect the relevant algorithms will similarly evolve over time. We also decline to narrow the definition to exclude prediction, classification, evaluation and analysis because we believe that each of these types of output and use are of relevance in healthcare and can result from fundamentally similar technologies.

Comments. Several commenters expressed concern that the proposed definition included and implicated algorithms that are not directly tied to clinical workflows or capture large areas of software solutions used in certified EHR systems or types of interventions that are not conducive to source attributes or feedback gathering, specifically noting concerns with gathering feedback from passive clinical support. One commenter noted that the proposed definition could be interpreted to classify any list of patients, information form, or a comparison against a population average as Predictive DSI and recommended that ONC should remove the overly broad examples or clarify that the definition applies only when the predictive modifier applies.

Response. We appreciate the comments, and we acknowledge that our discussion regarding the term ''intervention,'' at 88 FR 23786, which included mention of ''alerts, order sets, flowsheets, dashboards, patient lists, documentation forms, relevant data presentations, protocol or pathway support, reference information or guidance, and reminder messages,'' was imperfectly placed. It was not our intention to intimate that each of these kinds of ''interventions,'' would always fall under the Predictive DSI definition but that each kind of intervention *could* be a Predictive DSI if they are driven by algorithms or models that derive relationships from training data and then produce an output that results in prediction, classification, recommendation, evaluation, or analysis. We believe that source attributes can be provided for a Predictive DSI that is used in operations, scheduling, payment, and other workflows and that there is value in doing so, for instance, for medical coders to evaluate the relevance of codes suggested by a Predictive DSI. We note that feedback gathering is limited to evidence-based decision support interventions, which have a more limited scope. We believe that our finalized definition and associated examples provide interested parties with better clarity on technology within the definition's scope.

Comments. Several commenters expressed concern that the proposed definition does not adequately distinguish Predictive DSI from evidence-based DSI, which they believed is also defined too broadly. Commenters provided examples they believed should be excluded from the definition, such as passive decision support, reminders for preventative care, industry standard growth charts, well established reference ranges, default selections in the system, suggested word completions when typing, or rules-based decision support. Several commenters recommended that DSIs should be limited to predictive, evidence-based medicine support interventions impacting clinical choice, and solutions supporting fact-based administrative functions, such as scheduling appointments or bed availability, should be carved out.

Response. We have provided a set of examples, discussed above, along with our finalized definition in § 170.102 of Predictive DSI as meaning technology that supports decision-making based on algorithms or models that derive relationships from training data and then produce an output that results in prediction, classification, recommendation, evaluation, or analysis. We also have clarified the scope of evidence-based DSIs, for purposes of requirements in § 170.315(b)(11), as being limited to only those DSIs that are actively presented to users in clinical workflow to enhance, inform, or influence decision-making related to the care a patient receives and that do not meet the definition for Predictive DSI at § 170.102. We decline to further limit the scope of the Predictive DSI definition, especially for administrative functions, which would likely benefit from the transparency our requirements would provide. We note that even appointment scheduling and block scheduling predictive models have been demonstrated to be of insufficient quality, causing harm to patients.[107] We believe that greater transparency on the quality of these models could have avoided harm to patients by users interpreting predictions more judiciously or choosing not to use the model, or by motivating developers to retrain the models.

Comments. Several commenters recommended that ONC limit the definition to exclude health care providers that have developed their own tools for internal use regardless of whether they are enabled by or interface with the EHR the provider uses from the proposed regulatory requirements. Commenters remarked that the distinction between health care providers and EHR vendors offering DSI services through certified health IT products is important as providers have greater understanding and experience with self-developed DSI tools they use internally and should not be subject to the same requirements as vendors offering DSI tools in certified health IT products for commercial use.

Response. We appreciate the comments. With regards to the definition of Predictive DSI, we did not propose and have not finalized a definition that is dependent on the entity or party developing the Predictive DSI. In other words, ''who develops'' a Predictive DSI is separate and distinct from how we define what a Predictive DSI is for the purpose of this regulation. Along those lines, while health care providers may develop Predictive DSIs (as we have defined), we have not excluded those provider-authored Predictive DSIs from meeting the regulatory definition. However, it is important for commenters to keep in mind that the definition is only one part of the Program's policy approach to Predictive DSIs. In response to comments that appeared to conflate ''the who'' and ''the what'' with respect to the definition, we clarify that a health

[107] Samorani M., Harris S.L., Blount L.G., et al (2021) Overbooked and Overlooked: Machine Learning and Racial Bias in Medical Appointment Scheduling. Manufacturing & Service Operations Management 24(6):2825–2842. *https://doi.org/10.1287/msom.2021.0999.*

care provider who self-develops a tool that meets our definition of Predictive DSI is not subject to the requirements in § 170.315(b)(11). We believe that 'self-developed' tools, which may be developed by informaticians in a health system and then applied to individual patients by clinical users or others without knowledge of the development or evaluation process could benefit from the inclusion of transparency information guiding their use. And our finalized certification criterion in § 170.315(b)(11) would result in health care providers being equipped with the technological capabilities to deliver such transparency through Health IT Modules certified to § 170.315(b)(11). We describe requirements further below that Health IT Modules certified to § 170.315(b)(11) must support the technical capability for source attribute information to be accessed and modified by users as well as the limited contexts in which developers of certified health IT are required to populate those attributes. Specifically, as already noted, we have limited the scope of our transparency requirements for source attribute information to apply to Predictive DSIs that are supplied by the health IT developer as part of its Health IT Module.

Comments. One commenter urged ONC to revise the proposed definition of Predictive DSI in a manner that specifically excludes laboratory results reported to a health care provider via a Health IT Module when such laboratory results are derived using an algorithm. The commenter noted their concern that the broad definition of Predictive DSI could cause Health IT developers to believe that a laboratory offering a test whose result is derived using an algorithm, and which is reported via an interfaced laboratory information system (LIS), must provide source attribute information about the test. The commenter also noted instrumentation result generation should not be considered covered by this DSI intervention rule, because laboratories' instrumentation remains under the auspices of standards established by the College of American Pathologists (CAP) and CLIA. One commenter expressly requested that we adopt an exception for radiologists in implementing DSI because they stated that DSI is not useful to that specialty and thus we should exempt them until the CMS Appropriate Use Criteria (AUC) program is available.

Response. We appreciate the comments. As noted above, we respectfully decline to include any exclusionary criteria in our definition for Predictive DSI, including exclusions for specific types of organizations that develop the Predictive DSI, exclusions for specific types of technology that may be considered a Predictive DSI, and exclusions for organizations or technology that may be subject to other federal requirements and authorities, like the Clinical Laboratory Improvement Amendments regulations,[108] the CMS Appropriate Use Criteria program,[109] or Medicare Advantage Program regulations related to utilization management.[110] Related to the lab example provided by the commenter, and reflective of our final policy, this example would generally *not* be within the scope of a developer of certified IT's accountability, unless the developer of certified health IT specifically supplied the laboratory Predictive DSI as part of its Health IT Module certified to § 170.315(b)(11). As indicated by the comment, the certified health IT would be receiving a lab result for an outside entity using instrumentation separate and distinct (not included as a part of the developer's certified health IT), even if that result was arrived at by the laboratory using a Predictive DSI.

Comments. One commenter requested clarification on whether patient matching algorithms are subject to the Predictive DSI definition, and thus included in the risk management and reporting requirements. The commenter was supportive of including patient matching algorithms under the proposed definition given that the models use example data to determine accuracy prior to implementation and produce an output stating which patient it believes matches to which record given the data it is presented with. The commenter observed that by being able to understand the matching algorithms themselves, the healthcare continuum can better react and hone its data capture practices ensuring the algorithms receive the best quality data to guarantee the best possible match given the algorithms' determinations. Relatedly, a second commenter requested clarification on whether an algorithm that assigns similarity scores without labels is not a Predictive DSI.

Response. We appreciate the comment and refer readers to our finalized definition for Predictive DSI as technology that supports decision-making based on algorithms or models that derive relationships from training data and then produces an output that results in prediction, classification, recommendation, evaluation, or analysis. We are aware of a variety of methods to perform patient matching, including identifying whether specific fields are exact matches, or whether certain strings of text contain a high proportion of matching characters, and not all of them are based in relationships derived from training data.[111] Such patient matching methods would likely not be considered Predictive DSI if they were not based on relationships derived from training data. We further note that the exclusion of unsupervised machine learning approaches, which generally do not predict an unknown value but rather identify the similarity or closeness of data, described at 88 FR 23786, is likely to apply to some patient matching algorithms, which would also likely not be considered Predictive DSI. That same clarification would apply to other algorithms that generate a similarity or closeness score without labeled training data (for instance, patient phenotyping or search recommendations based on the similarity between search strings and document contents), which would likely not be considered Predictive DSI. Other patient matching algorithms, especially those leveraging a supervised learning approach, are likely to meet the definition of a Predictive DSI.

Comments. A different commenter was concerned with the proposed definition of Predictive DSI including the term ''algorithm'' because it suggested a more inclusive set of health IT than they believed was intended by legislative and regulatory scope, which they stated would create confusion in the marketplace. The commenter recommended refining DSI's definition by removing ''algorithms'' to limit scope specifically to decision support driven by models using example data. Some commenters recommended ONC shift the criterion back to a specific focus on

[108] CLIA regulations include federal standards applicable to all U.S. facilities or sites that test human specimens for health assessment for to diagnose, prevent, or treat disease. CDC, in partnership with CMS and FDA, supports the CLIA program and clinical laboratory quality. For more information, see *https://www.cdc.gov/clia/index.html.*

[109] We note that CMS rescinded the regulations for the AUC program in the 2024 Physician Fee Schedule Final Rule (88 FR 79262). For more information about the program, see *https://www.cms.gov/medicare/quality/appropriate-use-criteria-program.*

[110] See, *e.g.,* CMS Medicare Advantage Program Final Rule (April 2023), *https://www.federalregister.gov/documents/2023/04/12/2023-07115/medicare-program-contract-year-2024-policy-and-technical-changes-to-the-medicare-advantage-program* (clarified coverage criteria for basic benefits and the use of prior authorization, added continuity of care requirements, and required an annual review of utilization management tools).

[111] Government Accountability Office. Health Information Technology: Approaches and Challenges to Electronically Matching Patients' Records across Providers. Jan 15, 2019.

clinical DSIs as an initial starting point for the revised criterion.

Response. We appreciate the comment and the concern. Our definition for Predictive DSI includes technology that supports decision-making based on both models and algorithms that derive relationships from training data and then produce an output that results in prediction, classification, recommendation, evaluation, or analysis. We understand that not all interested parties share the same conception of how an algorithm is related to a model or vice versa. Regardless, the existence of an algorithm in or as part of a technology is not, alone, determinative in meeting our definition for Predictive DSI. In addition to including an algorithm, a technology must also support decision-making based on the algorithm and that algorithm must derive, or learn, relationships from training data and then produce an output that results in prediction, classification, recommendation, evaluation, or analysis. We also decline to limit the scope of our definition to focus on clinical uses as previously discussed in this section.

Attestation for Predictive Decision Support Interventions

In proposed § 170.315(b)(11)(v)(A), at 88 FR 23786, we proposed that developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) attest ''yes'' or ''no'' to whether their Health IT Module enables or interfaces with Predictive DSIs based on any of the data expressed in the standards in § 170.213. This attestation requirement would have the effect of permitting developers of certified health IT to certify to § 170.315(b)(11) without requiring their Health IT Modules to enable or interface with Predictive DSIs. However, for those developers of certified health IT that attest ''yes'' as described in § 170.315(b)(11)(v)(A), we described in the HTI–1 Proposed Rule additional applicable requirements related to source attributes and IRM practices (88 FR 23786).

We clarified that ''enables'' means that the developer of certified health IT has the technical capability to support a predictive model or DSI within the developer's Health IT Module. We clarified that applications developed by other parties and self-developed applications that are used within or as a part of a Health IT Module would mean that the Health IT Module is considered to ''enable'' Predictive DSIs. We provided an example, stating that if the calculations or processing for a Predictive DSI occur within the Health IT Module, either through a standalone application developed by an *other party*[112] or an application self-developed by a developer of certified health IT for use within a Health IT Module, we would consider this ''enabling.'' In contrast, we clarified that ''interfaces with'' means that the Health IT Module facilitates either (1) the launch of a predictive model or DSI or (2) the delivery of a predictive model or DSI output(s) to users when such a predictive model or DSI resides outside of the Health IT Module and provided examples. We noted that some organizations may use USCDI data exported or sourced from a certified Health IT Module to develop data-driven advanced analytics leveraging predictive models or technologies to provide insights for healthcare. We also noted that in such circumstances, our proposed requirements would only apply if the output of the predictive model subsequently interfaced with a Health IT Module. The proposed requirement would not establish requirements for predictive technologies that are not enabled or do not interface with a Health IT Module.

Finally, we clarified that *other parties* includes any party that develops a DSI, a model, or an algorithm that is used by a DSI and is not a developer of certified health IT (88 FR 23796). We said these other parties could include, but are not limited to: a customer of the developer of certified health IT, such as an individual health care provider, provider group, hospital, health system, academic medical center, or integrated delivery network; a third-party software developer, such as those that publish or sell medical content or literature used by a DSI; or researchers and data scientists, such as those who develop a model or algorithm that is used by a DSI.

Comments. Commenters were generally supportive of the proposal to enable Health IT Modules to be certified to § 170.315(b)(11) without the health IT developer being obligated to provide Predictive DSIs to their customers by having developers of certified health IT attest ''yes'' or ''no'' to whether their Health IT Module enables or interfaces with Predictive DSIs based on any of the data expressed in the standards in § 170.213. Commenters requested that we reflect that health IT developers would not be compelled to provide (or author) Predictive DSIs due to the attestation statements adopted in this provision.

Notwithstanding the general support, many commenters did not support the ''enables or interfaces with,'' construct associated with the attestation proposed in § 170.315(b)(11)(v)(A). Many commenters noted that the ''enables or interfaces with,'' scope was a vague, ambiguous, and problematic phrase when applied to the proposed definition for Predictive DSI. Commenters, specifically health IT developers, were concerned that it would be hard to comply with the ''enables or interfaces with'' scope on which conditional requirements for source attributes and IRM practice requirements would rely. Commenters requested that we further define and narrow the scope of ''enables or interfaces with,'' and commenters stated that ONC should clearly define the scope of activities or technologies to which the related requirements for source attributes and IRM practices apply. For example, some commenters suggested that source attribute and IRM practice requirements should only apply in specific situations, such as when entities have contracts specifically covering the enablement and use of such technologies. Commenters also expressed substantive concerns that the phrase ''enables or interfaces with'' would require health IT developers to meet the transparency requirements for all third-party apps that customers utilize via § 170.315(g)(10) technology. They also stated that it would be difficult for developers to know when these third-party apps ''enable or interfaced with'' their Health IT Module and difficult to require third parties to provide source attributes information, particularly when there is no contractual relationship between the health IT developer and those third parties.

Taken together and as we looked at the substance of comments comprehensively, we noticed that commenters described circumstances that would otherwise make the original intent behind the attestation proposal moot. Instead of enabling a health IT developer that did not provide or author Predictive DSIs to meet the attestation for proposed § 170.315(b)(11)(v) by attesting ''no'' regarding their support for Predictive DSIs, many developers appeared to convey that they would need to attest ''yes'' because of their understanding of the proposed scope for ''enable or interface with.'' This was because they interpreted our proposal for ''enable or interface with'' to include their accountability for customer actions associated with Predictive DSIs, which would not necessarily be known at the

[112] Please note that ''other party'' is a term of art we described at 88 FR 23796. In this final rule, we have italicized *other party* and *other parties* to assist readers' understanding that we are using this term of art and not misspelling ''another.''

time of certification and, as a result, the developer of certified health IT would have to err on the side of expecting that one of their customers would enable or interface their Health IT Module with a Predictive DSI. In short, we understood from commenter feedback that developers of certified health IT could not reasonably validate whether customers were using Health IT Modules to enable or interface with Predictive DSIs.

On the whole, commenters contended that our proposal included ambiguities and challenges related to implementation, knowledge, and ongoing compliance. The latter of which would be the most difficult for developers of certified health IT based on what we had proposed. For example, if under our proposal, a developer had attested ''no'' and then months later a single customer had ''enabled or interfaced with'' an *other party* Predictive DSI with the developer's Health IT Module (certified to § 170.315(b)(11)), it was unclear whether the developer would need to reengage its ONC–ACB to change its certificate for § 170.315(b)(11) and attest ''yes'' and take on the additional compliance requirements. Comments also made clear that we should seek to minimize and separate how independent customer actions and decisions associated with Predictive DSIs interplay with conditional compliance requirements for developers of certified health IT under the Program.

Response. We appreciate commenters' feedback on the attestation proposal, its construction within the criterion at § 170.315(b)(11), and how to make it more implementable. In summary, the intent behind the proposed attestation statement and its associated framing was to establish a conditional approach whereby developers of certified health IT certifying to § 170.315(b)(11) would still be able to get certified to § 170.315(b)(11) even if their Health IT Module did not enable or interface with a Predictive DSI. We had hoped that this would relieve specific regulatory burdens for developers of certified health IT that had no intention to enable or interface with a Predictive DSI. However, as commenters pointed out, because of the broad scope of ''enable or interfaced with'' even those developers that could have plausibly attested ''no'' may still have felt it necessary to attest ''yes'' when seeking certification. Despite not knowing of customers using Health IT Modules to enable or interface with a Predictive DSI, these developers of certified health IT would need to attest ''yes'' as soon as single customer used their certified Health IT Module to enable or interface with a Predictive DSI. We interpreted these developer compliance concerns, about whether they would know if a customer had enabled or interfaced a Predictive DSI with their Health IT Module, as an important implementation issue and necessary to address as part of this final rule.

In consideration of these and similar comments, we have not adopted the attestation statement we proposed in § 170.315(b)(11)(v). Given the circumstances and concerns described by commenters, we have concluded that accurate attestations, relieved burden, and clear (initial and ongoing) compliance would not have been accomplished as proposed. Rather than adopt an attestation statement, we have finalized minimal, uniform requirements for all Health IT Modules certified to § 170.315(b)(11) while also maintaining a construction that enables a developer of certified health IT to certify a Health IT Module to § 170.315(b)(11) without being obligated to author, develop, or otherwise directly provide Predictive DSIs to their customers. In response to comments, we believe this synthesized approach provides developers of certified health IT with clear policy and layered compliance requirements that are specifically within the scope of the Program and that of the developer's control (*i.e.,* a customer's action will not create any corresponding compliance impact on a developer's § 170.315(b)(11) compliance).

As described throughout this section, we have removed ''enabled or interfaced with'' and replaced it with ''supplied by.'' The final rule's scope places the knowledge, decision, and ongoing compliance associated with including a Predictive DSI solely within the control of a developer of certified health IT. While the use of ''supplied by'' is a different configuration nexus than the proposed attestation statement that used ''enables or interfaces with,'' this approach similarly addresses our intent to only apply additional Predictive DSI related stewardship responsibilities to health IT developers who supply Predictive DSIs as part of their Health IT Module. The paragraphs that follow illustrate by way of final certification criterion requirements some of the changes we have made in response to comments associated with the certification criterion's focus on Predictive DSI's ''supplied by'' the health IT developer and the corresponding effect of not finalizing the attestation. We believe the finalized requirements provide much more certainty for health IT developers while still addressing our overall policy goal for § 170.315(b)(11)—to provide as part of the Program greater transparency associated with DSIs, particularly Predictive DSIs and their ability to be FAVES.

First, we have adopted requirements in § 170.315(b)(11)(iii), described previously in this final rule, that enables a limited set of identified users to select (*i.e.,* activate) electronic DSIs that are evidence-based in (b)(11)(iii)(A) and predictive in (b)(11)(iii)(B). We believe that this uniform requirement to enable the selection of a Predictive DSI represents a minimal level of effort beyond, and a slight modification to, what developers of certified health IT would have had to do if we had finalized the ''no,'' attestation. Such developers of certified health IT would have had to enable selection of evidence-based DSIs and supported source attribute fields for evidence-based DSIs. As stated previously, enabling the selection of Predictive DSIs would likely be operationalized through the same technical means as enabling selection of an evidence-based DSI. Additionally, and in acknowledgement of our proposed rule discussion that requirements for DSI configuration in § 170.315(b)(11)(ii) applied to both evidence-based DSIs and Predictive DSIs (88 FR 23783), we believe that Health IT Modules certified to § 170.315(b)(11) would have baseline expectations to support both user configuration of Predictive DSIs and user selection of Predictive DSIs. Finally, we believe that software development of fields to support source attributes (in § 170.315(b)(11)(v)(B)) for Predictive DSIs would likely not be substantially more burdensome than the work necessary to develop fields to support evidence-based DSI source attributes (in § 170.315(b)(11)(A)).

Second, the finalization of § 170.315(b)(11) without an attestation statement but with uniform requirements for users to configure and have the technical capability to select both evidence-based and Predictive DSIs achieves a policy goal to ensure that users have equal technical capabilities to access, record, and change Predictive DSI source attributes in § 170.315(b)(11)(v)(B) for Predictive DSIs they self-develop and for Predictive DSIs they purchase from other parties, in addition to potential Predictive DSIs supplied by the users' developer of certified health IT. Under the proposed attestation statement with the enables or interfaces with configuration nexus, users of Health IT Modules that attested ''no,'' would have technical challenges to use self-

developed or *other party*-developed Predictive DSIs. This is because Predictive DSI-related source attribute fields (proposed in § 170.315(b)(11)(vi)(C)) and Predictive DSI-related capabilities to author and revise source attributes (proposed in § 170.315(b)(11)(vi)(E)) would not have been required for those ''no attestation'' Health IT Modules to support. We believe that as the market for Predictive DSIs grows, equivalent technical capabilities for users to access, record, and change source attributes in § 170.315(b)(11)(iv) across Health IT Modules certified to § 170.315(b)(11) will be vital to promote Predictive DSIs that are FAVES.

Third, we have narrowed the focus of requirements related to providing IRM practices information on Predictive DSIs to those that are ''supplied by the health IT developer as part of its Health IT Module.'' This approach reduces the overall scope of technologies subject to final requirements in § 170.315(b)(11) while keeping the intent of the attestation statement we proposed. For instance, our finalized policy in § 170.315(b)(11)(vi) requires that for Predictive DSIs supplied by the developer of certified health IT as part of its Health IT Module the developer would have to address specific IRM practices associated with each Predictive DSI it supplies. As noted and similar to our intent with the ''no'' attestation proposal, based on the revised scope in this final rule, if a health IT developer does not supply any Predictive DSIs it will still be able to comply with § 170.315(b)(11) and will not have to meet, for example, IRM practice requirements in § 170.315(b)(11)(vi) because the health IT developer does not supply any Predictive DSIs as part of its Health IT Module. We note, however, if after certification to § 170.315(b)(11), a developer does begin to supply Predictive DSIs as part of its certified Health IT Module, it would need to comply with all applicable requirements in § 170.315(b)(11).

We interpret ''supplied by'' to include interventions authored or developed by the health IT developer as well as interventions authored or developed by an *other party* that the health IT developer includes as part of its Health IT Module, such as stated in the comments ''when entities have contracts specifically covering the enablement and use of such technologies.'' The concept of ''supplied by'' means that the developer of certified health IT has taken on stewardship and accountability for that Predictive DSI for the purposes of the Health IT Module. We interpret ''as part of its Health IT Module'' to mean that the developer of certified health IT has explicitly offered or provided its customers the technical capability to use or support a Predictive DSI, regardless of whether the Predictive DSI was developed by the developer of certified health IT or by an *other party.*

By way of example, ''supplied by the health IT developer as part of its Health IT Module'' would include the implementation of a publicly available predictive model, like LACE+,[113] if a developer of certified health IT includes this Predictive DSI as part of its product and it is part of what the developer offers its customers. As another example, ''supplied by the health IT developer as part of its Health IT Module'' would include incorporation of an *other party's* LLM, or other generative AI, that meets the definition of Predictive DSI and is part of what the developer offers its customers.

From a conformance perspective, ''supplied by the health IT developer as part of its Health IT Module'' means that developers of certified health IT are not accountable for populating source attribute information for, or applying IRM practices, to Predictive DSIs in instances where their customers choose to deploy a self-developed Predictive DSI or an *other party*-developed Predictive DSI for use within their certified health IT. This is true even if the customer leverages data from the developer of certified health IT's Health IT Module and even if the output from an *other party's* Predictive DSI is delivered to or through a Health IT Module into a customer's clinical workflow.

We reiterate that *other party* means any party that develops a DSI, a model, or an algorithm that is used by a DSI, and is not the developer of certified health IT or a subsidiary of the developer of certified health IT. This is consistent with our discussion in the HTI–1 Proposed Rule on 88 FR 23796.[114] This description of *other party* in this final rule preamble specifically excludes a subsidiary of a developer of certified health IT. We intend for purposes of our requirements in § 170.315(b)(11) that a subsidiary of a developer of certified health IT that develops a Predictive DSI would be considered the same as if it were the developer of certified health IT, subjecting Predictive DSIs developed by a subsidiary to the same requirements as a Predictive DSI supplied by a developer of certified health IT as part of its Health IT Module.

We note that Health IT Modules certified to § 170.315(b)(11) must support the technical capability for *other party* source attribute information to be entered into the Health IT Module's source attribute fields, per requirements elaborated below for final § 170.315(b)(11)(v)(B). We note that if a developer of certified health IT would like to include a capability for *other parties* to record source attributes into a Health IT Module in a way that shields the developer of certified health IT from having access to the *other party* source attributes, they may do so. However, we reiterate that developers of certified health IT are not required to receive, acquire, or otherwise obtain source attribute information for an *other party's* Predictive DSI unless such Predictive DSI is supplied by the developer of certified health IT as part of its Health IT Module.

Finally, and in consideration of comments received and the scope reductions we have made to this final certification criterion, we determined that a supportive Maintenance of Certification requirement as part of the Assurances Condition of Certification in 45 CFR 170.402(b) was necessary to fully implement our policy objectives and proposals. We have included in this final rule an Assurances Maintenance of Certification requirement that reinforces a certified health IT developer's ongoing responsibility in § 170.315(b)(11)(v)(A)(*1*) to enable user access to updated descriptions of source attribute information at § 170.315(b)(11)(iv)(A) and (B), to review and update as necessary IRM practices that must be applied for each Predictive DSI the health IT developer supplies as part of its Health IT Module in § 170.315(b)(11)(vi), and to ensure the ongoing public accessibility of updated summary IRM practice information as submitted to their ONC–ACB via hyperlink in § 170.523(f)(1)(xxi).

This Maintenance of Certification requirement is a § 170.315(b)(11)-specific instantiation of general Program requirements described in § 170.402(a) as well as an adaptation of what we proposed at § 170.315(b)(11)(vii)(D), which proposed to establish an ''annual

[113] van Walraven, Carl, Jenna Wong, and Alan J. Forster. ''LACE+ index: extension of a validated index to predict early death or urgent readmission after hospital discharge using administrative data.'' *Open Medicine* 6.3 (2012): e80.

[114] As noted in HTI–1 Proposed Rule, *Other parties* can include, but are not limited to: a customer of the developer of certified health IT, such as an individual health care provider, provider group, hospital, health system, academic medical center, or integrated delivery network; a third-party software developer, such as those that publish or sell medical content or literature used by a DSI; or researchers and data scientists, such as those who develop a model or algorithm that is used by a DSI (88 FR 23796).

and, as necessary, update'' requirement for developers with Health IT Modules certified to § 170.315(b)(11) (88 FR 23805). In consideration of comments received on § 170.315(b)(11) as a whole and the corresponding changes we made to the final certification criterion to focus on Health IT Module capabilities, it became clear that the ongoing transparency of source attribute and IRM practices associated with § 170.315(b)(11) would best fit under the Program as a developer-level responsibility compared to a product-level responsibility. As such, it made the most sense to shift the nature of these proposals from the more technical certification criterion to the Assurances Condition. Accordingly, we have finalized at § 170.402(b)(4) that starting January 1, 2025, and on an ongoing basis, developers of Health IT Modules certified to § 170.315(b)(11) must review and update, as necessary, source attribute information in § 170.315(b)(11)(iv)(A) and (B), risk management practices described in § 170.315(b)(11)(vi), and summary information provided through § 170.523(f)(1)(xxi).

First, we have finalized this Maintenance of Certification requirement to serve as a discrete connection for developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) to have complete and up-to-date descriptions of source attribute information (in § 170.315(b)(11)(iv)(A) and (B)) at the time of certification and on an ongoing basis while their Health IT Module is certified to § 170.315(b)(11). This Maintenance of Certification requirement builds on three existing Assurances Condition of Certification requirements at § 170.402(a)(1), (2) and (3), respectively, stating that a health IT developer must provide assurances to the Secretary that it ''. . . will not take . . . any other action that may inhibit the appropriate exchange, access, and use of electronic health information,'' ''must ensure that its health IT certified under the ONC Health IT Certification Program conforms to the full scope of the certification criteria,'' and ''must not take any action that could interfere with a user's ability to access or use certified capabilities for any purpose within the full scope of the technology's certification.'' While we believe these existing requirements within the Assurance Condition pertain to both evidence-based and Predictive DSIs, as well as IRM practices, we believe this specific additional Maintenance of Certification requirement is necessary because of the unique, evolving, and dynamic nature of DSIs. Moreover, it is important for users of health IT certified to § 170.315(b)(11) as well as the Secretary to have as an explicit assurance that developers of certified health IT are keeping source attribute information up-to-date and, as applicable, that such developers are committed to IRM practices.

For example, both evidence-based and Predictive DSIs use EHI as key input data in underlying rules and models. Supplying DSIs without accompanying accurate and up-to-date documentation could inhibit the appropriate use of EHI in two ways. First, it could lead the health IT developer's customers to fail to use the DSI in appropriate ways, most obviously by omission of an updated statement of the DSI's intended use as required at § 170.315(b)(11)(iv)(B)(*2*)(*i*). Similarly, supplying DSIs without accompanying documentation could lead to the use of a DSI on unintended populations, on individuals from groups for which the DSI does not perform adequately, or by leading to the use of a DSI for which associated risks have not been appropriately identified and mitigated. Further, supplying a DSI without accompanying documentation could inhibit the selection and use of a DSI that would make appropriate use of EHI. Without information on the DSI supplied by the developer of certified health IT, users will not be able to adequately determine whether the developer of certified health IT's supplied DSI is fit for their purpose, or whether they should select a more effective DSI.

While we believe that, under our proposal, developers of certified health IT would have taken actions to continually maintain information associated with DSIs and IRM practices, in accordance with Assurances requirements in § 170.402(a)(1), (2), and (3), this Maintenance of Certification requirement adds necessary specificity to the overall Assurances Condition of Certification and ensures that developers of certified health IT are firmly aware of their ongoing obligations associated with the certification criterion at § 170.315(b)(11). Moreover, this Maintenance of Certification requirement ensures that actions taken by the developer of certified health IT enable a user to access § 170.315(b)(11)-related documentation on an ongoing basis will not inhibit the appropriate use of EHI. In establishing this Maintenance of Certification requirement, we address acute transparency concerns from public comments regarding the accuracy, relevance, and timeliness of the source attribute information provided by the developers of certified health IT. As reflected in several source attributes seeking information on the ongoing maintenance of intervention implementation and use, and in particular the validity and fairness of predictions in local data, models and data used to drive Predictive DSIs will change over time (88 FR 23792); if developers of certified health IT do not continue to keep associated attribute information up to date, their failure to do so could have adverse impacts on user trust, accuracy, usage, and safety.

Second, we have finalized in this Maintenance of Certification requirement that developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) review and update as necessary risk management practices described in § 170.315(b)(11)(vi). This is substantially similar to what we proposed at § 170.315(b)(11)(vii)(D), which was to review annually and, as necessary, update IRM practice documentation. We discuss comments received to proposed § 170.315(b)(11)(vii)(D) further in this final rule preamble.

Last, we have finalized in this Maintenance of Certification requirement that developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) review and update as necessary summary information provided to the developer's ONC–ACB, consistent with what we proposed at § 170.315(b)(11)(vii)(C), which required that summary information be submitted to the health IT developer's ONC–ACB via publicly accessible hyperlink, as well as what we proposed at § 170.523(f)(xxi), which required ONC–ACBs to ensure that all of the information required to be submitted by the health IT developer to meet IRM requirements in § 170.315(b)(11)(vii)(C) were available via public hyperlink. We discuss comments received to proposed § 170.315(b)(11)(vii)(C) and § 170.523(f)(xxi) further in this final rule preamble.

Comments. While some commenters agreed with and were supportive of the proposed definition and our explanation of the differences between ''Enables'' and ''Interfaces with,'' several commenters expressed concern that the proposed phrase ''enables or interfaces with'' was overly broad when applied to the proposed definition for Predictive DSI and requested that we further define and narrow the scope of these terms. These commenters stated that ONC should clearly define the scope of activities or technologies that ''enable or

interface with'' Predictive DSIs to narrow the scope of this requirement to make it clear that the HTI–1 Proposed Rule applies in situations such as, for example, when entities have contracts specifically covering the enablement and use of such technologies. Commenters also expressed concern that the phrase ''enables or interfaces with'' would require health IT developers to meet the transparency requirements for all third-party apps that customers utilize via § 170.315(g)(10) technology, and that it would be difficult for developers to require third parties to provide source attributes information, particularly when there is no contractual relationship between the health IT developer and *other party* developers.

Response. We appreciate the comments and have modified our final scope for Health IT Modules that must provide source attribute information and our scope for which Predictive DSIs must be subject to IRM practices in response to public comment. We understand through public comments that interested parties viewed the scope contingent on ''enables or interfaces with'' as too broad and ambiguous, especially given that the scope of these terms would impact conditional requirements related to source attributes and risk management by way of the proposed attestation in § 170.315(b)(11)(v). In considering alternative constructions that would clarify our intent and in consideration of commenters' concerns, we have finalized a construction that narrows and replaces the two concepts of ''enables,'' and ''interfaces with,'' with ''supplied by.'' This modification is reflected in the finalized text of § 170.315(b)(11)(v) and regulatory text in § 170.315(b)(11)(vi) to establish conditional requirements for Health IT Modules that include an *other party's* Predictive DSI that is supplied by the health IT developer.

For example, if a user ordered a lab test using the existing certification criterion capability for computerized provider order entry-laboratory (§ 170.315(a)(3)) and the lab test result was derived from a Predictive DSI used by the laboratory, such a configuration would be out of scope and the Health IT Module would not subject to the requirements in § 170.315(b)(11)(v), because the Predictive DSI that rendered the lab test result was not supplied by (*i.e.,* included as part of the Health IT Module) the developer of the certified health IT.

We believe that these modifications significantly narrow the scope of our proposal and clarify which *other party* Predictive DSI configurations are subject to requirements in § 170.315(b)(11) for source attributes. We also note that the phrase ''supplied by'' is also included in the text of § 170.315(b)(11)(vi) to establish a conditional requirement that for each Predictive DSI supplied by the health IT developer as part of its Health IT Module, is subject to risk analysis, risk mitigation, and governance, which we discuss more in section ''xi. Intervention Risk Management (IRM)'' later in this final rule. We believe that developers of certified health IT with Health IT Modules that supply an *other party's* Predictive DSI as part of their Health IT Module would be generally aware of and be well positioned to make source attribute information available for user review as well as apply IRM practices given the likelihood of a high degree of technical coordination and formalized business relationship between a developer of certified health IT and an *other party* in such scenarios.

Comments. One commenter expressed concern that the definition of Predictive DSI included the terms ''interfaces with,'' and ''enabled by'' could potentially incorporate test results generated using laboratory processes that contain algorithmic components, if the outputs of those tests are transmitted to an EHR, and requested that the definition exclude laboratory results because labs are already subject to other federal requirements and should not be subject to additional requirements due to their results being made available through an EHR.

Response. We thank the commenter for their input. However, we clarify that neither our proposed nor final definition in § 170.102 included the terms ''interfaces with,'' or ''enabled by.'' These terms of art were used in the HTI–1 Proposed Rule to establish a configuration nexus that would subject Health IT Modules to additional requirements if such Health IT Modules enabled or interfaced with a Predictive DSI. As noted above, and given that our final policy nexus is dependent on ''supplied by the health IT developer as part of its Health IT Module,'' we note that if the test result is generated by a Predictive DSI used by the lab itself for the generation of results but the Predictive DSI is not supplied by the developer of the certified Health IT Module, it would be out of scope of the requirements established by the final policy. As another example, if a user ordered a lab test using the existing certification criterion capability for Computerized provider order entry-laboratory (§ 170.315(a)(3)) and the lab test result was derived from a Predictive DSI used by the laboratory, such a configuration would be out of scope and the Health IT Module would not subject to the requirements in § 170.315(b)(11), because the Predictive DSI that rendered the lab test result was not supplied by the health IT developer as part of its Health IT Module.

vi. Source Attributes

At 88 FR 23787, we proposed in § 170.315(b)(11)(vi) that Health IT Modules certified to § 170.315(b)(11) enable a user to review a plain language description of source attribute information as indicated at a minimum via direct display, drill down, or link out from a Health IT Module. We noted that § 170.315(g)(3) ''safety-enhanced design,'' applies to the existing § 170.315(a)(9) criterion and in keeping with that applicability, we proposed that safety-enhanced and user-centered design processes described in § 170.315(g)(3) would apply to the new certification criterion proposed in § 170.315(b)(11) as well. We proposed to update § 170.315(g)(3) accordingly to reference the proposed § 170.315(b)(11).

Comments. Commenters were generally split on supporting or not supporting the proposal in § 170.315(b)(11)(vi) that Health IT Modules certified to § 170.315(b)(11) enable a user to review a plain language description of source attribute information as indicated at a minimum via direct display, drill down, or link out from a Health IT Module. Those in support noted that it would have the benefit of allowing users to assess the DSI's quality and thereby enhancing trustworthiness; enable those with sufficient knowledge to understand the data to make informed purchasing decisions; and give flexibility that ensures that the recommendations and guidance provided by these systems align with the organization's unique workflows and patient populations, facilitating seamless integration into clinical practice. Several commenters agreed that user feedback can be a useful tool to support quality improvement within health IT and emphasizing transparency and customization allows healthcare organizations to tailor decision support systems to their specific needs. Other commenters urged ONC not to adopt the direct display, drill down, or link requirement observing that including too much information in the direct display can negatively impact usability and user adoption in comparison to providing rational and accessible paths to deeper information via click-paths that are based on user-centered design principles. These commenters worried that requiring ''at a minimum direct

display, drill down, or link out,'' could unintentionally inhibit innovative user interfaces and user designs to enable user access to source attributes.

Response. We thank commenters for their support, and we note that requirements originally proposed in § 170.315(b)(11)(vi) for source attributes built off more than a decade of existing expectations for source attributes in the current CDS criterion at § 170.315(a)(9)(v) where the expectation for direct display, drill down, or link out had been described at 77 FR 54215. However, in consideration of comments, we have not finalized the requirements for source attribute information to be available via direct display, drill down, or link out from a Health IT Module. Rather we have finalized a source attributes requirement in § 170.315(b)(11)(iv) without the text ''at a minimum via direct display, drill down, or link out from a Health IT Module.'' While we have not finalized a requirement for presenting source attribute information to users in the regulation text at § 170.315(b)(11)(iv), we reiterate the requirement in § 170.315(b)(11)(v)(A)(*1*) that Health IT Modules enable a limited set of identified users to access complete and up-to-date plain language descriptions of source attribute information in paragraphs § 170.315(b)(11)(iv)(A) and § 170.315(b)(11)(iv)(B). And we have also included a requirement in § 170.315(b)(11)(v)(B)(*1*) to enable a limited set of identified users to record, change and access the same source attribute information. The phrase ''limited set of identified users'' conveys that the capability is not required for all users of the Health IT Module. Rather, that the capability can be constrained to a smaller userbase that are identified to have the privileges necessary to use the capabilities in § 170.315(b)(11), including the capability to record, change, and access source attributes and source attribute information. We have provided this flexibility so that any number and configuration of users may record, change, and access source attribute information according to organizational needs. For example, if a client of a developer of certified health IT hosts source attributes for each deployed evidence-based or Predictive DSI centrally, a Health IT Module could include a hyperlink from a dashboard or other user interface to a user at the point-of-care. Additionally, this flexibility could limit record, change, and access privileges to a user who has responsibilities for an organization's procurement and implementation decisions.

Finally, we did not receive any substantive or direct feedback regarding our proposal to update ''safety-enhanced design,'' to reference the certification criterion finalized in § 170.315(b)(11). We continue to believe that just as the CDS criterion in § 170.315(a)(9) was subject to safety-enhanced design requirements, so too should the revised criterion in § 170.315(b)(11). Thus, we have finalized our proposed modification to § 170.315(g)(3) ''safety-enhanced design,'' to reference the certification criterion finalized in § 170.315(b)(11).

Comments. Commenters requested clarity on the proposal for source attributes noting that the proposal was ambiguous as to what source attributes would need to be implemented and requested that ONC provide more clarity on the expectation of how source attributes must be implemented in a Health IT Module. Specifically, one commenter requested clarification on whether software should support source attribution when clinically appropriate, noting that many health care providers and health systems have structures in place to track appropriate source attributes. One commenter requested additional clarity on how the information being available at the point of care should be used in real time stating that most of the source attribute information will be relevant to the organization while it makes procurement and implementation decisions versus during care delivery.

Response. We appreciate the commenters' suggestions and have finalized our proposal with modifications in consideration of these and related comments. We have made several modifications to reduce the ambiguity cited by commenters related to the source attributes proposals. We have separately identified requirements related to accessing up-to-date and complete information for DSI supplied in the Health IT Module at § 170.315(b)(11)(v)(A) and requirements related to enabling customers to modify source attributes and source attribute information for DSI at § 170.315(b)(11)(v)(B). We also separately list source attribute categories for evidence-based and Predictive DSI at § 170.315(b)(11)(iv)(A) and (B), respectively. We believe that information available as source attributes will have value both as reference information to individual users evaluating the use of a DSI on an individual patient—for instance, by assessing whether it has been recently evaluated at their health system and whether it has been shown to perform well for a patient like theirs—and for the organization during procurement, implementation, and analysis.

To further address potential ambiguity about how source attributes must be implemented in Health IT Modules certified to § 170.315(b)(11), we have finalized uniform requirements in § 170.315(b)(11)(iv) for Health IT Modules to support source attributes listed at § 170.315(b)(11)(iv)(A) and (B). This means that all Health IT Modules certified to § 170.315(b)(11) must support the categories, but not necessarily the content, for each source attribute listed at § 170.315(b)(11)(iv)(A) and (B). For example, Health IT Modules must support user access to complete and up-to-date source attribute information in § 170.315(b)(11)(iv)(B) only if the Predictive DSI is supplied by the health IT developer as part of its Health IT Module.

We have provided additional specificity about the technical capabilities required to support source attributes at § 170.315(b)(11)(v). As described above, we have not finalized our proposal for an attestation statement. Rather, we have finalized in § 170.315(b)(11)(v) a set of four capabilities that Health IT Modules must support related to source attributes. Each of these capabilities was proposed in different parts of § 170.315(b)(11) in the HTI–1 Proposed Rule.

First, we have finalized requirements for ''Source attribute access and modification'' in § 170.315(b)(11)(v). Specifically, we finalized a requirement in § 170.315(b)(11)(v)(A)(*1*) that is substantially similar to what we proposed in § 170.315(b)(11)(vi) to ''Enable a user to review a plain language description of source attribute information as indicated and at a minimum via direct display, drill down, or link out from a Health IT Module . . . .'' The finalized ''access'' requirement states in § 170.315(b)(11)(v)(A)(*1*) that for evidence-based and Predictive DSIs supplied by the health IT developer, the Health IT Module must enable a limited set of identified users to access complete and up-to-date plain language descriptions of source attribute information specified in § 170.315(b)(11)(iv)(A) and (B) as finalized. As discussed earlier, we have not finalized proposed requirements for Health IT Modules to make source attribute information available via direct display, drill down, or link out.

Second, we have finalized at § 170.315(b)(11)(v)(A)(*2*) that for Predictive DSIs supplied by the health IT developer as part of its Health IT Module, the Health IT Module must

indicate when information is not available for review for source attributes in paragraphs (b)(11)(iv)(B)(*6*); (b)(11)(iv)(B)(*7*)(*iii*), (*iv*), and (*v*); (b)(11)(iv)(B)(*8*)(*ii*) and (*iv*); and (b)(11)(iv)(B)(*9*). This requirement is finalized as a modified version of what was proposed at § 170.315(b)(11)(vi)(D)(*1*) and § 170.315(b)(11)(vi)(D)(*2*), which required Health IT Modules to indicate a source attribute is missing if the source attribute included the ''if available'' phrase. We clarify that per conformance with this certification criterion and its associated maintenance of certification requirement adopted as part of § 170.402(b)(4), if and when information related to these source attributes are generated, the developer of certified health IT must make this information available to users. For example, if the developer of certified health IT gets newly available information on the validity of the intervention in local data (§ 170.315(b)(11)(iv)(B)(*8*)(*ii*)) following the deployment of a Predictive DSI, that information must be made available as source attributes information to reflect up-to-date descriptions of source attributes.

Third and fourth, we have finalized two requirements related to the ability to ''modify'' source attributes and source attribute information at § 170.315(b)(11)(v)(B). At § 170.315(b)(11)(v)(B)(*1*), we have finalized a requirement that for evidence-based DSIs and Predictive DSIs, the Health IT Module must enable a limited set of identified users to record, change, and access source attributes in paragraphs (b)(11)(iv)(A) and (B) of this section. At § 170.315(b)(11)(v)(B)(*2*) we have finalized that, for Predictive DSIs, a Health IT Module must enable a limited set of identified users to record, change, and access additional source attributes not specified in § 170.315(b)(11)(iv)(B). These requirements are substantially similar to what we proposed in § 170.315(b)(11)(vi)(E) while retaining the ability to access or review this information as would have been required in proposed § 170.315(b)(11)(v). In proposed § 170.315(b)(11)(vi)(E) we proposed that a Health IT Module must enable a limited set of identified users to ''author and revise,'' source attribute information beyond source attributes listed. We note that the capability to record and change replaces the proposed capability to author and revise.

Comments. Commenters requested guidance on the level of detail required in these descriptions and specification of ''plain language descriptions'' for which audience (*e.g.,* developers, clinicians, and other end-users) and guidelines on how to present this information, noting the concern that a user may have difficulty finding the required documentation depending on how the interface is designed. Commenters expressed concern that the proposal to enable a user to review a plain language description of source attribute information could result in legal liability and vulnerability for clinicians and health care providers, underscoring the need that the information provided in the new source attributes for Predictive DSI are useful and understandable.

Response. We thank commenters for their concerns. We note that requirements related to a plain language description are now included at § 170.315(b)(11)(v)(A)(*1*). When we indicate ''plain language description,'' we mean language that the intended audience can readily understand and use because that language is clear, concise, well-organized, accurately describes the information, and follows other best practices of plain language writing. We encourage model developers to consider what information would be useful for users to determine if a Predictive DSI is FAVES without providing difficult to understand technical details. We agree that providing this information in a useful form will be essential. Comments regarding legal liability are outside the scope of this rulemaking. Therefore, we decline to finalize any such change.

Comments. One commenter requested clarity regarding cases where third-party IT that is enabled or interfaced with certified health IT but is modified by users or a different third-party developer such that the added functionality results in the generation of a Predictive DSI, and whether such cases would be subject to conditional requirements for source attributes listed in § 170.315(b)(11)(vi)(A) and deployment of or engagement in intervention risk management practices discussed in § 170.315(b)(11)(vii).

Response. In a scenario where an *other party* technology is modified by a different *other party (e.g.,* users or a different third-party developer) such that the initial technology meets the definition of a Predictive DSI, we would categorize the modified technology as a Predictive DSI developed by an *other party.* A Health IT Module may be expected to have the technical capability for users to record, change and access source attributes of this modified technology, and may be expected to provide up-to-date source attribute information if the Predictive DSI is supplied by the developer of certified health IT as part of the Health IT Module.

vii. Source Attributes—Demographic, SDOH, and Health Status Assessment Data Use

We proposed at 88 FR 23787 to include as source attributes in § 170.315(b)(11)(vi)(A)(*1*) through (*4*) the source attributes currently found in § 170.315(a)(9)(v)(A)(*1*) through (*4*). Additionally, we proposed that the use of three additional specific types of data in a DSI be included as source attributes in § 170.315(b)(11)(vi)(A)—Demographic data elements in § 170.315(b)(11)(vi)(A)(*5*), SDOH data elements in § 170.315(b)(11)(vi)(A)(*6*), and Health Status Assessment data elements in § 170.315(b)(11)(vi)(A)(*7*). We noted at 88 FR 23787 that ''types of data in a DSI'' means that the DSI includes any of these data as inputs or otherwise expressly rely on any of these data in generating an output or outputs. We explained that by proposing to modify the source attributes as part of proposed § 170.315(b)(11)(vi)(A) relative to the existing attributes in § 170.315(a)(9)(v)(A), we expected that information would be made available to users if the specific data elements within these three data categories were used in the DSI.

Context note. We note for readers that while all of the proposals just summarized were part of proposed § 170.315(b)(11)(vi), we have finalized modified versions of these requirements as part of § 170.315(b)(11)(iv)(A). As a result, we discuss the finalized requirements with that context in mind.

Comments. The majority of commenters supported the proposal to include the requirement that certified Health IT Modules should provide users with source attributes for DSI, including the three additional specific types of data of demographic, SDOH, and health status assessment data elements. These commenters stated that it would have the benefit of enabling individuals and organizations to understand the nature of certified health IT, whether there are inherent biases, and how best to use the technology for a specific patient population. Commenters also stated that requiring developers of certified health IT to report on these data elements' inclusion will assist providers in both ensuring the whole patient is cared for and that there is transparency as part of that whole-person care. Commenters noted that the proposed requirements would address pressing concerns that AI algorithms can reinforce biases related

to socioeconomic status, race, ethnicity, sexual orientation, gender identity, sex, and other identities and conditions, observing that recent advances in AI stand to potentially harm patients by reinforcing implicit and explicit biases that do not reflect the diverse population of America and that may only increase health inequities. Commenters supported the public transparency requirements for source attribute information as an important measure to avoid exacerbating these inequities.

A minority of commenters did not support the proposal stating that the HTI–1 Proposed Rule would create significant implementation burden with unclear benefits. One commenter suggested that the HTI–1 Proposed Rule may also paradoxically increase disparities by reducing innovation and the implementation of DSIs due to increased regulatory burden. One commenter expressed concern that the preamble was unclear on what it meant for an evidence-based decision support intervention to ''use'' or ''include'' patient demographics and observations, SDOH, or health status assessments.

Response. We thank commenters for their support and agree that by highlighting when an evidence-based DSI uses patient demographics, SDOH, or health status assessments data elements,[115] users are empowered to interrogate and ensure that the DSI is appropriate. We believe that identification of race, ethnicity, language, age (date of birth), sexual orientation, gender information, SDOH, and health status assessments, such as disability, data elements, if included as part of an evidence-based DSI, would greatly improve the possibility of identifying and mitigating the risks of employing evidence-based DSIs for patient care, including those related to exacerbating racial disparities and promoting bias. We believe that this requirement represents a low burden that is unlikely to reduce innovation and implementation of DSIs. We also thank commenters for identifying ambiguities in what it means for an evidence-based decision support intervention to ''use'' or ''include'' these data elements. We clarify that our intention is to enable a user to understand if one or more of these data elements are included as inputs or otherwise expressly relied upon to generate an output in an evidence-based DSI. We also intend that, if the data elements are included, the user is informed which one(s) are used in the evidence-based DSI. This means that a user must be able to review whether a data element relevant to those categories in § 170.315(b)(11)(iv)(A)(*5*)–(*13*) (as expressed by the standards in § 170.213) is used in the evidence-based DSI, and if so, which specific data element or elements are used in the evidence-based DSI.

We do not prescribe how this information is communicated to a user, nor do we prescribe a minimum level of context at this time. For example, we do not require that a source attribute indicating the use of an SDOH data element in § 170.315(b)(11)(iv)(A)(*6*) must describe *how* the data element is used as part of the evidence-based DSI. Instead, we require a Health IT Module to enable a user to review whether an SDOH data element is used as part of the evidence-based DSI and which SDOH data element (as expressed by the standards in § 170.213) is used as part of the evidence-based DSI.

After consideration of comments, we have finalized as part of § 170.315(b)(11)(iv)(A) patient demographic, SDOH, and health status assessment data elements in § 170.315(b)(11)(iv)(A)(*5*) through (*13*) as expressed in the standards in § 170.213. We note that, consistent with the dates established in § 170.213, compliance with USCDI v1 will be required to initially meet this certification criterion until compliance with USCDI v3 becomes required as part of this certification criterion (*i.e.,* January 1, 2026). As a result, for the first compliance date associated with § 170.315(b)(11) a Health IT Module may include, but is not required to include, identification of the use of patient demographic data elements that are only found in USCDI v3 as part of evidence-based DSIs in § 170.315(b)(11)(iv)(A)(*5*)–(*13*).

Comments. Several commenters responded to our solicitation for comment on whether we should require a certain format or order in which these source attributes must appear to users. Commenters noted that the proposed source attribute requirements would require each organization to craft their own documentation process and suggested that ONC collaborate with interested parties to implement and refine a standards-based approach for capturing and sharing source attributes, including sharing both machine-readable and human-readable tables/lists of DSI source attribute information. Commenters also observed that requiring information about DSIs to be submitted in a standard format will focus the scope of the information disclosed, create consistency in the kind of information shared about these AI tools, and contribute to a presentation of this information for end users that is repeatable and digestible. Commenters noted that without a standardization and strategic placement, providers moving across organizations will experience the added stress of learning each organization's method of addressing DSI, compounding burden. One commenter supported including HL7 consensus-based implementation guides for AI information, and another commenter recommended that ONC should produce a document format for DSI developers to use in conveying information to EHR developers and interface specialists. One commenter suggested that there are two common ways to present this type of long list of data: alphabetically or by type (often organized alphabetically underneath each category) and recommended categorizing by type of data then presenting each list therein alphabetically. For example: Demographic Data: date of birth, race, sex Health Status: disability status, smoking status.

One commenter observed that to implement a standardized format may be burdensome for health IT developers but also will be beneficial to reduce bias in decision making and will encourage smaller, third-party applications to be more transparent and responsible in their development, stating that there are potential benefits to requiring documentation of what a clinical decision support algorithm does, and provides certainty that a level of testing and trials has been done to ensure the relevance and accuracy of the model.

Response. We appreciate the comments received regarding a standardized format for source attribute information. We noted in the HTI–1 Proposed Rule that we were not aware of widely agreed upon best practices for the format in which these elements or source attributes information should be displayed. We are also not aware of a consensus-based standardized format that might best meet the objective described by the commenter to reduce bias in decisions making. However, we are aware of industry efforts to standardize a format to display information about technology in the form of a ''model card'' or ''nutritional label'' for healthcare (88 FR 23794). We did not propose a specific format for source attributes, and we decline to finalize any specific formats. We believe

[115] For purposes of this final rule, health status assessments are assessments of a health-related matter of interest, importance, or worry to a patient, patient's family, or patient's health care provider that could identify a need, problem, or condition. See ONC's Interoperability Standards Advisory (ISA) at *https://www.healthit.gov/isa/uscdi-data-class/health-status-assessments#uscdi-v3.*

this represents an ideal space for interested parties across industry, academia, government, and the non-profit sector (such as SDOs and patient advocacy organizations) to collaborate. We note that part of our rationale for being flexible in the use of standardized formats and placement of source attributes within users' workflows is precisely because there is a lack of consensus. We look forward to working with interested parties to develop consensus-based standards across numerous and far-reaching types of use cases.

viii. Source Attributes for Predictive Decision Support Interventions

At 88 FR 23788–23795, we proposed source attributes applicable for all Predictive DSIs that are enabled by or interface with certified Health IT Modules certified to § 170.315(b)(11). These source attributes were intended to provide users with greater insight into the model incorporated into a particular Predictive DSI and intended to provide information for an array of uses, including in support of so-called ''model cards'' or algorithm ''nutrition labels'' that have been described by others.[116] This proposed requirement applied to developers of certified health IT that attest ''yes'' in § 170.315(b)(11)(v)(A).

We noted that the proposals for source attributes would not require disclosing or sharing intellectual property (IP) existing in the developer's health IT, including *other parties'* IP. We reiterated that source attributes in § 170.315(b)(11)(vi) would not require disclosure of proprietary information or IP (88 FR 23788). We also noted that if developers of certified health IT would like to include a capability for *other parties* to record source attributes into a Health IT Module in a way that shields the developer of certified health IT from having access to the *other party* source attributes, they could do so, but that this was not proposed as a required technical capability within the proposed criterion.

New Source Attributes for Predictive DSI

At 88 FR 23789, we proposed to add fourteen new source attributes for Predictive DSIs that enable or interface with Health IT Modules. Consistent with our proposals in § 170.315(b)(11)(vi), we proposed that these new source attributes listed in § 170.315(b)(11)(vi)(C) would be in plain language and available for user review via direct display, drill down, or link out from a Health IT Module certified to § 170.315(b)(11) and for which the developer attested ''yes'' in § 170.315(b)(11)(v)(A).

We clarified that we proposed to require that developers must enable a user to review a plain language description of source attribute information as indicated and at a minimum via direct display, drill down, or link out from a Health IT Module and that information on these source attributes must be provided by the developer of certified health IT unless the attribute contained the phrase ''if available'' (discussed at 88 FR 23789) or was developed by an *other party,* as proposed at § 170.315(b)(11)(vi)(D) discussed at 88 FR 23795–23796.

Context note. We note for readers that while all of the proposals just summarized were part of proposed § 170.315(b)(11)(vi)(C), we have finalized modified versions of these requirements as part of § 170.315(b)(11)(iv)(B). As a result, we discuss the finalized requirements with that context in mind.

Comments. Commenters were mixed in their support or opposition to requirements for source attributes for Predictive DSI, with those in support noting that it would create greater transparency for patients and providers that is key to building trust in AI. Commenters who were supportive noted that it would be critical for the end user to understand how a Predictive DSI is developed, evaluated, and how it should be used appropriately. Commenters also noted that health care providers would benefit because transparency promotes the exercise of a provider's judgment at the point of care, which can help avoid errors and mitigate algorithmic biases, and that source attributes will help organizations make informed decisions around potential implementation. One commenter noted that complex predictive models that incorporate difficult-to-observe validity or fairness issues may lead to harm if left unchecked, resulting in bias that can lead to decisions that can have a collective, disparate impact on certain groups of people even without the programmer's intention to discriminate.

Response. We thank commenters for their feedback and their support. As expressed in our proposals for § 170.315(b)(11), we believe that transparency is a prerequisite for high-quality Predictive DSIs to be trusted by clinicians, patients, health systems, software developers, and other interested parties. We believe that transparency can help to reduce the harm of complex predictive models by informing the use, disuse, updating or decommissioning of such models. As described in more detail below, we have finalized in § 170.315(b)(11)(iv)(B) modified versions of our proposals for Predictive DSI-specific source attributes.

Comments. Several commenters did not support our proposal, with many expressing concerns that our proposal is too prescriptive and limiting to industry innovation, the source attribute categories and disclosure requirements create unnecessary burden on health IT developers and providers, and stifle competition. Several commenters were concerned that the proposed source attribute disclosure requirements could compromise patient privacy and requested clarification on the granularity of data elements that developers must disclose. Commenters recommended ONC limit the type of data that is made publicly available from high-impact DSIs to protect patient information privacy and security and safeguard protected health information (''PHI'') or sensitive data.

Response. We respectfully disagree with these commenters. In developing proposed source attributes for Predictive DSIs, we sought a balance between limited prescriptiveness and sufficient detail to enable thorough transparency of source attribute information to users. Our selection of the proposed attributes was guided by reviews of existing model reporting guidelines, including seventeen different sets of industry- and academia-developed recommendations for information to be reported on models and related standards.[117]

[116] Mitchell, Margaret, et al. ''Model cards for model reporting.'' Proceedings of the conference on fairness, accountability, and transparency. 2019.

[117] Scott, Ian, Stacy Carter, and Enrico Coiera. ''Clinician checklist for assessing suitability of machine learning applications in healthcare.'' *BMJ Health & Care Informatics* 28.1 (2021).

Liu X, Cruz Rivera S, Moher D, Calvert MJ, Denniston AK; SPIRIT–AI and CONSORT–AI Working Group. Reporting guidelines for clinical trial reports for interventions involving artificial intelligence: the CONSORT–AI extension. *Nat Med.* 2020;26(9):1364–1374. doi:10.1038/s41591–020–1034–x.

Moons KGM, Kengne AP, Woodward M, et al. Risk prediction models, I: development, internal validation, and assessing the incremental value of a new (bio)marker. *Heart.* 2012;98(9):683–690. doi:10.1136/heartjnl–2011–301246.

Rivera SC, Liu X, Chan AW, Denniston AK, Calvert MJ; SPIRIT–AI and CONSORT–AI Working Group. Guidelines for clinical trial protocols for interventions involving artificial intelligence: the SPIRIT–AI Extension. *BMJ.* 2020;370:m3210. doi:10.1136/bmj.m3210.

Steyerberg EW, Vergouwe Y. Towards better clinical prediction models: seven steps for development and an ABCD for validation. *Eur Heart J.* 2014;35(29):1925–1931. doi:10.1093/eurheartj/ehu207.

Moons KGM, de Groot JAH, Bouwmeester W, et al. Critical appraisal and data extraction for

Continued

Because these guidelines are designed to support innovation and competition in the development and validation of predictive models in the academic literature, we believe that their use will similarly leave sufficient space for innovation by a variety of entities. In our review, we emphasized attributes that: (1) were most commonly included in the reviewed reporting guidelines; (2) we believed would be most interpretable by both health IT professionals and users; (3) were focused on identifying issues of bias; and (4) were intended to show that the model would perform effectively outside of the specific context in which it was developed. In finalizing Predictive DSI source attributes in § 170.315(b)(11)(iv)(B), we have provided information on what we believe should be included in each attribute based on our understanding of the current best practices in this area. However, given the varied technologies, applications, and contexts in which Predictive DSIs may be used, we have sought to keep requirements sufficiently flexible to meet varied use cases. We note that under that this policy establishes different requirements for developers of certified health IT that supply Predictive DSIs versus those certified health IT developers that do not supply Predictive DSIs. Many developers of certified health IT that do not supply a Predictive DSI as part of their Health IT Module are among those developers with smaller revenues and fewer clients. These developers will be able to certify to the criterion at § 170.315(b)(11) while expending limited additional development resources on products they have certified currently. Specifically, these developers will likely have no costs related to providing complete and up-to-date source attribute information for Predictive DSI supplied by the developer or engaging in risk management and annually update risk management information.

We believe that our finalized Predictive DSI source attributes strike a balance between prescriptiveness and flexibility that is necessary to foster a nascent information ecosystem that can help users understand whether the Predictive DSI they are using (as supplied by their health IT developer as part of its Health IT Module) is FAVES. Moreover, we believe these source attributes help establish a consistent transparency baseline, or foundation, especially given that we have not established requirements for specific measures. Rather, we encourage industry, academic, professional associations, and other interested parties to determine which information best fits each use case. We also do not believe that the information in source attributes creates a risk to patient privacy, given the level of detail at which information should be provided, as described in more detail in response to concerns related to intellectual property. We also note that we are affording flexibilities related to source attributes that are only required once information for them become available, such as source attributes related to validity and fairness of prediction in external and local data. We have finalized the categories of source attributes related to Predictive DSIs at § 170.315(b)(11)(iv)(B) with modifications and clarifications to source attribute category subparagraphs, described below in this final rule.

Comments. Several commenters, including health information technology companies, insurance companies, software developers, and professional trade associations, expressed concerns that providing users with access to information described as part of source attributes would expose proprietary information regarding the predictive algorithm or model and risk exposing intellectual property (IP) among other risks, including that disclosure of such information would stifle competition and innovation. Some commenters suggested ONC specify that the information in our proposals does not include confidential information such as IP. Some commenters were concerned that source attributes could enable reconstruction of the algorithm and that it would create a power imbalance between small and startup ''*other parties*'' and large incumbent developers of certified health IT, which could either refuse to display source attributes from *other parties* or use information in those source attributes inappropriately. While many commenters were vague in their concerns related to revealing IP and trade secrets a small number of commenters identified the ''Intervention Development'' category of source attributes as problematic and another commenter noted that the output of the intervention would constitute IP. During further fact-finding, commenters mentioned specific concerns around source attribute information on how input and output variables were identified, as well as the model parameters, hyperparameters, or the results of tuning, which they described as crucial pieces of intellectual property, proprietary information, or trade secrets. Another commenter included ''model type, target definition (intended use), and inputs'' as information that could include IP or proprietary information.

Several commenters suggested ways to mitigate IP and proprietary information concerns, including listing data classes instead of data elements used in the algorithm; limiting source attribute information to summary information for high-risk use cases only; limiting source attribute requirements to algorithms developed by developers of certified health IT; requiring only links to DSIs centrally supported by a government-sponsored resource and to information maintained by the FDA if the DSI is regulated as a medical device; and giving developers the ability to exclude or redact source attribute

---

systematic reviews of prediction modelling studies: the CHARMS checklist. *PLoS Med.* 2014;11(10):e1001744.

Collins GS, Reitsma JB, Altman DG, Moons KGM. Transparent Reporting of a Multivariable Prediction Model for Individual Prognosis or Diagnosis (TRIPOD): the TRIPOD statement. *Br J Surg.* 2015;102(3):148–158.

Cohen JF, Korevaar DA, Altman DG, et al. STARD 2015 guidelines for reporting diagnostic accuracy studies: explanation and elaboration. *BMJ Open.* 2016;6(11):e012799. doi:10.1136/bmjopen-2016–012799.

Luo W, Phung D, Tran T, et al. Guidelines for developing and reporting machine learning predictive models in biomedical research: a multidisciplinary view. *J Med internet Res.* 2016;18(12):e323. doi:10.2196/jmir.5870.

Breck E, Cai S, Nielsen E, Salib M, Sculley D. The ML Test Score: a rubric for ML production readiness and technical debt reduction. *Proceedings of the 2017 IEEE International Conference on Big Data.* December 11–14, 2017:1123–1132. doi:10.1109/BigData.2017.8258038.

Wolff RF, Moons KGM, Riley RD, et al; PROBAST Group†. PROBAST: a tool to assess the risk of bias and applicability of prediction model studies. *Ann Intern Med.* 2019;170(1):51–58. doi:10.7326/M18–1376.

Mitchell M, Wu S, Zaldivar A, et al. Model Cards for model reporting. In: *Proceedings of the Conference on Fairness, Accountability, and Transparency.* Association for Computing Machinery; January 29, 2019.

Sendak MP, Gao M, Brajer N, Balu S. Presenting machine learning model information to clinical end users with model facts labels. *NPJ Digit Med.* 2020;3:41. doi:10.1038/s41746–020–0253–3.

Hernandez-Boussard T, Bozkurt S, Ioannidis JPA, Shah NH. MINIMAR (Minimum Information for Medical AI Reporting): developing reporting standards for artificial intelligence in health care. *J Am Med Inform Assoc.* 2020;27(12):2011–2015.doi:10.1093/jamia/ocaa088.

Norgeot B, Quer G, Beaulieu-Jones BK, et al. Minimum Information About Clinical Artificial Intelligence Modeling: the MI–CLAIM checklist. *Nat Med.* 2020;26(9):1320–1324. doi:10.1038/s41591–020–1041–y.

Silcox C, Dentzer S, Bates DW. AI-enabled clinical decision support software: a ''trust and value checklist'' for clinicians. *NEJM Catalyst.* 2020;1(6). doi:10.1056/CAT.20.0212.

Vasey, Baptiste, et al. ''Reporting guideline for the early-stage clinical evaluation of decision support systems driven by artificial intelligence: DECIDE–AI.'' *Nature medicine* 28.5 (2022): 924–933.

information they considered proprietary.

Response. As described in detail below, we respectfully disagree with the claims that our proposed, and now final, requirements for source attributes in § 170.315(b)(11)(iv)(B) would result in disclosures of IP, trade secrets, or proprietary information. Nor do we believe that our requirements for source attributes would stifle competition and innovation. Given the overall scope changes and numerous clarifications offered through this final rule to narrow health IT developer's scope of responsibilities (to only those Predictive DSIs that are supplied as part of its Health IT Module) we believe we have substantively address commenters' concerns regarding exposure of proprietary information to *other parties* as well as exposure to proprietary information originating from *other parties.* Additionally, we believe that the transparency needs are so acute for Predictive DSIs that the public benefit outweighs any remaining concerns. Overall, we anticipate that better information regarding Predictive DSIs will bolster the use of high-quality, fair, appropriate, valid, effective, and safe predictive algorithms across the healthcare landscape.

First, we do not agree that the information we require for Predictive DSI source attributes is new or novel within the healthcare context, presenting authors of Predictive DSIs with new or novel concerns related to IP or proprietary information. We note that we analyzed and drew from more than a dozen widely accepted and used reporting guidelines, used by researchers and developers to demonstrate the validity of algorithms in peer-reviewed literature.[118] We believe that much of the same information required for publication by the *New England Journal of Medicine* or the *Journal of the American Medical Association,* for example, ought to be routinely and consistently available for user review to improve the trustworthiness of Predictive DSIs. We note that some reporting guidelines, from which we draw our own source attributes, have more than 15,000 citations across peer-reviewed, academic literature.[119]

Second, we have clarified the scope of our requirements by adding detail to the information expected as part of source attributes in what is now finalized at § 170.315(b)(11)(iv)(B). We note that these explicit requirements in regulation text mirror the requirements described previously in preamble or represent a subset of requirements previously described in preamble. The information required in source attributes is not intended to include detailed information on model parameters, hyperparameters, detailed specifics around how input or output variables are defined, transformed, or otherwise operationalized. We do not believe that information at that level of detail is necessary for source attributes in § 170.315(b)(11)(iv)(B) or necessary for users of a Predictive DSI to determine whether it is fair, appropriate, valid, effective, and safe.

Third, as it relates to ''Intervention Development,'' source attributes, which include input features, such as exclusion and inclusion criteria that influenced the data set; use of race, ethnicity, language (REL), SDOH, and health assessment variables as input features; and a description of relevance of training data to intended deployed setting, we note that these source attributes are important to give users a sense of whether they ought to use the Predictive DSI on an individual in front of them, or on individuals generally seen within the user's organization. Understanding whether specific input features, such as race, sex, or food insecurity is part of the training data set for a Predictive DSI could present a user with critical information on its relevance and validity to individual patients or patient cohorts for which the Predictive DSI is being applied. We further ask in § 170.315(b)(11)(iv)(B)(*4*)(*iii*) for some sense of how representative demographic variables are within a Predictive DSI's training data set, which could be equally important if the Predictive DSI was trained on data dominated by one racial group and applied to a different group.

To further mitigate concerns around IP, we have limited the input features that must be included to those listed at § 170.315(b)(11)(iv)(A)(*5*)–(*13*). We understand that resources are expended to identify and operationalize numerous input features to improve Predictive DSI performance. We believe this list narrows the scope of features that must be reported and addresses concerns about revealing IP underlying curation of input features more broadly. Furthermore, in developing information for source attributes, we encourage model developers to consider the level of information that would be useful for health systems and end users to best determine if a Predictive DSI is FAVES without providing difficult to understand technical details that might reveal trade secretes or proprietary information. We also reiterate that information provided should be described in plain language, as stated at § 170.315(b)(11)(v)(A)(*1*).

We disagree with commenters concerns that identifying the output of the intervention would constitute IP. We provided an example of a prediction of the likelihood that an individual will be readmitted among individuals recently discharged (88 FR 23789). We do not believe that the description of an output, at the low level of detail provided in the example, is likely to constitute intellectual property or trade secrets. We believe that a description of the output produced by the model, along with ''intended use,'' is foundational to understanding how the model is meant to be deployed and used.

Fourth, we appreciate the many commenters that raised IP and proprietary information concerns while also providing ways to mitigate those concerns, primarily by limiting the number or the scope of source attributes that should be available to users. Based on the scope changes to final § 170.315(b)(11) and other clarifications issued throughout this final rule, we have not finalized additional mitigation suggestions by commenters. We believe that the clarifications provided as part of this response on the level of detail required for source attributes (as well as other corresponding responses below) will sufficiently mitigate concerns related to IP.

Last, while we understand concerns raised by commenters regarding a potential to create a power imbalance between small and startup ''*other parties*'' and large incumbent developers of certified health IT, which could either refuse to display source attributes from *other parties* or use information in those source attributes inappropriately, we believe our finalized scope for Predictive DSI source attributes addresses these concerns. Particularly, we note that these source attributes must be complete and up-to-date if they are supplied by the health IT developer as part of its Health IT Module. In this scenario, *other party* source attributes could be directly supplied to a developer certified health IT's customer (who will have both the ability to select this *other party's* Predictive DSI and have a Health IT Module support Predictive DSI source attribute categories for the *other party's* source attributes, even if their developer

[118] See footnote 117.

[119] Table 1. Summary of 15 Model Reporting Guideline Papers. Lu JH, Callahan A, Patel BS, et al. Assessment of Adherence to Reporting Guidelines by Commonly Used Clinical Prediction Models From a Single Vendor: A Systematic Review. *JAMA Netw Open.* 2022;5(8):e2227779. doi:10.1001/jamanetworkopen.2022.27779.

does not supply a Predictive DSI as part of its Health IT Module, due to requirements at § 170.315(b)(11)(iii)(B) and § 170.315(b)(11)(iv)(B)). Further, if developer of certified health IT a with Health IT Module certified to § 170.315(b)(11) would like to include a capability for *other parties* to record source attributes into a Health IT Module in a way that shields the developer of certified health IT from having access to the other party source attributes, the developer of certified health IT may do so.

Comments. Several commenters were concerned that our proposal requires health IT software developers to expend significant resources to gather information from numerous sources and is an unnecessary burden. Specifically, commenters noted that requiring developers of certified health IT to monitor, catalog, request information, and conduct analysis requires significant resources that will need to be redirected from development, enhancement, and assessment of its own software.

Response. We appreciate the comment and as part of this final rule we have substantially reduced the scope of the final requirements to be fully within the developer of certified health IT's purview, such that the developer will know and be able to fully estimate the resources it will need to expend to maintain complete and up-to-date source attribute information (which could be limited if, for example, the developer does not supply any Predictive DSIs as part of its Health IT Module). We appreciate the comment and as part of this final rule we have substantially reduced the scope of the finalized requirements to be fully within the developer of certified health IT's purview, such that the developer will know and be able to fully estimate the resources it will need to expend to maintain complete and up-to-date source attribute information (which could be limited if, for example, the developer does not supply any Predictive DSIs as part of it Health IT Module). We also believe that this scope and associated information is necessary for the trustworthy use of Predictive DSIs and that the benefits will be commensurate with the burden implied. As stated numerous times throughout the preamble, our intention in requiring such work is to better ensure that high quality Predictive DSIs can be more effectively used to improve patient care.

Given the many comments received from interested parties, we have limited the source attributes that developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) are required to complete and keep current to those that are related to Predictive DSIs supplied by the developer of certified health IT, which we believe would limit the resources required to gather information from *other parties.* We describe in further detail these requirements in subsequent responses in this final rule. We reiterate that Health IT Modules must support the capability for *other party* source attribute information to be accessible to users, but that developers are not required to receive or proactively acquire such information for user access from these *other parties* just because a user selects (*i.e.,* activates) a Predictive DSI using the developer's Health IT Module.

Comments. Some commenters recommended that the requirements should be limited to require summary information of source attributes and only for high-impact Predictive DSI that presents a greater risk of potential harm. One commenter recommended that ONC should take a risk-based approach and limit Predictive DSIs in scope and exclude low-risk use cases for consumers, such as general wellness.

Response. We appreciate the comments. However, the Program is not predicated on levels of risk that a technology may pose. As previously noted, we believe that identifying whether a Predictive DSI is ''high-risk'' or could have a ''high-impact'' across millions of patients is not appropriate for this rulemaking because Predictive DSIs that may in some sense be ''low-risk,'' such as those that predict appointment no-shows can (in some cases indirectly) impact the healthcare of millions of individuals and thereby be ''high-impact.'' We also believe that it is important to require the same information for Predictive DSIs supplied by developers of certified health IT. We reiterate that we have not established requirements for specific measures of validity or fairness, for example. Rather, we encourage industry, academic, professional associations, and other interested parties to determine which information best fits each use case. For instance, a radiological or oncologic society might develop recommendation on how to measure fairness for a Predictive DSI that predicts onset of melanoma in diverse populations, and we encourage the use of those measures as they continue to be refined. We are also aware of ongoing work to standardize approaches to select specific measures and performance targets and encourage developers to follow those best practices.[120] We believe our requirements at § 170.315(b)(11)(iv)(B) are consistent with industry and academia-developed reporting guidelines, and are appropriately balanced and flexible, while ensuring a consistent baseline of information users need to make informed decisions regarding their use of a Predictive DSI.

Comments. Several commenters expressed concerns that our proposal was duplicative of FDA requirements, noting that they believed our proposal imposes duplicative and unnecessary requirements for software solely based on its use within certified health IT, creating additional burdens for device manufacturers who are also regulated by the FDA. Commenters expressed concern regarding the existing authority that the FDA has over device CDS, which may result in a duplication of efforts with differing requirements, meaning providers and EHR vendors would need to satisfy two sets of regulations. One commenter noted that they believe that in some instances, publication of source attribute information distinct from existing labeling could require supplemental FDA authorization. Some commenters suggested that regulating source attributes would be accomplished more effectively by the FDA.

Response. We appreciate the concerns expressed by these commenters, which is why we worked closely with the FDA on development of our proposals in § 170.315(b)(11), especially regarding Predictive DSI-specific source attributes. We are aware that technologies that meet the definition for Predictive DSI within the Program may be considered Non-Device CDS, be considered CDS with device software functions, or lie outside of FDA's purview, depending on the specifics of the technology. We worked with the FDA expressly to minimize duplication of effort and maximize alignment across our distinct and different authorities.

We coordinated with FDA to ensure that the information required within source attributes in our finalized § 170.315(b)(11) is complementary and not conflicting with the information that FDA describes in its CDS Guidance, finalized in September 2022.[121] Specifically, we believe that both (1) the

[120] Health AI Partnership. ''Define performance targets,'' *https://healthaipartnership.org/guiding-question/define-performance-targets* Data Science and Public Policy, Carnegie Mellon University. ''Aequitas'' *http://www.datasciencepublicpolicy.org/our-work/tools-guides/aequitas/.*

[121] See *https://www.fda.gov/regulatory-information/search-fda-guidance-documents/clinical-decision-support-software.*

content of the information described for source attributes in § 170.315(b)(11)(iv) and (2) the capabilities required in § 170.315(b)(11)(iii) and § 170.315(b)(11)(v) are complementary and aligned with FDA CDS guidance and could reduce burdens for entities that develop device software functions that also meet the definition of Predictive DSI.

We note that section 520I(1)(E) of the Food Drug & Cosmetics (FD&C) Act (Pub. L. 75–717, Jun. 1938) excludes from the definition of ''device,'' software functions that, among other things, are intended for the purpose of enabling a healthcare professional to independently review the basis for recommendations that such software presents. As part of this alignment effort across both FDA and ONC regulatory requirements, we identified and have finalized source attribute information that could plausibly address some of the informational requirements in 520I(1)(E)(iii) of the FD&C Act, including:

- § 170.315(b)(11)(iv)(B)(*2*) Purpose of the intervention, including: (*i*) Intended use of the intervention; (*ii*) Intended patient population(s) for the intervention's use; (*iii*) Intended user(s); and (*iv*) Intended decision-making role the intervention was designed to be used/for (*e.g.,* informs, augments, replaces clinical management).
- § 170.315(b)(11)(iv)(B)(*4*) Intervention development details and input features, including at a minimum: (*i*) Exclusion and inclusion criteria that influenced the data set; (*ii*) Use of variables in 170.315(b)(11)(iv)(A)*(5)–(13)* as input features; (*iii*) Description of demographic representativeness according to variables in § 170.315(b)(11)(iv)(A)*(5)–(13)* including, at a minimum, those used as input features in the intervention; and (*iv*) Description of relevance of training data to intended deployed setting.
- § 170.315(b)(11)(iv)(B)(*7*) Quantitative measures of performance, including: (*i*) Validity of intervention in test data derived from the same source as the initial training data; and (*v*) References to evaluation of use of the intervention on outcomes, if available, including, bibliographic citations or hyperlinks to evaluations of how well the intervention reduced morbidity, mortality, length of stay, or other outcomes.

We believe that these similarities will reduce compliance burden in three ways. First, an entity that develops device software functions that also meet the definition of Predictive DSI would be able to fulfill informational requirements for both FDA and ONC purposes using the same or similar information. Second, an entity that develops device software functions that also meet the definition of a Predictive DSI may be eligible to be considered Non-Device CDS according to FDA guidance, if the developer of the Predictive DSI fulfils informational requirements according to Program requirements in § 170.315(b)(11) and § 170.402(b)(4). Specifically, we note that the capability to enable a limited set of identified users to select evidence-based DSIs and Predictive DSIs in § 170.315(b)(11)(iii) and access source attributes for these DSIs in § 170.315(b)(11)(v) could be the technical mechanism by which technologies meet requirements in section 520I(1)(E)(iii) of the FD&C Act, described as Criterion 4 of the FDA CDS guidance. Finally, we believe that burdens will be reduced across entities regulated by FDA and ONC because an entity that develops device software functions that also meet the definition of a Predictive DSI could leverage Program requirements to enable users to select Predictive DSIs in § 170.315(b)(11)(iii) and access source attribute information in § 170.315(b)(11)(v). These capabilities could serve as the technical means to deliver information to users about the credibility of the device software function that is necessary for ''independent review,'' without having to build a parallel technological means to deliver such information.

For example, for those software functions that are considered non-device CDS, and therefore are not the focus of the FDA's regulatory oversight, our source attribute requirements are complementary to the required factor ''intended for the purpose of enabling such healthcare professional to independently review the basis for such recommendations that such software presents so that it is not the intent that such healthcare professional rely primarily on any of such recommendations to make a clinical diagnosis or treatment decision regarding an individual patient'' (section 520I(1)(E)(iii) of the FD&C Act). In this case, our requirements are supportive of meeting aspects which may be part of determining that a Predictive DSI is not a medical device and therefore not the focus of the FDA's oversight.

For those CDS software that are medical devices and the focus of the FDA's oversight, we note our requirements are consistent with best practices and recommendations similarly provided by the FDA. In such cases, as these recommendations are consistent across our agencies, we believe that providing such information should not increase burden on developers who may be responsible for meeting both FDA and ONC requirements.

We note that our authorities and policy objectives for decision support are not identical to those of the FDA, and so the information required for source attributes may not be identical to the information that would enable independent review according to FDA's guidance and determination, and that the inverse is also true. For instance, we have included source attributes related to the determination of fairness, as well as measures of local validation pursuant to the purposes enumerated in 42 U.S.C. 300jj–11(b)(11) and (4) to support development of a nationwide health information technology infrastructure that improves efforts to reduce health disparities and that provides appropriate information to help guide medical decisions at the time and place of care, respectively, but the FDA CDS guidance did not explicitly describe measures related to fairness or local validation in their description of independent review. We note that a determination regarding information necessary for independent review lies with, and would continue to lie with, the FDA.

Beyond the FDA CDS guidance, we note alignment with several categories of source attribute information in the finalized § 170.315(b)(11)(iv)(B) and IRM practices described in § 170.315(b)(11)(vi) across other FDA guidance documents including the FDA's draft guidance on Marketing Submission Recommendations for a Predetermined Change Control Plan for Machine Learning Device Software Functions (PCCP–ML guidance) [122] and the FDA's guidance on Content of Premarket Submissions for Device Software Functions. We also note important differences between these requirements and FDA guidance, which highlights our complementary—yet distinct—regulatory authorities. Specifically, we highlight that the source attributes for ongoing maintenance of intervention implementation and use in the finalized § 170.315(b)(11)(iv)(B)(*8*) are similar to information described within FDA's PCCP–ML draft guidance. However, specific emphases for fairness measures in local data (at § 170.315(b)(11)(iv)(B)(*8*)(*iv*)) and

[122] See *https://www.fda.gov/regulatory-information/search-fda-guidance-documents/marketing-submission-recommendations-predetermined-change-control-plan-artificial.*

descriptions of the frequency by which the intervention's performance is corrected when risks related to validity and fairness are identified (at § 170.315(b)(11)(iv)(B)(*9*)(*ii*)) are not requirements of the FDA's PCCP–ML draft guidance. We also note that our source attribute information pertains to an expanded set of technologies because it is not limited to Predictive DSI that are unlocked or those that developers intend to modify over time. Our scope for technology that meets the definition of Predictive DSI is more expansive than what the PCCP–ML guidance considers because we view transparency into the performance of Predictive DSIs in a local health system or clinic to be particularly important to users to determine if a given Predictive DSI is fit for use on or with their patients, particularly in the case of older Predictive DSI that are rarely retrained based on local data. We believe that ensuring certified health IT has a place to provide this information, or indicate its omission, will be of value to users deciding on whether a technology is fit-for-purpose at their organization, but may be beyond the scope of FDA's review and approval process.

Similar examples exist in what FDA describes in its Premarket Submissions for Device Software Functions guidance, including documentation recommendations related to ''software description,'' which align with ONC final requirements in § 170.315(b)(11)(iv)(B)(*1*) for details and output of the intervention and § 170.315(b)(11)(iv)(B)(*4*) for intervention development details and input features, as well as FDA guidance for a ''risk management file,'' which aligns with requirements in § 170.523(f)(1)(xxi) for summary risk management information to be available via publicly accessible hyperlink. We believe that these similarities will reduce the burden on complying with our Program requirements for those Predictive DSI that have device software functions.

We are aware that some Predictive DSI may not be within FDA's purview because, consistent with the history of our Program, we have not focused requirements for DSIs on specific use cases. Thus, we believe that ONC is well positioned to regulate certified health IT in ways that are different from how FDA regulates device software functions and disagree with commenters' suggestion that more effective regulation of source attributes could be accomplished by the FDA, or that there is conflict between FDA labeling requirements and source attributes, because we have different authorities and, where similar requirements may be needed within these differing scopes, our agencies have worked closely to ensure complementary recommendations and requirements. These technologies, especially in the aggregate, impact how healthcare is delivered, and we believe our complementary authorities will provide important benefits to users.

Comment. Several commenters expressed concern that the list of required source attributes that must be disclosed is overly broad and potentially impractical to implement. Commenters requested clarity regarding how DSI developers would satisfy the proposed requirement of providing access of source attributes to an end user and how that information would need to be presented or formatted. They further noted the concern that providing access to users of such broad source attribute information could result in an interface that impairs physician usability. Another commenter suggested that the health IT developers should be required to instead provide a configuration option through which third-party vendors of Predictive DSI could include their source attributes during the integration with health IT or implementation within a hospitals or provider's database. Another commenter suggested that the health IT developers should be required to instead provide a configuration option through which third-party vendors of Predictive DSI could include their source attributes during the integration with health IT or implementation within a hospitals or provider's database.

Response. We appreciate comments regarding implementation of our source attributes requirements for user review and implications for usability. While our proposals required a Health IT Module to enable users to review source attribute information, we did not specify either that a user must review source attribute information or that source attribute information be presented at a specific time or manner to a user. We noted in the HTI–1 Proposed Rule that we understood that source attribute information may be presented in varied ways at various points of workflow and contain varying levels of detail and do not intend to limit the options by which this information can be made available (88 FR 23788). We also said, consistent with prior ONC discussion related to existing § 170.315(a)(9)(v) requirements for source attributes (77 FR 54215), the proposal would not require the automatic display of source attributes information when a recommendation, alert, or other decision support output is presented that resulted from a DSI (88 FR 23788). Last, we noted that we were not aware of widely agreed upon best practices for the format in which this source attribute information should be displayed. However, we are aware of industry efforts to standardize a format to display information about technology in the form of a ''model card'' or ''nutritional label'' for healthcare (88 FR 23794). We believe that rather than prescribing uniform presentation of this kind of information, that developers of certified health IT should work with their customers to determine the best format and structure of source attribute information. Finally, we note that we did not prescribe a mechanism, standard, or process for how developers of certified health IT should receive or acquire information from *other parties* for source attributes in the HTI–1 Proposed Rule and have also not done so in this final rule.

Comments. Several commenters expressed concern that our proposal would require health IT developers with certified health IT to regulate other developer's Predictive DSI and stated that health IT developers should not be responsible for the Predictive DSI of their customers or *other parties* and that health IT developers' certification should not be contingent on *other parties* providing information to the developer.

Response. We thank the commenters for their concerns. As described elsewhere in this final rule, we have adopted modified final rule requirements and a reduced scope to address these concerns. Specifically, we have finalized a different scope with respect to *other party* source attributes, such that developers of certified Health IT are only required to make source attribute information available when the health IT developer supplies the *other party's* Predictive DSI as part of its Health IT Module. In alignment with the comments, the finalized requirements of § 170.315(b)(11) do not extend to developers of certified health IT being accountable for Predictive DSIs developed by their customers or *other party* Predictive DSIs implemented by their customers.

Comments. One commenter expressed concern that the proposal will not be effective at creating broad, uniform transparency throughout the Predictive DSI marketplace because ONC has authority to regulate certified health IT, which is only a portion of the predictive model marketplace. The commenter noted that the proposal would create imbalance in the marketplace between developers of certified health IT and developers of noncertified health IT. The commenter also stated that

information from third-party developers will be inconsistent and intermittent.

Response. We believe that the scope of our definition for Predictive DSI and our requirements for Predictive DSIs supplied by developers of certified health IT are sufficiently calibrated to affect a substantial portion of the DSI marketplace and that developers of certified health IT are well-positioned to ensure that information is updated routinely and consistently for Predictive DSI they supply as part of their health IT.

Comments. One commenter expressed concern that our proposals would result in inefficiencies for developers, and that transparency goals would be more efficiently achieved through regulations that directly apply to creators of clinical decision alert content. They noted that in some cases that would be those developing EHRs, but in most instances, those creating alerts are either third-party businesses or health care providers themselves.

Response. We agree with the commenter that there is a growing market for DSIs created by *other parties,* which could include third-party businesses or health care providers using certified health IT. While we have not finalized our proposals to require developers of certified health IT to indicate when source attributes are missing for all *other party*-developed Predictive DSIs, we have finalized that a developer of certified health IT must complete and keep current descriptions of source attribute information as specified in § 170.402 (b)(4) for all interventions supplied by the health IT developer, including *other party* interventions the health IT developer supplies as part of its Health IT Module. We believe this scope appropriately focuses on what a developer of certified health IT can readily and efficiently access in terms of source attribute information. We also finalize that for source attributes in § 170.315(b)(11)(iv)(B)(*6*); (b)(11)(iv)(B)(*7*)(*iii*), (*iv*), and (*v*); (b)(11)(iv)(B)(*8*)(*ii*) and (*iv*); and (b)(11)(iv)(B)(*9*) a health IT developer must indicate when information is not available for review. This requirement pertains to both source attributes related to Predictive DSIs authored by the developer of certified health IT and to Predictive DSIs developed by *other parties* that are supplied by the developer as part of its Health IT Module.

Comments. Numerous commenters requested that we clarify that the certification requirements for developers of certified health IT do not convey an obligation for health care providers to review all the source attributes of a DSI each time they choose to use a tool.

Response. Nothing in our proposals nor this final rule would compel a user of certified health IT to review source attributes. However, we note it would be a best practice for users to conduct such affirmative reviews in an effort to identify potentially discriminatory tools, as discriminatory outcomes may violate applicable civil rights law.[123]

Comments. Several commenters expressed concern that our proposal for source attributes for Predictive DSIs is overly broad and should instead be narrowed to specifically focus on AI and machine learning algorithms, noting that there are substantial risks of bias associated with these models if they are not constructed in a manner that allows the end user to understand how they were constructed and will be maintained going forward.

Response. We appreciate the comments and agree that bias associated with AI and machine learning algorithms could create substantial risks if they are presented to the end user without information to understand how they were constructed, evaluated, and should be maintained. We believe that recent scrutiny of other predictive models has shown that those models can similarly present substantial risk if presented without this information. We note that most of our source attributes are specific to Predictive DSIs, which encompasses AI and machine learning algorithms. We have only amended existing requirements for evidence-based DSIs by asking for specific data elements to be identified when used by the DSI, including race, ethnicity, language, sexual orientation, gender identity, sex, date of birth, SDOH, sexual orientation, and health assessments data elements (*e.g.,* disability status).

Comments. Several commenters applauded HHS's efforts to recognize the challenges of complex predictive models and the general need for public disclosure of source data to determine reliability. Commenters also encouraged HHS to consider additional measures to oversee the explain-ability of the data output and for HHS to adopt broad policies that ensure public access to both models and their data sources. One commenter stated that they believed that the information presented under ''source attributes'' should be in the public domain and not just presented to end users, and information about which datasets were used to train and evaluate a DSI should be in the public domain and added to the required ''source attributes.''

Response. We thank commenters for their support. However, we decline to consider additional measures regarding the concept of ''explain-ability,'' at this time and instead we include a requirement for risks related to intelligibility to be analyzed and mitigated at § 170.315(b)(11)(vi). We also appreciate the feedback regarding the value of making public the information we are requiring for source attributes. We view access to source attribute information as a necessary step for users of Predictive DSIs to determine the quality of Predictive DSIs they use. We decline to require public disclosure of source attribute information at this time. Rather, we believe that it is vital to implement the policies that we have finalized in this rule, learn from their implementation, and revisit ways to improve transparency over time. As the industry as a whole gains experience with making source attributes available to users of Predictive DSIs, we may consider broader and public availability of source attribute information in future rulemakings.

Meanwhile, we remind interested parties that under current Program requirements related to the Communications Condition and Maintenance of Certification requirements in § 170.403 users have explicit rights to discuss publicly various aspects regarding the performance of certified health IT. Specifically, we note that in § 170.403(a)(1)(iv) users have the right to describe relevant information regarding their experiences when using a Health IT Module. We also noted in

[123] See U.S. Dept of Health & Human Servs., Office for Civil Rights, Notice of Proposed Rulemaking, Nondiscrimination in Health Programs and Activities, 87 FR 47824, 47880 (Aug. 4, 2022), *https://www.federalregister.gov/documents/2022/08/04/202216217/nondiscrimination-in-health-programs-and-activities* (prohibiting discrimination on the basis of race, color, national origin (including limited English proficiency), sex (including sexual orientation and gender identity), age, or disability in certain health programs or activities *through the use of clinical algorithms in their decisionmaking*); Title VI of the Civil Rights Act of 1964, 42 U.S.C. 2000d *et seq.* (prohibiting discrimination on the basis of race, color, or national origin (including limited English proficiency) in federally funded programs or activities); Title IX of the Education Amendments of 1972, 20 U.S.C. 1681 *et seq.* (prohibiting sex discrimination in federally funded education programs or activities); the Age Discrimination Act of 1975, 42 U.S.C. 6101 *et seq.* (prohibiting age discrimination in federally funded programs or activities); Section 504 of the Rehabilitation Act of 1973, 29 U.S.C. 794 (prohibiting disability discrimination in federally funded or federally conducted programs or activities); and the Americans with Disabilities Act, 42 U.S.C. 12101 *et seq.* (prohibiting disability discrimination by employers, state and local government entities, and businesses that are open to the public, among others).

the ONC Cures Act Final Rule that algorithms would be considered ''non-user-facing aspects of health IT'' as they are not readily apparent to persons using health IT for the purpose for which it was purchased or obtained (85 FR 25731). Thus, communications regarding algorithms (*e.g.,* mathematical methods and logic) could be restricted or prohibited, while communications regarding the output of the algorithm and how it is displayed in a health IT system could not be restricted as ''non-user-facing aspects of health IT.'' Given this, we note that source attribute information is user-facing and is relevant to a user's experience using certified health IT. Thus, source attribute information is among the kinds of information that customers may freely discuss publicly.

We also note our discussion in the HTI–1 Proposed Rule regarding an individual's ability to obtain information about any use of a Predictive DSI—or other emerging technologies—in their healthcare through the HIPAA Privacy Rule individual's right of access (88 FR 23795).[124]

In many cases, developers of certified health IT serve as HIPAA business associates to their covered entity customers, such as health care providers or health plans.[125] If an individual requests access to their health information from a HIPAA covered entity (*e.g.,* a health care provider that transmits health information in electronic form in connection with an HHS adopted standard transaction) that individual, generally, has a right to access medical and health information (protected health information (PHI)) about themselves in one or more designated record sets (DRS) maintained by or for the individual's HIPAA covered entity.[126] The DRS could include underlying data and information used to generate recommendations about an individual's healthcare, such as information about the use of a Predictive DSI in a healthcare decision and source attribute information associated with use of a Predictive DSI in a healthcare decision.[127]

Comments. One commenter agreed that developers should implement practices and processes when a model's performance is inconsistent with its intended use and recommended that we include in regulations a specific process for developers to follow. Another commenter recommended including ''identification of intended user qualifications.''

Response. We agree with commenters that developers should implement processes to update models and have included relevant source attributes describing the process of updating models at § 170.315(b)(11)(iv)(B)(*8*) and (*9*). However, we decline to specify a process by which this is performed because it is likely to vary across Predictive DSI. Information on intended user qualifications would be appropriately included at § 170.315(b)(11)(iv)(B)(*2*)(*iii*) ''intended users,'' but we do not explicitly require such information to be there.

Comments. One commenter requested that DSIs based on studies or recommendations from Federal Agencies should be exempt from any other reporting requirements other than identifying the Agency and the study.

Response. We decline to exempt any DSIs described in § 170.315(b)(11) from any of the applicable reporting requirements based on where the recommendations originate. We believe that recommendations from a federal agency, such as the Centers for Disease Control and Prevention, should include all the source attributes, not only the bibliographic citation, as is suggested by the commenter. For the same reason that transparency would be helpful for any evidence-based DSI, so too would transparency be valuable for DSIs based on studies or recommendations from federal agencies.

Comments. Numerous commenters supported the FAVES framework described in the HTI–1 Proposed Rule, noting that these concepts reflect a consensus view of the characteristics of high-quality Predictive DSIs. One commenter expressed concern that the effectiveness in regulating source attributes would be hampered by reliance on highly defined input fields which can be made subject to political analysis (*e.g.,* FAVES) and related noncomputational tests to guide to desired political outcomes, and instead suggested that ONC, rather than focusing on redesign of models and model parameters, instead emphasize transparency as to when an AI algorithm is being used.

Response. We appreciate the many statements of support for our framing of ''high-quality,'' predictive algorithms to mean that such algorithms are fair, appropriate, valid, effective, and safe, or FAVES. However, we do not believe a Program requirement for Health IT Modules to indicate when an AI algorithm was used to support decision-making is appropriate (as users should already understand if they're using a predictive AI to support their decision-making) nor sufficient for users to understand the quality of such AI algorithms. We believe that defined source attribute categories, coupled with a description of the characteristics that make up a high-quality Predictive DSI, are necessary to provide consistent information that will more effectively promote the use of those Predictive DSI where appropriate. Further, we note that while we have defined input fields, we have not established requirements for specific measures or identified specific thresholds for content that is related to those categories.

Comments. Several commenters encouraged ONC to work with interested parties to further develop guidance and standards. Specifically, one commenter urged ONC and HHS to convene interested parties to develop a consensus set of meta-data that should and, must be, transparently provided by DSI developers, and strongly supported ONC requiring a standard representing a Structure Product Label for Predictive Decision Support. One commenter encouraged additional regulatory parameters and encouraged ONC to consider requirements for regular, algorithmic impact assessments that analyze data sets, biases, and how users interact with the systems, and the overall design and monitoring of system outputs, as well as to include expressly incorporating data-set best practices and data standards requirements.

Response. We appreciate these comments and will continue to collaborate with interested parties inside and outside of government to ensure that information resulting from our transparency requirements is meaningful for patient care and decision-making.

Given the comments received from a range of interested parties, and to clarify the scope of information required for an applicable Predictive DSI, we have finalized our proposals in § 170.315(b)(11)(iv)(B) with modification. We note that the information required here as source attribute information is similar to the ''meta-data'' described by commenters.

---

[124] 45 CFR 164.524.

[125] See definitions of ''business associate'' and ''covered entity'' at 45 CFR 160.103.

[126] For more information about the HIPAA Privacy Rule individual's right of access, see OCR's HIPAA Access Guidance: *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html.*

[127] See, *e.g.,* OCR's HIPAA FAQs 2048 and 2049, *https://www.hhs.gov/guidance/document/faq-2048-does-individual-have-right-access-genomic-information-generated-clinical; https://www.hhs.gov/hipaa/for-professionals/faq/2049/does-an-individual-have-a-right-under/index.html#:~:text=Under%20the%20HIPAA%20Privacy%20Rule,a%20clinical%20laboratory%20may%20hold.*

First, rather than include references to evidence-based source attributes as proposed, we have added new subparagraphs as part of the ''Intervention details'' source attribute at § 170.315(b)(11)(iv)(B)(*1*) to include similar general attribute information. Specifically, at § 170.315(b)(11)(iv)(B)(*1*)(*i*) we require ''The name and contact information for the developer of the intervention,'' and at § 170.315(b)(11)(iv)(B)(*1*)(*ii*) we require ''Funding source of the intervention,'' which are substantially similar to the proposed inclusion of bibliographic information (since citations include the name and contact information for corresponding authors) and ''developer of the intervention and ''Funding source of the intervention'' is directly parallel to ''Funding source of the intervention development technical implementation'' all of which we proposed to apply to Predictive DSIs in the HTI–1 Proposed Rule. Commenters noted, and we agree, that bibliographic citation of the intervention finalized at § 170.315(b)(11)(iv)(A)(*1*) likely would not be relevant for all Predictive DSIs and other source attributes specific to evidence-based DSIs at § 170.315(b)(11)(iv)(A) were duplicative of source attributes in § 170.315(b)(11)(iv)(B).

Second, we have made explicit in regulation text several requirements described in the HTI–1 Proposed Rule's preamble to ensure that health IT developers clearly understand the source attribute requirements applicable to Health IT Modules presented for certification to § 170.315(b)(11). We have finalized these requirements to address many commenters' concerns regarding proprietary information and to help convey at what level of detail Predictive DSI source attributes should be available for a limited set of identified users to record, change, and access.

Comments. We received numerous comments from interested parties indicating that more clarity was needed to help communicate the scope and detail of information included as source attributes in what is now finalized at § 170.315(b)(11)(iv)(B).

Response. We agree and have finalized regulation text at § 170.315(b)(11)(iv)(B) to clarify the scope and detail of information required to be available for user review. We note that these explicit requirements in regulation text mirror the requirements described previously in preamble or represent a subset of requirements previously described in preamble. We also reiterate our preamble discussion that the requirements do not require disclosing or sharing IP or proprietary information existing in the developer's health IT, including *other parties'* IP and proprietary information.

Intervention Details

We proposed three source attributes related to details of predictive models and their proper use in § 170.315(b)(11)(vi)(C)(*1*) ''Intervention Details,'' Including ''Output of the intervention,'' ''Intended use of the intervention,'' and ''Cautioned out-of-scope use of the intervention.'' We refer readers to 88 FR 23789–23790 for a detailed discussion of our proposed rationale for these source attributes as well as examples and additional instruction, which we have made explicit in the regulation text below.

We have finalized § 170.315(b)(11)(iv)(B)*(1)* as follows: ''Details and output of the intervention, including: *(i)* Name and contact information for the intervention developer; *(ii)* Funding source of the technical implementation for the intervention(s) development (for which we have modified the wording order from the HTI–1 Proposed Rule to make the source attribute read clearer and we have also made this corresponding change for evidence-based DSIs as well); *(iii)* Description of value that the intervention produces as an output; and *(iv)* Whether the intervention output is a prediction, classification, recommendation, evaluation, analysis, or other type of output.''

We have finalized § 170.315(b)(11)(iv)(B)*(2)* ''Purpose of the intervention, including: *(i)* Intended use of the intervention; *(ii)* Intended patient population(s) for the intervention's use; *(iii)* Intended user(s); and *(iv)* Intended decision-making role for which the intervention was designed to be used/for (*e.g.,* informs, augments, replaces clinical management).''

We have finalized § 170.315(b)(11)(iv)(B)*(3)* as follows ''Cautioned out-of-scope use of the intervention, including: *(i)* Description of tasks, situations, or populations where a user is cautioned against applying the intervention; *(ii)* and Known risks, inappropriate settings, inappropriate uses, or known limitations.''

Intervention Development

We proposed at 88 FR 23790 three source attributes related to model development in § 170.315(b)(11)(vi)(C)(*2*), ''Intervention Development,'' including ''Input features of the intervention including description of training and test data,'' ''Process used to ensure fairness in development of the intervention,'' and ''External validation process, if available.'' We refer readers to 88 FR 23790–23795 for a detailed discussion of these source attributes in the HTI–1 Proposed Rule.

We have finalized § 170.315(b)(11)(iv)(B)*(4)* as follows ''Intervention development details and input features, including at a minimum: *(i)* Exclusion and inclusion criteria that influenced the data set; *(ii)* Use of variables in 170.315(b)(11)(v)(A)*(5)–(13)* as input features; *(iii)* Description of demographic representativeness according to variables in § 170.315(b)(11)(iv)(A)*(5)–(13)* including, at a minimum, those used as input features in the intervention; and *(iv)* Description of relevance of training data to intended deployed setting.''

We have finalized § 170.315(b)(11)(iv)(B)*(5)* as follows ''Process used to ensure fairness in development of the intervention, including: *(i)* Description of the approach the intervention developer has taken to ensure that the intervention's output is fair; and *(ii)* Description of approaches to manage, reduce, or eliminate bias.''

We have finalized § 170.315(b)(11)(iv)(B)*(6)* as follows ''External validation process including: *(i)* Description of the source, clinical setting, or environment where an intervention's validity and fairness has been assessed, other than the source training and testing data; *(ii)* Party that conducted the external testing; Description of demographic representativeness of external data according to variables in § 170.315(b)(11)(iv)(A)*(5)–(13)* including, at a minimum, those used as input features in the intervention; and Description of external validation process.''

Quantitative Measures of Intervention Performance

We proposed at 88 FR 23791–23792, five source attributes relevant to validation or evaluation of the performance (including accuracy, validity, and fairness) of the predictive model and evaluation of its effectiveness in § 170.315(b)(11)(vi)(C)(*3*) ''Quantitative measures of Intervention Performance,'' including ''Validity of prediction in test data,'' ''Fairness of prediction in test data,'' ''Validity of prediction in external data, if available,'' ''Fairness of prediction in external data, if available,'' and ''References to evaluation of use of the model on outcomes, if available.'' Together, these source attributes were intended to be a presentation of the

measure or set of measures related to the model's validity (often referred to as performance) and fairness when tested in data derived from the same source as the initial training data as well as when tested in data external to—that is, from a different source than—the primary training data. ''References to evaluation of use of the model on outcomes, if available,'' are bibliographic citations or links to evaluations of how well the intervention, or model on which it is based accomplished specific objectives such as reduced morbidity, mortality, length of stay or other important outcomes.

We have finalized § 170.315(b)(11)(iv)(B)(*7*) as follows ''Quantitative measures of performance, including: *(i)* Validity of intervention in test data derived from the same source as the initial training data; *(ii)* Fairness of intervention in test data derived from the same source as the initial training data; *(iii)* Validity of intervention in data external to or from a different source than the initial training data; *(iv)* Fairness of intervention in data external to or from a different source than the initial training data; and *(v)* References to evaluation of use of the intervention on outcomes, including, bibliographic citations or hyperlinks to evaluations of how well the intervention reduced morbidity, mortality, length of stay, or other important outcomes.''

Ongoing Maintenance of Intervention Implementation and Use

At 88 FR 23792, we proposed three source attributes related to the ''ongoing maintenance of intervention implementation and use,'' including, ''Update and continued validation or fairness assessment schedule,'' ''Validity of prediction in local data, if available,'' and ''Fairness of prediction in local data, if available.'' These source attributes were a description of the process and frequency by which the model's performance is measured and monitored in the local environment and corrected when risks related to validity and fairness are identified.

We have finalized § 170.315(b)(11)(iv)(B)*(8)* as follows ''Ongoing maintenance of intervention implementation and use, including: *(i)* Description of the process and frequency by which the intervention's validity is monitored over time; *(ii)* Validity of intervention in local data; *(iii)* Description of the process and frequency by which the intervention's fairness is monitored over time; and *(iv)* Fairness of intervention in local data.''

Update and Continued Validation or Fairness Assessment Schedule

At 88 FR 23792 we proposed a source attribute, ''*Update and continued validation or fairness assessment schedule*'' and described it as including ''the process and frequency by which the model's performance is measured and monitored in the local environment and corrected when risks related to validity and fairness are identified.'' Information from this attribute is important to assess whether the model is up to date or may reflect outdated trends.

We have finalized § 170.315(b)(11)(iv)(B)(*9*) as follows ''Update and continued validation or fairness assessment schedule, including: *(i)* Description of process and frequency by which the intervention is updated; and *(ii)* Description of frequency by which the intervention's performance is corrected when risks related to validity and fairness are identified.''

ix. Missing Source Attribute Information

At 88 FR 23795–23796 we proposed that a Health IT Module certified § 170.315(b)(11) would need to clearly indicate when a source attribute listed is not available for the user to review, including in two specific circumstances. First, we proposed that for source attributes that include the ''if available'' phrase, a Health IT Module must clearly indicate when such source attribute is not available for review. Second, we proposed that when a Health IT Module enables or interfaces with a DSI developed by *other parties* that are not developers of certified health IT, that Health IT Module must clearly indicate when any source attribute is not available for the user to review. We explained that this meant that a Health IT Module that supports a DSI developed by *other parties* that are not developers of certified health IT would have needed to clearly indicate when any attribute listed is not available for the user to review, regardless of whether the DSI is a Predictive DSI, as defined at § 170.102, or an evidence-based DSI.

At 88 FR 23796, we clarified that ''*other parties,*'' as used in our proposal, included any party that develops a DSI, a model, or an algorithm that is used by a DSI and is not a developer of certified health IT. These could include, but were not limited to: a customer of the developer of certified health IT, such as an individual health care provider, provider group, hospital, health system, academic medical center, or integrated delivery network; a third-party software developer, such as those that publish or sell medical content or literature used by a DSI; or researchers and data scientists, such as those who develop a model or algorithm that is used by a DSI.

We reiterated that while we did not prescribe how a certified Health IT Module would need to indicate that an attribute was missing that the certified Health IT Module would need to communicate an attribute was missing unambiguously and in a conspicuous manner to a user. We noted that these ''*other parties*'' may or may not have a contractual relationship with the developer of certified health IT. However, we sought comment on whether we should require developers of certified health IT with Health IT Modules that enable or interface with Predictive DSIs to display source attributes for *other parties* with which the developer of certified health IT has a contractual relationship.

Comments. We received mixed comments supporting and opposing our proposal to require a Health IT Module to clearly indicate when a source attribute is not available for the user to review. Among those who opposed our proposal, they conveyed that indicating to a user when a source attribute was unavailable would create burdens on health IT developers who do not readily have access to source attribute information and would position health IT developers to enforce information gathering requirements on other companies, including third-party vendors with which the health IT developer has no formal contract and health IT customers that create clinical decision support data. Many commenters who opposed this proposal supported an alternative requirement that would require certified developers to (1) provide source attributes and indicate when information was missing for those interventions they themselves authored (*i.e.,* self-developed interventions) and (2) for those interventions that were developed by *other parties* with which the developer of certified health IT worked to implement into their Health IT Modules as opposed to all *other parties,* regardless of the health IT developer's relationship with those *other parties.* In other words, commenters suggested limiting the transparency requirement to those other parties the health IT developer has a contractual relationship with or to require health IT developers to include functionality to display the information and letting their customers decide whether to display information about their own Predictive DSI or that of other developers with whom the customers have a contractual relationship.

Response. We thank commenters for their concerns. We agree with commenters regarding the burden and implementation issues associated with identifying missing information as we proposed and have made changes to the scope in response. In particular, we have addressed the concerns raised about Predictive DSIs developed by *other parties* with which the developer of certified health IT has no formal relationship. The finalized policy, described below more closely aligns with the commenters' alternative policy, which we believe addresses these concerns.

While we noted in the HTI–1 Proposed Rule that missing source attribute information would be foundational for users' understanding of the DSI regardless of whether the intervention developer was a developer of certified health IT, a customer of the developer of certified health IT, an academic health system, integrated delivery network, a third-party software developer, or *other party* (88 FR 23795), we also acknowledged that we understood there may be circumstances where a developer of certified health IT may not have information pertaining to a source attribute for a Health IT Module to enable such user review.

In response to public comments received, we have made two overall adjustments. First, we did not finalize our proposals for missing source attributes as it relates to *other parties* as proposed. This is because, as discussed elsewhere in this section, we have constrained the overall scope of the certification criterion and the developer of the certified Health IT Module's accountability to those Predictive DSIs supplied by the health IT developer as part of its Health IT Module. As a result, in circumstances where a developer of certified health IT has not supplied an *other party's* Predictive DSI as part of its Health IT Module the developer is not accountable for the unavailability of those Predictive DSI's source attribute information. Second, we have finalized a certification requirement for Health IT Modules to indicate when information is not available for specific source attributes only. Specifically, we have finalized at § 170.315(b)(11)(v)(A)(*2*) requirements that for Predictive DSIs, a Health IT Module must indicate when information is not available for review for source attributes in § 170.315(b)(11)(iv)(B)(*6*); (b)(11)(iv)(B)(*7*)(*iii*), (*iv*), and (*v*); (b)(11)(iv)(B)(*8*)(*ii*) and (*iv*); and (b)(11)(iv)(B)(*9*). We note that the implication of this finalized policy is twofold: (1) developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) must enable a limited set of identified users to access complete and up-to-date plain language descriptions for all source attributes, except those listed in § 170.315(b)(11)(v)(A)(*2*); and (2) developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) must enable such access for evidence-based and Predictive DSIs at least when those DSIs are supplied by the health IT developer as part of its Health IT Module.

We are aware that, in some limited circumstances, information for specific source attributes related to Predictive DSIs supplied by the health IT developer as part of its Health IT Module may not be available nor re-creatable. For example, health IT developers that supply Predictive DSIs that use models provided through the peer reviewed literature, such as ASCVD, eGFR, APACHE IV, and LACE+ models referenced elsewhere in this final rule,[128] may not have access to training data that would allow them to: 1) provide a description of demographic representativeness of the training data (§ 170.315(b)(11)(iv)(B)(*4*)(*iii*)); 2) generate measures of validity in test data derived from the same source as the initial training data (§ 170.315(b)(11)(iv)(B)(*7*)(*i*)); and 3) generate measures of fairness in test data derived from the same source as the initial training data (§ 170.315(b)(11)(iv)(B)(*7*)(*ii*)). In cases where information is only available through published literature, developers may provide information for these source attributes that indicate that the relevant information is not available and that it cannot be replicated. In these cases, we encourage organizations to perform external validation of these models and we believe that providing users information on the results of that work will be of high value. We note that where source attribute information is available for Predictive DSIs in these scenarios, or where source attribute information can be extrapolated from the literature (*e.g.,* intended use, cautioned out-of-scope use, or intended population, etc.) source attribute information should be accessible and modifiable consistent with requirements in § 170.315(b)(11)(v).

[128] Goff Jr, David C., et al. ''2013 ACC/AHA guideline on the assessment of cardiovascular risk: a report of the American College of Cardiology/American Heart Association Task Force on Practice Guidelines.'' *Circulation* 129.25_suppl_2 (2014): S49–S73.

Levey, Andrew S., et al. ''A more accurate method to estimate glomerular filtration rate from serum creatinine: a new prediction equation.'' *Annals of internal medicine* 130.6 (1999): 461–470.

Comments. Commenters that expressed support for this proposal commended our efforts and requested we strengthen this provision to require that all source attribute information is available for user review. Some commenters expressed support for the proposal stating that it would send a signal to health care providers about the trustworthiness of a DSI tool and encourage AI developers to be transparent. One commenter expressed concern that our proposal would allow health IT developers to opt-out of reporting information and allowing developers to indicate when source attributes are missing should be the exception and not the rule. Another commenter expressed concern that this provision places no limits on how much or what type of data can be missing while still complying with source data transparency requirements and could incentivize developers to not provide any data that might show bias or lead to any type of negative conclusion by potential users.

Response. We thank commenters for their support. As addressed more fully in the response directly above, we have made substantial adjustments to the certification criterion's scope and health IT developers accountability expectations. As a result of these changes, we have also addressed commenter concerns that there would be no limit on how much or what type of data can be missing. We have finalized in § 170.315(b)(11)(v)(A)(*2*) that only source attributes in § 170.315(b)(11)(iv)(B)(*6*); (b)(11)(iv)(B)(*7*)(*iii*), (*iv*), and (*v*); (b)(11)(iv)(B)(*8*)(*ii*) and (*iv*); and (b)(11)(iv)(B)(*9*) may be missing and in these circumstances a health IT developer must indicate when information is not available for review.

Comments. Some commenters expressed concern that the proposal to require Health IT Modules to display missing source attributes could result in unfair market dynamics, in which developers of certified health IT will make available full and complete source attribute information for their homegrown or native DSIs while being less inclined to collect and meaningfully display such information from *other parties* developing and offering Predictive DSIs. Several commenters noted that the proposal would not compel third-party creators to provide the information to the health IT developer, or to renegotiate existing contracts to compel the provision of source attributes.

Response. We thank commenters for these concerns and suggestions. We did not propose and we have not finalized

a policy that regulates *other parties* and this final rule does not compel *other parties* to provide source attribute information to developers of certified health IT. Rather, we believe there is sufficient market-driven motivation for *other parties* to provide source attribute information for Predictive DSIs they author or develop to health care providers who seek to use their Predictive DSI's in addition to any of the ones supplied by a developer of certified health IT as part of its Health IT Module. We believe health IT users are likely to develop the expectation that information is available through source attributes and trust and choose to use Predictive DSIs that have the information contained in source attributes compared to those that do not, which may also create competitive pressure in the market to provide source attribute information. For example, the market incentives consumers have when choosing between vehicles that have complete history reports regarding accident damages, manufacturer buybacks, registration records, odometer readings, and ownership transfers, and those vehicles that do not. We believe similar market incentives will result in more source attribute information being made available for user review than would be the case absent the requirement to indicate when source attributes were not available for review.

In response to the commenter concerned about unfair market dynamics, we note that we have finalized a requirement that Health IT Modules must be capable of displaying source attributes from *other parties* and for users to be able to modify attributes for those Predictive DSI. But that is where the finalized requirements stop. With the exception of Predictive DSIs authored by the health IT developer or those it expressly chooses to supply as part of its Health IT Module, we have not required health IT developers with Health IT Modules certified to § 170.315(b)(11) to receive, acquire, or otherwise produce source attributes related to *other party* DSIs. We encourage those *other parties* to work with their customers to ensure that source attribute information is full and complete, thereby addressing any potentially unfair market dynamics.

Comments. Another commenter suggested that developer of the other system, at most, could denote if a DSI it interfaces with is in fact a third-party model, thus informing the user of the need to seek out any desired information from the primary developer of the DSI in question.

Response. As part of this final rule's focus on providing information only for Predictive DSIs supplied in Health IT Modules, we decline to require that Health IT Modules display or ''denote'' when another system includes a third-party model.

Comments. Commenters stated that communicating that a model is third-party is sufficient and stated that while the proposed language of saying source attribute information is ''not available for user review'' is both unnecessarily pejorative to the third party and misleading to the end user.

Response. We have finalized at § 170.315(b)(11)(v)(B)(*1*) that Health IT Modules must ''Enable a limited set of identified users to record and change source attributes in paragraphs (b)(11)(iv)(A) and (B) of this section,'' but have left flexibility to developers of certified health IT and their customers to choose if and how to indicate that information is missing, when they believe doing so is valuable, so that they may avoid pejorative and misleading language.

Comments. One commenter expressed concern with the phrase ''*other parties*'' because it could encompass healthcare delivery organizations that self-develop Predictive DSI for ''in-house'' use to augment their purchased EHR system and requested an exemption from certain requirements, and that they not be penalized by ONC or their EHR vendor who could pass on ''costs'' to use their ''in-house'' tools.

Response. We thank the commenter for their concern. We believe this final rule's focus on providing information only for Predictive DSIs supplied by health IT developers in their Health IT Modules will reduce concerns around a need for specific exemptions or that developers of certified health IT might pass on costs, since those developers are only likely to incur costs for those Predictive DSI they supply. Predictive DSI that a healthcare delivery organization self-developed and used to augment their Health IT Module would likely not be considered supplied by health IT developers.

As noted previously in this final rule, we have maintained our description of ''*other parties.*'' For the purposes of the Program, compliance clarity, and distinguishing a health IT developer's own authored and supplied Predictive DSIs from everyone else, we use the phrase ''*other party,*'' which could include a health care provider who self-develops a Predictive DSI. That said, as we have conveyed this final rule's requirements, being described as an *other party* imposes no specific regulatory compliance requirement.

x. Authoring and Revising Source Attributes

At proposed § 170.315(b)(11)(vi)(E), we proposed that Health IT Modules certified to § 170.315(b)(11) support the ability for a limited set of identified users to author (*i.e.,* create) and revise source attributes and information provided for user review beyond the specific source attributes we enumerated (88 FR 23796–23797). This proposal applied to source attributes related to both evidence-based DSIs and Predictive DSIs that would be enabled by or interfaced with a certified Health IT Module, including any Predictive DSIs that could have been developed by users of the certified Health IT Module, and we described specific examples in the HTI–1 Proposed Rule. While we did not propose to require a developer of certified health IT to be directly involved in the authoring or revision of source attribute information provided for user review, we proposed that the certified Health IT Module would need to support the technical ability for a limited set of identified users to create new or revised attribute information alongside other source attribute information proposed as part of § 170.315(b)(11)(vi)(A) and (C).

Comments. A majority of commenters did not support the proposal that Health IT Modules certified to § 170.315(b)(11) support the ability for a limited set of identified users to author (*i.e.,* create) and revise source attributes and information provided for user review beyond what was proposed. One commenter supported the concept of hospitals and providers creating their own Predictive DSI models and suggested that developers should only be expected to create functionality to allow users to enter their own source attributes and that developers should not have responsibility for gathering that information for users for input into the products. One commenter expressed concern that it is unclear whether the expectation is that developers must allow for customers to revise the source attributes that developers have themselves defined for DSIs they have developed, noting that allowing revisions would seem problematic as it could inappropriately alter the meaning and information being relayed to end-users. Commenters recommended that we clearly indicate that this requirement applies solely to additional/supplementary source attributes for DSIs developed by the developer of certified health IT themselves stating that DSIs that are not directly implemented or enabled by the developer should be out of scope for the

criterion. Commenters were especially concerned that the proposal failed to define the intent for, or characteristics of, the limited set of identified users and would enable those users to create extra regulatory requirements for developers of certified Health IT Modules.

Response. We appreciate the comments and believe that coupled with the proposed scope for the certification criterion that some commenters may have misinterpreted the intent behind our proposal and how the technical capabilities for a Health IT Module would play out as part of implementation. We note that several source attributes, particularly those now finalized in § 170.315(b)(11)(iv)(B)(*6*)–(*9*) pertain to activities that may occur within individual customer sites, so that processes to measure validity and fairness, as well as the results of those processes, are likely to differ across customer sites. We believe individual customers will have substantial value in revising these source attributes. We clarify that developers of certified health IT are not responsible for content recorded, changed, or accessed by these users and are not responsible for gathering information for or from users that wish to record or change source attribute information.

We nevertheless understand commenters' concerns related to modification of source attributes related to Predictive DSIs that are developed by health IT developers. We clarify that developers of certified health IT are not responsible for the accuracy or use of source attribute information that is modified by their users. Rather, developers of certified health IT are required to have Health IT Modules that support the capability for their users to author or revise source attribute information. We emphasize that this capability is not dependent on the entity that developed the Predictive DSI or related source attributes and we decline to limit this capability to only those additional/supplementary source attributes for DSIs developed by a developer of certified health IT. We note that a Health IT Module is required to enable a ''limited set of identified users,'' to author and revise source attributes. We believe this stipulation ensures that a Health IT Module is capable of enabling some specified users, but not all users, to have the capability to author and revise source attributes and we believe this mitigates concerns around inappropriate alteration. This requirement will not provide these users with the ability to create additional regulatory requirements but simply to display information related to source attributes of their choosing. We note that several certification criteria include the phrase ''limited set of identified users,'' including the CDS criterion at § 170.315(a)(9), which developers of certified health IT have had more than a decade of experience supporting.

Comments. Some commenters did not agree with the proposal that Health IT Modules certified to § 170.315(b)(11) support the ability for a limited set of identified users to author (*i.e.,* create) and revise source attributes and information provided for user review beyond what was proposed in § 170.315(b)(11)(vi)(A) and (C). These commenters noted that it could be burdensome on device manufactures, be at odds with FDA device requirements, adulterate the functionality of the device, and could possibly invalidate any testing and validity provided by the developers or require such robust testing for all permutations that quality and cost could be impacted. Commenters were concerned about the impact on FDA approved devices, observing that allowing third-party developers and users to alter source attribute information, including information related to the ''intended use'' of the device, may be considered an alteration to the device and impact FDA approval.

Response. We appreciate commenters' concerns regarding FDA-approved medical devices and alterations to the devices intended use source attribute. We note that the source attribute related to intended use is a description of what the output of the Predictive DSI should be used for and not a bound indication of what a devices may be approved to do. While we do not expect users to change the intended use of a Predictive DSI, the requirement is that a Health IT Module enable a limited set of users to change and record source attribute information. We believe that developers of certified health IT and their customers are best positioned to jointly decide how broadly to provide the ability to change and record source attributes and under what circumstances. Customers could then decide what set of users should have the ability to record and change source attribute information in the capabilities adopted in final § 170.315(b)(11)(iv)(A) and (B). In many cases, we believe that FDA requirements and the information included as source attributes are closely aligned, limiting burden on developers. Where that is not the case, we believe the information provided as source attributes will have substantial values to users commensurate with implied burden. Though required, developers concerned about changes to their original source attribute information are free to include a capability to allow users to review the original source attributes even when the information has been changed by end users.

We have finalized our requirements related to revising source attribute information with modifications at § 170.315(b)(11)(v)(B)(*1*), which requires that a Health IT Module must enable a limited set of identified users to record and change source attributes in § 170.315(b)(11)(iv)(A) and (b)(11)(iv)(B). As previously discussed, § 170.315(b)(11)(v)(B) is a modified version of proposed § 170.315(b)(11)(iv) and § 170.315(b)(11)(vi)(E), combining the ''author and revise'' concepts of § 170.315(b)(11)(iv)(E) with the ''review'' concept in § 170.315(b)(11)(iv). In finalizing this language, we intend to clearly convey that individuals can record and change information within the source attributes listed at § 170.315(b)(11)(iv)(A) and (b)(11)(iv)(B).

We are also aware of substantial activity by the public, industry groups, and other advocacy organizations to further transparency related to Predictive DSIs. Along those lines, we have observed that variations exist with respect to each initiative's priorities and that there is not strong consensus among these groups related to the information included as source attributes or transparency information.[129] As technology related to Predictive DSIs continues to evolve and as industry consensus matures, we expect that new information may need to be made available through source attributes for new models. In recognition of the fact that this final rule now sets a consistent, industry-wide baseline set of source attributes on which these groups may wish to build, we have retained a requirement at § 170.315(b)(11)(v)(B)(*2*) around authoring source attributes in addition to those listed in § 170.315(b)(11)(iv)(B). This capability will help support health care providers who wish to stay at pace with industry consensus around transparency and include additional source attribute information using their certified health IT to do so.

In § 170.315(b)(11)(v)(B)(*2*) we have finalized that for Predictive DSIs, the Health IT Module must enable a limited set of identified users to record, change, and access additional source attribute information not specified in paragraph (b)(11)(iv)(B). First, we have limited this

[129] See, for instance, work by the coalition for health AI *https://www.coalitionforhealthai.org/* and the health AI partnership *https://healthaipartnership.org/*.

capability to only Predictive DSI source attributes in § 170.315(b)(11)(iv)(B), whereas our proposal applied to both evidence-based and Predictive DSIs. This is intended to be responsive to commenters who worried that the scope of this capability was too burdensome to implement. Second, we have modified the capability from ''author and revise source attributes beyond those listed'' to the capability to ''record, change, and access additional source attribute information not specified.'' We believe this more clearly articulates the intent of the policy and addresses concerns regarding questions posed by interested parties on what ''beyond,'' meant within the context of their obligations. We clarify that developers of certified Health IT Modules are not responsible for the content recorded, changed, or accessed by these users.

xi. Intervention Risk Management (IRM) Requirements for Predictive Decision Support Interventions

At 88 FR 23797–23808, we proposed to establish ''intervention risk management'' (IRM) requirements. We proposed at 88 FR 23797 to require that by December 31, 2024, a developer of certified health IT that attested ''yes'' as part of our other proposal would need to employ or engage in certain IRM practices for all Predictive DSIs, as we proposed at 88 FR 23785 to define in § 170.102, that the developer's certified Health IT Module enables or interfaces with. We also proposed that developers of certified health IT analyze potential risks and adverse impacts associated with a Predictive DSI for the following characteristics: validity, reliability, robustness, fairness, intelligibility, safety, security, and privacy at § 170.315(b)(11)(vii)(A)(*1*) (88 FR 23799–23801). Similarly, we proposed that developers of certified health IT implement practices to mitigate risks associated with intervention Predictive DSIs at § 170.315(b)(11)(vii)(A)(*2*) (88 FR 23801–23802). And, related to governance, we proposed that developers of certified health IT would need to establish policies and implement controls for Predictive DSI governance, including how data are acquired, managed, and used in a Predictive DSI at § 170.315(b)(11)(vii)(A)(*3*) (88 FR 23802–23803).

With respect to documentation, we proposed at § 170.315(b)(11)(vii)(B) that developers of certified health IT compile detailed documentation of IRM practices and upon request from ONC make available such detailed documentation for any Predictive DSI that their certified Health IT Module enables or interfaces with (88 FR 23803–23804). We also proposed at § 170.315(b)(11)(vii)(C) to require developers of certified health IT to submit summary information to their ONC–ACB regarding IRM practices listed via a publicly accessible hyperlink that would allow any person to directly access the information without any preconditions or additional steps (88 FR 23804). Consistent with Program implementation for similar documentation requirements (84 FR 7484), we proposed that for this proposed summary information, the required documentation would need to be submitted to ONC–ACBs for review prior to issuing a certification (88 FR 23805).

Finally, we proposed at § 170.315(b)(11)(vii)(D) to require that developers of certified health IT review annually and, as necessary, update both detailed documentation and summary information associated with the certification criterion (88 FR 23805). We also proposed to establish a deadline of December 31, 2024, for developers of certified health IT with Health IT Modules to which the proposed requirements in that section apply to engage in IRM practices and develop both detailed documentation and summary information (88 FR 23797). This proposed deadline corresponded with other proposals in the HTI–1 Proposed Rule, including our proposed to update the Base EHR definition (88 FR 23808).

Comments. Commenters both supported and opposed our proposed IRM requirements at § 170.315(b)(11)(vii), with those in support noting the proposed risk management practices of risk analysis, risk mitigation, and governance are essential for ensuring the trustworthiness of Predictive DSIs. One commenter suggested that ONC strengthen its risk analysis requirements to include intended and reasonably expected DSI use(s), DSI evidence of safety, DSI efficacy, DSI level of automation, and conditions of DSI deployment, whereas another commenter recommended ONC limit its risk analysis requirements to predictive clinical DSIs. Commenters were especially supportive of our proposal to adopt NIST's AI Risk Management Framework (AI RMF) because they noted the characteristics in the proposal provide a robust framework to help with risk mitigation.[130] Some commenters recommended that we follow the Congressionally-created National Artificial Intelligence Advisory Committee (NAIAC) recommendation to use either the NIST AI RMF or similar processes and policies that align with NIST AI RMF. One commenter was supportive to use the NIST Characteristics for FAVES, but recommended revisions to the Fairness, Intelligibility, and Safety characteristics. One commenter who supported the proposal suggested that ONC should strengthen the proposed requirements to explicitly require that a health IT developer's risk mitigation practice include additional information on addressing bias, safeguarding privacy, security interests, and personal information, and create a full feedback loop.

Response. We appreciate these comments and agree that risk management practices are essential for ensuring the trustworthiness of Predictive DSIs and that these practices would promote transparency and accountability within healthcare. As described further in this section we have finalized in § 170.315(b)(11)(vi) substantially similar versions of our proposals. The finalized certification criterion requires that IRM practices must be applied for each Predictive DSI supplied by the health IT developer as part of its Health IT Module, including risk analysis, risk mitigation, and governance. We have also finalized modified versions of what we proposed related to IRM summary information in § 170.523(f)(1)(xxi) as well as the annual review and updated documentation requirements in § 170.402(b)(4). We have *not* finalized our proposal that developers of certified health IT compile detailed documentation of IRM practices listed in § 170.315(b)(11)(vii)(A) and upon request from ONC make available such detailed documentation for any Predictive DSI that their certified Health IT Module enables or interfaces with.

We thank commenters for their support of our proposal's consistency with the NIST AI RMF and the National Association of Insurance Commissioners (NAIC) recommendation to use either the NIST AI RMF or similar processes and policies that align with the NIST AI RMF.[131] While we encourage the use of

[130] NIST AI Risk Management Framework, *https://airc.nist.gov/AI_RMF_Knowledge_Base/Playbook.*

[131] As noted in the HTI–1 Proposed Rule (88 FR 23810) (footnote 289), we are aware of and coordinated with multiple federal agencies and activities focused on AI, including the NAIC, that are also exploring policies to prevent and mitigate bias in AI/ML and the intersection with privacy, equity, and civil rights. For more information about the Congressionally-created NAIC and its recommendation for federal agencies, please see the NAIC Year 1 Report (May 2023), available at:

a framework to help facilitate IRM and adapted the NIST AI RMF concepts and emphasis areas, conformance with this certification criterion does not require the use of any particular framework, approach, or methodology for providing information about risk management practices. As noted in HTI–1 Proposed Rule (88 FR 23798), we have left this flexibility given a lack of healthcare sector-specific guidance and the nascency of several emerging efforts for risk management of predictive software.

We appreciate commenters' suggestions on additional characteristics and additional kinds of risks that developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) should include as part of their IRM practices. However, we remained consistent with what we proposed and decline to add further characteristics. We believe that the eight areas we have finalized represent consensus focus areas, are based on the NIST AI RMF, and would be most relevant to Predictive DSIs. We will monitor implementation of this requirement and may consider modifications to these characteristics in future rulemaking.

Comments. Commenters not in support of the IRM requirements proposed at § 170.315(b)(11)(vi), expressed significant concerns that they would require disclosing IP or proprietary information, could compromise patient privacy, and increase administrative burdens. Other commenters did not support the IRM requirements because they thought they were too broad, noting that requiring a developer of certified health IT to perform IRM practices over a third party's DSI tool is neither feasible or competitively rational and recommended that we limit the scope so that developers are accountable for IRM practices for its own DSI only. Other commenters that did not support the IRM proposals urged ONC to consider a risk-based DSI approach that would classify high, moderate, and low risk DSIs and would provide developers with appropriately scaled risk-based controls based on potential harm to individual patients and populations. One commenter expressed concern that some developers may engage in risky practices that result in harm or privacy violations and requested more clarity on how certification criteria would exclude developers from engaging in these practices. One commenter expressed concern that there is not enough time for developers to meet the December 31, 2024, deadline due to the time to develop and implement the requirements and requested additional time to address the eight characteristics of risk.

Response. We thank commenters for their concerns and suggestions. As we have noted throughout this rulemaking, we believe that such transparency is a prerequisite for high-quality Predictive DSIs to be trusted by clinicians, patients, health systems, software developers, and other interested parties. When we developed the proposed IRM requirements, we sought a balance between limited prescriptiveness and sufficient detail to enable robust and broadly applicable reporting of information on risk management practices to users and the public. Our proposed requirements focused on potential risks and adverse impacts (harm) in eight areas, that include privacy and fairness, that may be associated with each Predictive DSI that is authored by the health IT developer.

In consideration of the feedback we received, we believe that the finalized IRM requirements strike the best balance, especially given that we have not established requirements for specific measures. Rather, we have given maximum flexibility to developers of certified health IT to determine which information best fits their unique circumstances and Predictive DSI use cases. We encourage developers of certified health IT to examine industry resources, such as the NIST AI RMF or the Health Equity Across the AI Lifecycle (HEAAL) framework,[132] as part of these requirements.

Further, as stated in the HTI–1 Proposed Rule (88 FR 23799), we believe that many such developers of certified health IT already employ or engage in IRM practices to comply with existing certification criteria (§ 170.315(g)(3) ''safety-enhanced design'' (SED) and § 170.315(g)(4) Quality management systems (QMS)). Thus, we continue to believe that the finalized requirement to provide information on these practices represents a low-level of burden for those developers. We believe that our IRM practice requirements are important for several reasons. First, all developers of certified health IT that seek certification to § 170.315(b)(11) and supply Predictive DSIs as part of their Health IT Module will become familiar with foundational IRM practices. Second, the public disclosure of the summary information of IRM practices employed or engaged by the developer of certified health IT, as described further below, will provide transparency to purchasers (potential users), users, and other interested parties, and contribute to appropriate information to help guide medical decisions. Lastly, our finalized requirements in § 170.315(b)(11)(vi)(A) will encourage development of healthcare-specific, consensus, and industry-based best practices for risk management.

We appreciate the concerns expressed about IP and proprietary information, patient information privacy, and administrative burden. As noted, as part of this certification criterion's preamble we have made scope adjustments in response to public comment that we believe substantially address these concerns. The finalized requirements for risk analysis and risk mitigation are limited to only those Predictive DSIs supplied by the developer of health IT as part of its Health IT Module. We have also clarified our expectations for governance requirements. With the exception of *other party* Predictive DSI's supplied by developers of health IT as part of their Health IT Module, we have *not* finalized the proposals (88 FR 23803) that caused commenters' concerns regarding the developer of certified health IT performing ''IRM practices over a third party's DSI.'' Specifically, we have not finalized that developers review risk management information from *other parties* nor that developers include risk management information from *other parties* as part of the documentation requirement.

We appreciate the concern expressed about information privacy and harm. We expect that model developers will use data for training and testing consistent with applicable law, patients' expectations, and any patient consent or preference given. We believe the scope changes we have made as part of this finalized certification criterion along with the high degree of flexibility we provide to developers of certified health IT to establish appropriate risk management practices mitigate concerns related to compromising IP, proprietary information, and patient privacy. While we appreciate the concerns raised by some commenters, based on the final certification criterion's scope, we believe they are outweighed by the need to promote greater and more meaningful disclosure of information by developers of health IT certified. We disagree with the claims that our requirements for summary information about risk management practices would result in

https://www.ai.gov/wp-content/uploads/2023/05/NAIAC-Report-Year1.pdf.

[132] Kim J., Hasan A., Kellogg K., et al. Development and preliminary testing of Health Equity Across the AI Lifecycle (HEAAL): A framework for healthcare delivery organizations to mitigate the risk of AI solutions worsening health inequities. medRxiv 2023.10.16.23297076; doi: *https://doi.org/10.1101/2023.10.16.23297076.*

disclosing IP or proprietary information as we are entrusting developers of certified health IT to disclose information at a level of detail according to their own judgments. Furthermore, based on the scope of the final certification criterion, it is reasonable to assume that developers of certified health IT are experts on their own products and services and possess sophisticated technical and market knowledge related to the implementation and use of health IT in a variety of settings in which their products are used. Through their accumulated experience developing and providing health IT solutions to their customers, health IT developers should be familiar with the types of risks that most users encounter, and therefore must describe these in sufficient detail to provide potential customers, patients, or researchers, with the information they need to make informed applicability, scope, and use decisions.

As for recommendations that we take a risk-based approach to IRM requirements, we appreciate the comment. However, the Program is not predicated on levels of risk and our requirements for certification to the DSI (formerly CDS) criterion has been and continues to be agnostic to specific use cases, intended uses, and risks. We reiterate that we are not establishing requirements for specific measures. Rather, we are giving maximum flexibility for developers of certified health IT to determine which information best fits their unique circumstances and Predictive DSI use cases.

As noted in the HTI–1 Proposed Rule (88 FR 23802), developers of certified health IT have the flexibility to choose an approach to meeting this requirement that addresses their own unique circumstances for their Predictive DSIs. However, we encourage developers to implement policies and controls to evaluate whether risk analysis and risk mitigation practices are being carried out as specified; to consider how policies and controls are monitored and updated; and to plan a schedule for updating those policies and controls. Policies and controls should include details on roles, responsibilities, staff expertise, authority, reporting lines, and continuity. We further encourage developers to have accountability and escalation policies and controls related to how management oversees the development, deployment, and management of Predictive DSIs.[133] These policies and controls should describe the developer of certified health IT's decision-making parameters or programs and include how management is held accountable for the impact of Predictive DSIs. We encourage developers to identify staff that are responsible for Predictive DSIs and related models and to develop policies to hold those staff accountable to the developer's established policies and procedures.[134] We believe that developers should plan escalation processes that permit significant issues with Predictive DSI development, integration, or use to reach appropriate levels of management and describe standards for timely resolution of issues with Predictive DSIs and related models.[135] If the developer uses a third party to assess risk, the developer should describe processes for determining whether assessments performed by a third party meet the standards and controls set forth in the developer's governance framework.

We appreciate the commenter's concerns about meeting the December 31, 2024, deadline, and the desire for an extension. We note that in prioritizing this certification criterion, we have finalized longer timelines for the adoption of other standards and certification criteria with, for example, a compliance date of January 1, 2026. We believe the extended dates for conformance with these other standards and certification criteria will make it more feasible for the industry to meet the December 31, 2024, deadline for the finalized requirements in § 170.315(b)(11). We discuss timing requirements in more detail below in the section on modifications to the ''Base EHR.''

After consideration of public comments received, we have finalized with modifications our proposed requirements for IRM practices. Specifically, we have finalized in § 170.315(b)(11)(vi) that IRM practices must be applied for each Predictive DSI supplied by the health IT developer as part of its Health IT Module. This finalized requirement applies to Predictive DSIs ''supplied by the health IT developer as part of its Health IT Module,'' which establishes an equivalent scoping between what we proposed under the attestation statement in proposed § 170.315(b)(11)(v) and what we have finalized in § 170.315(b)(11)(vi). As proposed, only those developers that attested ''yes,'' would have had to employ or engage in IRM practices and as finalized, only developers that supply Predictive DSIs are required to apply IRM practices. We have finalized § 170.315(b)(11)(vi)(A) requiring that Predictive DSIs must be subject to analysis of potential risks and adverse impacts associated with the following characteristics: validity, reliability, robustness, fairness, intelligibility, safety, security, and privacy, which is substantially similar to what we proposed. We have finalized § 170.315(b)(11)(vi)(B) requiring that Predictive DSIs must be subject to practices to mitigate risks, identified in accordance with (b)(4)(ii)(A) of this section, which is substantially similar to what we proposed. We have finalized § 170.315(b)(11)(vi)(C) requiring that Predictive DSIs must be subject to policies and implemented controls for governance, including how data are acquired, managed, and used, for all Predictive DSIs supplied by the health IT developer as part of its Health IT Module, which is substantially similar to what we proposed.

We have also finalized requirements in § 170.523(f)(1)(xxi) as part of the Principles of Proper Conduct for ONC–ACB's that an ONC–ACB shall, where applicable, ensure that summary information of the IRM practices listed in paragraph § 170.315(b)(11)(vi) is submitted by the health IT developer via publicly accessible hyperlink that allows any person to access the summary information directly without any preconditions or additional steps. We have finalized this requirement as a combination of what we proposed in § 170.315(b)(11)(vii)(C) and what we proposed as a modification the Principles of Proper Conduct for ONC–ACB in § 170.523(f)(1)(xxi)

Finally, as stated previously, we have finalized a new Assurances Maintenance of Certification requirement in § 170.402(b)(4) that requires developers of Health IT Modules certified to § 170.315(b)(11), starting January 1, 2025, and on an ongoing basis thereafter, review and update, as necessary, source attribute information in § 170.315(b)(11)(iv)(A) and (B), risk management practices described in § 170.315(b)(11)(vi), and summary information provided through § 170.523(f)(1)(xxi). This requirement is substantially similar to what we had included in our proposal (such as § 170.315(b)(11)(vii)(D)). We provide additional details on § 170.402(b)(4) in previous comment responses in section III.C.5.v. ''Predictive Decision Support Interventions, Attestation for Predictive

[133] Off. Comptroller Currency, Comptroller's Handbook: Model Risk Management (Aug. 2021), *https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/model-risk-management/index-model-risk-management.html.*

[134] Id.

[135] Id.

Decision Support Interventions,'' of this final rule.

We reiterate that ONC has not adopted specific risk analysis metrics or risk mitigation practices beyond describing eight characteristics in § 170.315(b)(11)(vi)(A) and we note that developers of certified health IT may vary their IRM practices based on their understanding of the risk of each Predictive DSI.

Comments. Several commenters expressed concerns that the nature of the proposed documentation required in the IRM disclosure requirements that developers would have to meet would require a third-party developer to share proprietary technical and governance information and requested clarification on the level of detail required in documentation that IRM practices are employed. One commenter requested clarification on how developers of health IT would meet the proposed documentation requirements in § 170.315(b)(11)(vii)(B) when they would need to obtain the documentation from third-party developers. Several commenters did not support our IRM proposals due to the burdens it would place on health IT developers and recommended that we limit the IRM proposals to health IT developers who develop their own Predictive DSI models.

Response. We thank commenters for their concerns. After consideration of these comments, we have not finalized the requirements described in the HTI–1 Proposed Rule preamble for developers of certified health IT to receive or have access to risk management information for Predictive DSIs developed by *other parties* (and that are not supplied by the developer as part of its Health IT Module). After consideration of these comments, we have not finalized the requirements described in the HTI–1 Proposed Rule (88 FR 23803) preamble for developers of certified health IT to receive or have access to risk management information for Predictive DSIs developed by *other parties* (and that are not supplied by the developer as part of its Health IT Module). This means there are no expectations that developers review risk management information from *other parties* with whom they have no relationship and with whom they have not expressly chosen to supply a Predictive DSI as part of their Health IT Module. This also excludes all *other party* Predictive DSIs that their customers choose to implement as well as any Predictive DSIs that their customers author.

Comments. Several commenters believed that developers, and not health care providers, should ultimately be responsible for the tools they create and bear responsibility for harmful outcomes resulting from the tools being used as intended. Whereas other commenters suggested that the responsibility for risk assessment and mitigation should be shared with DSI providers and authors of the toolset, rather than requiring the health IT developers to accept all responsibilities.

Response. We appreciate the commenters' concerns. We agree that multiple parties share responsibility for risk assessment and mitigation and the safe application of Predictive DSI, and note that this rule does not alter any party's responsibility for exercising sound professional judgment in making clinical decisions and complying with applicable laws.[136] Developers and health care providers should implement practices in full awareness that this final rule will not change their responsibility under other applicable law. We have finalized requirements aligned with our authorities for developers of certified health IT, and we anticipate these requirements for IRM practices will help spur much-needed conversations across providers and their health IT partners on how best to analyze, mitigate, and govern risks associated with Predictive DSIs.

As noted in the HTI–1 Proposed Rule, we are aware that, in addition to developers of certified health IT, users, such as healthcare organizations and clinicians, have responsibilities related to Predictive DSIs, including intervention or model risk management during implementation and use, as well as model validation (88 FR 23805). For example, we believe it is important that users maintain strong governance and controls to help manage model risk and how they will use outputs from interventions in decision-making, including monitoring any potential impacts of model use. Users of a Predictive DSI are also best able to report on how the Predictive DSI performs in real world and local settings, which can differ from their performance during testing.

Comments. One commenter expressed concern that the proposal was too broad and recommended that ONC exclude from its transparency and risk management requirements any DSI tools that are created by a health care provider organization for its own use, with no intent to commercialize the tool(s). One commenter expressed concern that ONC did not account for the difference between ''AI Developers'' and ''AI Deployers'' noting that each has unique and distinct roles, and risk analysis requirements should account for these separate roles.

Response. We appreciate the feedback. As we have noted as part of the certification criterion's discussion throughout this final rule, we have adjusted the scope of the certification criterion and clarified health IT developer responsibilities compared to health care providers and *other parties.* We clarify, based on the scope and policy for the final certification criterion, that ''DSI tools created by a health care provider'' for its own use are *not* in scope for Program requirements. More to the point, such health care providers will benefit from this final certification criterion's requirements because updated certified health IT will include more supportive capabilities for DSI transparency that they will be able to use for their own purposes. We appreciate the comment for differentiating between ''AI Developers'' and ''AI Deployers,'' however, we decline to establish different IRM practice requirements for different roles that may, or may not, exist across organizational boundaries. Our requirements pertain specifically to developers of certified Health IT Modules that supply Predictive DSIs as part of their Health IT Module.

Comments. Several commenters expressed concern about the potential liability of health IT developers and health care providers. One commenter expressed concern that some developers

[136] *See e.g.,* U.S. Dept of Health & Human Servs., Office for Civil Rights, Notice of Proposed Rulemaking, Nondiscrimination in Health Programs and Activities, 87 FR 47824, 47880 (Aug. 4, 2022), *https://www.federalregister.gov/documents/2022/08/04/2022-16217/nondiscrimination-in-health-programs-and-activities* (prohibiting discrimination on the basis of race, color, national origin (including limited English proficiency), sex (including sexual orientation and gender identity), age, or disability in certain health programs or activities *through the use of clinical algorithms in their decision-making*); Title VI of the Civil Rights Act of 1964, 42 U.S.C. 2000d *et seq.* (prohibiting discrimination on the basis of race, color, or national origin (including limited English proficiency) in federally funded programs or activities); Title IX of the Education Amendments of 1972, 20 U.S.C. 1681 *et seq.* (prohibiting sex discrimination in federally funded education programs or activities); the Age Discrimination Act of 1975, 42 U.S.C. 6101 *et seq.* (prohibiting age discrimination in federally funded programs or activities); Section 504 of the Rehabilitation Act of 1973, 29 U.S.C. 794 (prohibiting disability discrimination in federally funded or federally conducted programs or activities); and the Americans with Disabilities Act, 42 U.S.C. 12101 *et seq.* (prohibiting disability discrimination by employers, state and local government entities, and businesses that are open to the public, among others); The Health Insurance Portability and Accountability Act (HIPAA) Public Law 104–191,110 Stat. 1936 (August 21, 1996), codified at 42 U.S.C. 1320d–1320d8; HIPAA Privacy Rule, 45 CFR part 160 and subparts A and E of part 164; and The HIPAA Security Rule, 45 CFR part 160 and subparts A and C of part 164.

may attempt to shift liability for poor performing tools and recommended that the developer of the tool should bear the responsibility of ensuring optimal performance of the tool they developed and should bear the brunt of the liability when errors occur. One commenter recommended that we strengthen the requirements around IRM practices by requiring developers of certified health IT with Health IT Modules that enable or interface with Predictive DSIs to carry liability insurance that covers contingent bodily injury due to technology errors and omissions.

Response. We appreciate the commenter's concern for liability and accountability. We believe that our requirements for transparency in both performance, as indicated by the information required as part of source attributes, and in IRM practices will help users determine if tools are poor performing and make subsequent decisions on whether and how to use such tools. In general, these comments are outside of the scope of this rulemaking, and we decline to require liability insurance as part of our requirements and believe that issues of liability are outside the scope of this rulemaking. Those concerned or curious about it should reference federal, state, or tribal laws and regulations—or reliable sources information.

Comments. One commenter expressed concern that there is no requirement for real world testing in an uncontrolled environment and urged ONC require these activities are tested in real world scenarios before they are adopted to ensure DSIs are successful.

Response. We thank the commenter for their suggestion to require real world testing of Predictive DSIs. We note that among the source attributes listed in § 170.315(b)(11)(iv) there are two that would enable users to know if a Predictive DSI was tested for fairness at § 170.315(b)(11)(iv)(B)(*8*)(*iii*) and (iv) and validity in local data at § 170.315(b)(11)(B)(iv)(*8*)(*i*) and (*ii*). These source attributes are intended to support such real world testing; however, we are not requiring that such testing be done, so as noted within the certification criterion these source attributes may be missing. We also note that Health IT Modules certified to § 170.315(b)(11) must participate in real world testing as a Condition and Maintenance of Certification requirement as stipulated in § 170.405.

Risk Analysis

In the HTI–1 Proposed Rule (88 FR 23798–23799), we proposed to require developers of certified health IT to analyze potential risks and adverse impacts associated with a Predictive DSI that their certified Health IT Modules enable or interface with. NIST's AI RMF describes seven characteristics of trustworthy AI, and we proposed to adapt these concepts and require that developers of health IT with certified Health IT Modules that enable or interface with Predictive DSIs employ or engage in risk management practices related to the following characteristics: (1) validity; (2) reliability; (3) robustness; (4) fairness; (5) intelligibility; (6) safety; (7) security; and (8) privacy. We did not propose or describe risk tolerance associated with the eight characteristics, as we believe these should be decisions made by those involved with the design, development, deployment, and use of the technology. We proposed that developers of certified health IT must analyze the potential risks and adverse impacts, associated with a Predictive DSI that their certified Health IT Modules enable or interface with, related to lack or failure in the eight characteristics.

Comments. Several commenters were concerned that ONC did not establish or define regulatory baselines, measures, or thresholds for what constitutes FAVES for Predictive DSIs and noted that providers are not trained to independently assess whether a Predictive DSI was FAVES, nor is there a commonly accepted standard for review. Several commenters expressed concern that the IRM proposals could be duplicative of other federal agencies and could create conflicting regulatory schemes and urged ONC to consult and collaborate with federal partners and build on existing federal efforts to ensure bias, discrimination, and other health equity concerns were addressed through a unified AI government framework. One commenter recommended that the proposed ''Safety'' characteristic should explicitly exclude FDA-authorized AI and machine learning medical devices because they believe that a risk assessment for these tools is best made by the FDA due to their expertise in medical and clinical safety and being uniquely positioned to draw conclusions and develop guidelines for the safe and appropriate use of AI and machine learning tools.

Response. Given the broad uses of Predictive DSIs, ONC did not seek to establish specific baselines, measures, or thresholds for what constitutes FAVES in the HTI–1 Proposed Rule. These measures are likely to vary based on specific technologies and uses of Predictive DSI. In many cases, the safety and effectiveness of a software function, including clinical decision support or other kinds of decision support interventions, is within the purview of FDA regulatory oversight, when such functionality meets the definition of a ''device'' under the FD&C Act. As previously noted, ONC and FDA support a harmonized and complementary approach to predictive technology in accordance with our existing intersecting regulatory oversight. We sought to ensure there would be limited, if any, contradictory requirements. We note that we have afforded substantial flexibility to developers in practicing IRM. For tools that have been authorized by the FDA, we believe it would be appropriate for developers to provide information on FDA authorization as part of the ''Safety'' characteristic. Furthermore, given the intersecting interest across the Department to address the use of AI in health, we consulted extensively with our HHS partners at AHRQ, FDA, and OCR as well as our federal partners at the FTC and VA in developing the HTI–1 Proposed Rule to advance our shared goals of promoting greater trust in Predictive DSIs in healthcare that are fair, appropriate, valid, effective, and safe to deliver patient care, enable an effective marketplace, and greater competition.[137]

After consideration of these comments, we have finalized requirements at § 170.315(b)(11)(vi)(A) that for each Predictive DSI supplied by the health IT developer as part of its Health IT Module, the Predictive DSI must be subject to analysis of potential risks and adverse impacts associated with Predictive DSI the following characteristics: validity, reliability, robustness, fairness, intelligibility, safety, security, and privacy. We note that we have narrowed the scope of Predictive DSIs for which a developer is expected to analyze risks and adverse impacts to only those Predictive DSIs that are supplied by the health IT developer. As stated previously, this is in response to public comments concerned with the overall scope of our IRM practice requirements and the related burdens, difficulty, and concerns around potential proprietary information related with getting such information from *other parties.*

Risk Mitigation

In the HTI–1 Proposed Rule, we proposed to require implementation of practices to mitigate risks associated with Predictive DSIs (88 FR 23801). In

[137] See generally HHS Press Release (April 2023), *https://www.hhs.gov/about/news/2023/04/11/hhs-propose-new-rule-to-further-implement-the-21st-century-cures-act.html.*

the HTI–1 Proposed Rule, we proposed § 170.315(b)(11)(vii)(A)(*2*) to require implementation of practices to mitigate risks associated with Predictive DSIs (88 FR 23801). We noted that risk mitigation practices should seek to address adverse impacts or minimize anticipated negative impacts of Predictive DSIs on patients and populations. We stated model risk mitigation should include disciplined and knowledgeable development and implementation practices that are consistent with the real-world context of the model's use, intended specific application of the model, and goals of the model user.

Comments. One commenter expressed concern that some developers may engage in risky practices that result in harm or privacy violations and requested more clarity on how certification criteria would exclude developers from engaging in these practices. One commenter encouraged ONC to clearly define the types of risks or harms that would disqualify a developer from Program certification. One commenter expressed concern that our proposal lacked requirements for DSI systems on managing complaints, post market surveillance, and error or misuse detection guidance, as well as reporting requirements related to these issues.

Response. We thank commenters for their concerns. We note that developers should implement practices in full awareness that this final rule will not change their responsibility under other applicable laws,[138] including those that provide legal protections to minimize risk practices and prohibit discrimination. We expect that model developers will use data for training and testing consistent with applicable law, patients' expectations, and any patient consent or preference given. We decline to further specify practices that would disqualify a developer from the Program, beyond the eight characteristics that must be addressed. As it relates to managing complaints and reporting requirements, we note that ONC has long maintained a ''health IT inquiry and feedback portal,'' available where users and the public can file complaints and ask questions about products certified under the Program.[139] We also reiterate that developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) will be required to engage in real world testing per requirements at § 170.405.

Comments. Several commenters supported our proposal for risk mitigation requirements. Several commenters recommended that ONC adopt a tiered or risk-based approach to IRM practices and adopt requirements that would only apply to applications that present a meaningful risk to patients, allowing ONC to focus on high risk DSIs. These commenters generally supported the assessment of risk in predictive models but stated that requiring all models to adhere to the same set of compliance and regulatory rigor seems both unnecessary and overly burdensome. Some of these commenters also thought a risk-based approach was appropriate for determining whether and which disclosure requirements were necessary to prevent stifling innovation and prevent overly restrictive reviews.

Response. We appreciate the comments supporting our proposal for risk mitigation. We decline to accept the recommendation to take a risk-based DSI approach as suggested. We reiterate that the Program is not predicated on levels of risk and the DSI criterion will continue to be agnostic to specific use cases, intended uses, and risks. As stated in the HTI–1 Proposed Rule (88 FR 23799), we will require the developers of certified health IT engage in and document risk management practices related to eight characteristics: (1) validity; (2) reliability; (3) robustness; (4) fairness; (5) intelligibility; (6) safety; (7) security; and (8) privacy. However, we have provided substantial flexibility in the risk management practices developers engage in within those characteristics and the associated documentation. Developers may therefore choose to apply different levels of rigor to the risk analysis, risk mitigation, and governance of different Predictive DSIs. Similarly, developers of certified health IT may choose to apply different levels of detail describing their approaches to risk management practices as part of the summary information that must be summited per requirements in § 170.523(f)(1)(xxi).

This approach also aligns with HIPAA Security Rule requirements for covered entities and business associates. HIPAA covered entities, such as health care providers and health plans, are generally among the customers of developers of certified health IT. In many cases, developers of certified health IT serve as HIPAA business associates to their covered entity customers, such as health care providers or health plans,[140] and thus must comply with the HIPAA Security Rule. The HIPAA Security Rule requires covered entities and business associates to identify and assess risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI (''ePHI'') when conducting the risk analysis and risk management required by the Security Rule, including any risks of third-party access to a covered entity's or business associate's information systems that contain electronic protected health information.[141]

As noted in the HTI–1 Proposed Rule, similar to when a HIPAA covered entity or business associate engages with a cloud service provider,[142] a developer of certified health IT, supplying an *other party*-developed Predictive DSI as part of its Health IT Module,[143] should understand the ways in which the technology or solution offered by the *other party* would seek to connect to or integrate with the certified health IT developer's product(s), so that the covered entity or business associate can appropriately conduct its own risk analysis and establish risk management

[138] See HIPAA Privacy and Security Rules, 45 CFR part 160 and subparts A and E of part 164; 15 U.S.C. 45(a) (Section 5 of the FTC Act) and Health Breach Notification Rule in 16 CFR part 318; U.S. Dept of Health & Human Servs., Office for Civil Rights, Notice of Proposed Rulemaking, Nondiscrimination in Health Programs and Activities, 87 FR 47824, 47880 (Aug. 4, 2022), *https://www.federalregister.gov/documents/2022/08/04/2022-16217/nondiscrimination-in-health-programs-and-activities* (prohibiting discrimination on the basis of race, color, national origin (including limited English proficiency), sex (including sexual orientation and gender identity), age, or disability in certain health programs or activities *through the use of clinical algorithms in their decision-making*); Title VI of the Civil Rights Act of 1964, 42 U.S.C. 2000d *et seq.* (prohibiting discrimination on the basis of race, color, or national origin (including limited English proficiency) in federally funded programs or activities); Title IX of the Education Amendments of 1972, 20 U.S.C. 1681 *et seq.* (prohibiting sex discrimination in federally funded education programs or activities); the Age Discrimination Act of 1975, 42 U.S.C. 6101 *et seq.* (prohibiting age discrimination in federally funded programs or activities); Section 504 of the Rehabilitation Act of 1973, 29 U.S.C. 794 (prohibiting disability discrimination in federally funded or federally conducted programs or activities); and the Americans with Disabilities Act, 42 U.S.C. 12101 *et seq.* (prohibiting disability discrimination by employers, state and local government entities, and businesses that are open to the public, among others).

[139] *https://inquiry.healthit.gov/support/plugins/servlet/desk/portal/2.*

[140] See definitions of ''business associate'' and ''covered entity'' at 45 CFR 160.103.

[141] See the definition of ''electronic protected health information'' at 45 CFR 160.103.

[142] U.S. Department of Health and Human Services, Office for Civil Rights (OCR), Guidance on HIPAA & Cloud Computing: *https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html.*

[143] As noted in HTI–1 Proposed Rule at 88 FR 23796, we note that these ''other parties'' may or may not have a contractual relationship with the developer of certified health IT.

policies, as well as enter into appropriate Business Associate [144] Agreements (BAAs).[145] For example, a health IT developer providing certified health IT as a business associate may consider including in its risk analysis any risks associated with a decision by a covered entity to connect or integrate an *other party's* Predictive DSI with the developer's certified health IT products.[146] Under the HIPAA Security Rule, business associates have an independent obligation to identify and manage risks, regardless of whether or not a BAA exists.[147] If a business associate relationship exists and a BAA does not exist, the absence of a BAA does not relieve the business associate from HIPAA Security Rule obligations.

After consideration of these comments, we have finalized at § 170.315(b)(11)(vi)(B) that for each Predictive DSI supplied by the health IT developer as part of its Health IT Module, the Predictive DSI must be subject to practices to mitigate risks, identified in accordance with § 170.315(b)(11)(vi)(A). We note that we have narrowed the scope of Predictive DSIs for which a developer is expected to mitigate risks to only those Predictive DSIs that are supplied by the health IT developer as part of its Health IT Module. As stated previously, this is in response to public comments concerned with the overall scope of our proposed IRM practices requirements and the related burdens, difficulty, and potential proprietary information concerns related with getting such information from *other parties.*

[144] See definition of ''business associate'' at 45 CFR 160.103. Business associates include a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

[145] See 45 CFR 164.308(b) for information about the Security Rule's requirements for BAAs. 45 CFR 164.502(e) permits a covered entity to disclose PHI to a business associate and to allow a business associate to create, receive, maintain, or transmit PHI on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. Additional guidance on BAAs, often referred to as business associate contracts, is available at *https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.*

[146] The risk is based on the connection permitted to the certified health IT product by the health IT developer and not whether the developer has a direct or contractual relationship to the other party.

[147] Business associates are required to comply with the requirements of the HIPAA Security Rule. 45 CFR 164.302. See OCR's Direct Liability of Business Associates, *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html;* OCR's Security Rule Guidance material, available at: *https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html?language=es.*

Governance

In the HTI–1 Proposed Rule, we proposed § 170.315(b)(11)(vii)(A)(*3*) to require that developers of certified health IT establish policies and implement controls for Predictive DSIs (88 FR 23802). We proposed that a developer of a certified Health IT Module that enables or interfaces with a Predictive DSI must establish policies and implement controls for how data are acquired, managed, and used for said Predictive DSI.[148] Governance should encompass models, software and data developed or provided by *other parties* as well as internally developed interventions.[149]

At 88 FR 23802–23803, we provided a discussion of the flexibility developers of certified health IT would have to choose an approach to meeting this proposed requirement that addresses their own unique circumstances for their Predictive DSIs. This included setting and enforcing priorities for managing and using data as a strategic asset, which is a concept that identifies key activities of data governance as data identification, data management policy, data issues management, data assessment, data oversight, and data communications.[150]

Comments. Several commenters supported our requirement to include ''governance'' as part of the IRM practices. However, many commenters also expressed concern regarding our expectation that developers of certified health IT review governance information from *other parties* or that *other parties* provide the developer of certified health IT with relevant IRM information so that such information may be available for both detailed and summary documentation.

Response. We appreciate commenters' concerns. In response to public comments, we have not finalized the requirements described in the HTI–1 Proposed Rule for developers of certified health IT to receive or have access to specific risk management information from *other parties* except when the health IT developer supplies an *other party* Predictive DSI as part of its Health IT Module. We have finalized as part of Governance requirements in § 170.315(b)(11)(vi)(C), that for each Predictive DSI supplied by the developer as part of its Health IT Module, the Predictive DSI must be subject to policies and implemented controls for governance, including how data are acquired, managed, and used. As a result, we clarify that the expectation described in the HTI–1 Proposed Rule that developers receive or have access to risk management information for Predictive DSIs developed by *other parties* is generally inapplicable, unless the developer of health IT is the one supplying the *other party's* Predictive DSI as part of its Health IT Module.

The NIST AI RMF Govern Section 6 discusses a need for policies and procedures to be in place to address AI risks and benefits arising from third-party software and data.[151] We note that while not required to follow the NIST AI RMF, developers of certified health IT may wish to review Govern Section 6 as this section provides a number of suggested actions and documentation questions that we believe would be informative towards meeting governance requirements.[152] Similarly, The Office of the Comptroller of Currency similarly described several best practices related to risk management of models developed by third parties, including seventeen specific items included on its internal control questionnaire.[153] Many of these practices could apply to the development of governance processes pertaining to risk management of models authored by *other parties* including, for example, ''When relying on third-party models, does management obtain ongoing performance monitoring and outcomes analysis of the model conducted by third parties''.[154]

[148] See, *e.g.,* The Organisation for Economic Co-operation and Development (OECD), *Recommendation of the Council on Health Data Governance, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0433;* General Accountability Office (GAO), AI: *An Accountability Framework for Federal Agencies and Other Entities* (June 2021), *https://www.gao.gov/assets/gao-21-519sp.pdf;* See generally GAO, *Artificial Intelligence in Health Care: Benefits and Challenges of Technologies to Augment Patient Care,* (Nov. 2020), *https://www.gao.gov/products/gao-21-7sp.*

[149] See NIST AI RMF 1.0, *https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.*

[150] See for example Federal Data Strategy, Data Governance Playbook, *https://resources.data.gov/assets/documents/fds-data-governance-playbook.pdf.*

[151] NIST AI RMF. Govern, Section 6. Available at: *https://airc.nist.gov/AI_RMF_Knowledge_Base/Playbook/Govern.*

[152] Ibid. Transparency and Documentation.

[153] See Bd. Governors Fed. Rsrv. Sys., Off. of Comptroller of the Currency, Supervisory Guidance on Model Risk Management, SR Letter 11–7, (April 2011), *https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm;* Off. Comptroller Currency, Comptroller's Handbook: Model Risk Management (Aug. 2021), *https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/model-risk-management/index-model-risk-management.html.*

[154] *Id.*

Compile Detailed IRM Practice Documentation

In the HTI–1 Proposed Rule, we proposed that a health IT developer that attests ''yes'' as part of proposed § 170.315(b)(11)(v)(A) would need to compile detailed documentation regarding IRM practices and upon request from ONC make available such detailed documentation to ONC for any Predictive DSI, as defined in § 170.102, that the certified Health IT Module enables or interfaces with (88 FR 23803). We noted our belief that a developer of certified health IT subject to this proposed requirement should be able to provide detailed documentation of their IRM practices, if ONC requests such information, without much effort because this information should be a byproduct of employing or engaging in IRM practices.

Comments. Several commenters were not supportive of the proposed requirements for detailed documentation of IRM practices and expressed concern that including the term ''interfaces with'' as it relates to the proposed IRM practices results in a policy that is too broad. Specifically, commenters noted that obtaining detailed documentation related to a third party's DSI tool is neither feasible nor competitively rational and recommended that we limit the scope so that developers are accountable for IRM practices for its own DSI only. One commenter requested clarification on how developers of health IT would meet the proposed documentation requirements when they would need to obtain documentation from third-party developers.

Response. As discussed throughout this section, we have finalized a more specific and limited scope for Predictive DSIs that are supplied by the health IT developer as part of its Health IT Module. After consideration of these comments, we have not finalized the proposals requiring developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) to compile detailed documentation regarding the IRM practices listed in paragraph (b)(4)(iii) of this section and upon request from ONC, make available such detailed documentation for each Predictive DSI.

Request for Comment

- Users of Certified Health IT and Predictive DSI Management

This request for comment included in the HTI–1 Proposed Rule (88 FR 23805–23806) focused on the DSI section, and we sought input on shared responsibilities with users related to FAVES DSIs, including intervention or model risk management during implementation (deployment) and use, as well as model validation. We welcomed technical and policy comments on this section. We received many insightful comments on this request for comment. We appreciate the input provided by commenters and may consider their input to inform a future rulemaking.

- Data Practices and Governance: Ethical, Legal, and Social Implications of Data Collection and Use

This request for comment included in the HTI–1 Proposed Rule (88 FR 2380–23807) focused on the DSI section and related to ONC's authorities under the HITECH Act and the Cures Act with respect to adopting standards, implementation specifications, and certification criteria as part of the Program, overseeing developers of certified health IT through Conditions and Maintenance of Certification requirements, and serving in a coordinating role with respect to health IT. We welcomed technical and policy comments on this section. We received many insightful comments on this request for comment. We appreciate the input provided by commenters and may consider their input to inform a future rulemaking. We will also share relevant comments with our federal partners in the Department.

- Technical Data Standards and Data Management: Electronic Data Source, Capture, and Use

This request for comment included in the HTI–1 Proposed Rule (88 FR 23808) focused on the DSI section and how ONC can further support standardization and harmonization in these areas. We welcomed technical and policy comments on this section. We received many insightful comments on this request for comment. We appreciate the input provided by commenters and may consider their input to inform a future rulemaking.

xii. Public Disclosure and Availability of Summary Documentation and Corresponding Proposals for ONC–ACBs in § 170.523(f)(1)(xxi)

In the HTI–1 Proposed Rule, we proposed that a health IT developer that attested ''yes'' consistent with our other proposals would need to submit summary information of the IRM practices to its ONC–ACB via publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps (88 FR 23804). We also proposed a new Principle of Proper Conduct for the ONC–ACBs to require ONC–ACBs to report the proposed summary information that they received from developers of certified health IT on the Certified Health IT Product List (CHPL) for the applicable Health IT Modules. We noted our belief this new Principle of Proper Conduct is consistent with existing public disclosure requirements (*e.g.,* 45 CFR 170.523(f)(1)(xii) and § 170.523(f)(1)(xx)) under the Program and would help ensure accountability for the public availability of information. We proposed to require that this summary information be made available to ONC–ACBs via publicly accessible hyperlink by December 31, 2024.

We stated that ''summary information'' should describe risk management practices we enumerated in our proposals for the Predictive DSIs with which a certified Health IT Module enables or interfaces within general terms. We noted that ''summary information,'' is not specific to any single Predictive DSI. Rather, the information pertains to the suite or portfolio of Predictive DSIs enabled by or interfaced with the certified Health IT Module. We noted that the summary information likely encompasses variation in risk management practices for different kinds of Predictive DSIs.

Similar to our policy associated with the API-focused certification criteria in § 170.315(g)(10)(viii)(B), at 88 FR 23805, we proposed that all IRM documentation be available via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps. We clarified that for the proposed IRM documentation, summary information would need to be submitted to the developer of certified health IT's ONC–ACB for review prior to issuing a certification. The availability of documentation as part of the certification process is also consistent with existing requirements for API documentation in § 170.315(g)(10)(viii)(B) (API documentation requirements were proposed in the Cures Act Proposed Rule (84 FR 7484) and finalized in the ONC Cures Act Final Rule (88 FR 25748)).

To support submission of documentation, and consistent with other Principles of Proper Conduct in § 170.523(f)(1), we proposed a new Principle of Proper Conduct for IRM practice documentation in § 170.523(f)(1)(xxi) that ONC–ACBs report the information required in § 170.315(b)(11)(vii)(C) on the CHPL for the applicable certified Health IT Modules. We believe this new Principle of Proper Conduct will assist in promoting greater transparency for the

Program and will strengthen ONC–ACB oversight regarding IRM documentation.

Comments. Several commenters expressed concern with the proposed requirement to make summary information about IRM practices available publicly because they believed it would require developers to risk revealing their intellectual property or proprietary information, increase administrative burdens, provide little value to the public, and potentially create imbalance in the marketplace. A few commenters suggested that the non-public information that the developer makes available to prospective and existing clients as part of Program certification requirements is sufficient to demonstrate adequate IRM practices. Another commenter recommended flexibility for health care providers that develop health IT solutions specific for use within their EHR platform so that disclosure of proprietary model information would be permissive.

Response. We appreciate and understand commenters concerns about revealing proprietary information. However, we do not agree that intellectual property or trade secrets are jeopardized through publication of summary risk management information. Our final policy gives developers of certified health IT flexibility to determine what information to describe at what level of detail they feel is most appropriate. To clarify, the summary information of IRM practices requirement do not need to include public disclosure of specific information on code, model tuning, parameter or hyperparameter selection, or details on how individual input or output variables were selected or operationalized, which we understand to form the underpinnings of developers concerns related to intellectual property. We encourage developers to provide information that they determine would be useful to inform potential users of whether a model is FAVES without providing information at the level of detail that might constitute proprietary information.

We recognize there may be some burden associated with making summary information of IRM practices publicly available but we believe the benefits of such transparency outweigh those burdens, especially given that we have not required generation of more detailed IRM practice information as proposed. A primary objective of our policy is to increase trust in the development and use of Predictive DSIs and this includes making summary information on risk management practices available to patients, researchers, policymakers, and other interested parties.

Comments. Some commenters expressed support for the proposed requirement to make summary information regarding IRM publicly accessible. One commenter urged ONC to include an additional requirement to require a developer to enclose an intelligible end-user fact sheet that would disclose data used for training, potential risks, concerns for bias, performance, and generalizability, at a minimum, and in clear, concise language.

Response. We appreciate the comments and suggestions. We note that much of the information the commenters requested is included within the source attributes listed at § 170.315(b)(11)(iv). We decline at this time to require developers to disclose source attribute information publicly, but we have finalized the requirement to publicly disclose summary of IRM practices.

After consideration of these comments, we have finalized requirements proposed in § 170.523(f)(1)(xxi) requiring that ONC–ACBs shall, where applicable, ensure that summary information of the IRM practices listed in paragraph § 170.315(b)(11)(vi) is submitted by the health IT developer via publicly accessible hyperlink that allows any person to access the summary information directly without any preconditions or additional steps.[155]

xiii. Annual Review

Finally, in the HTI–1 Proposed Rule at § 170.315(b)(11)(vi)(D), we proposed to require developers of certified health IT that attested ''yes'' to review annually and, as necessary, update detailed and summary documentation (88 FR 23805). We noted that we viewed the detailed documentation required as being a by-product of the proposed requirement for the developer of certified health IT to engage or employ in IRM practices. Thus, we expect that developers of certified health IT subject to this proposed requirement would review documentation associated with their IRM practices annually and, as necessary, update their documentation. Further, we noted our belief that developers of certified health IT that attested ''yes'' would consider risk as part of ongoing development cycles, and these risks should be assessed in a timely manner so that risk analysis documentation is up to date. Similar to the HIPAA Security Rule,[156] which requires covered entities and business associates to conduct ongoing risk analysis,[157] we proposed that developers of certified health IT with Health IT Modules that enable or interface with Predictive DSIs review their IRM practices and update their documentation as necessary.

As noted in the HTI–1 Proposed Rule, we considered an annual review as a way to establish a minimum expectation for updating IRM documentation, and believed that would be good for Predictive DSIs to undergo a full validation process at some fixed interval, including updated documentation of all related activities (88 FR 23805). As noted in the HTI–1 Proposed Rule, we considered an annual review as a way to establish a minimum expectation for updating IRM documentation, and we believed that would be good practice for Predictive DSIs to undergo a full validation process at some fixed interval, including updated documentation of all related activities (88 FR 23805). While we did not propose more frequent reviews, we stated those may be appropriate for developers of certified health IT that have Health IT Modules that enable or interface with numerous or complex Predictive DSIs.

Comments. We did not receive substantive feedback regarding this requirement for annual review.

Response. As a result, consistent with all other policy changes we have made for this final certification criterion, we have finalized requirements in § 170.402(b)(4) that developers with Health IT Modules certified to § 170.315(b)(11), starting January 1, 2025 and on an ongoing basis thereafter review and update, as necessary, information in § 170.315(b)(11)(v)(A) and (B), risk management practices described in § 170.315(b)(11)(vi), and summary information provided through § 170.523(f)(1)(xxi). As noted previously (see prior comment responses in ''v. Predictive Decision Support Interventions, Attestation for Predictive Decision Support Interventions''), we have determined that a supportive Maintenance of Certification requirement as part of the Assurances

[155] Please visit the Program's Certified Health IT Product List (CHPL) for information about the Program's authoritative listing of all certified health IT that have been successfully tested and certified, available at *https://chpl.healthit.gov/#/search.*

[156] 45 CFR part 160 and subparts A and C of part 164.

[157] 45 CFR. 164.306(e) and 164.316(b)(2)(iii); see also OCR Guidance on Risk Analysis, *https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html* (noting that ''in order for an entity to update and document its security measures 'as needed,' which the HIPAA Security Rule requires, it should conduct continuous risk analysis to identity when updates are needed'').

Condition of Certification is necessary to fully implement our policy objectives and proposals. We believe that this finalized policy is substantially similar to what we proposed in § 170.315(b)(11)(vii)(D). Moreover, we believe that this finalized policy maintains a substantially similar, or reduces, scope for developers of certified health IT, depending on whether they supply a Predictive DSI as part of its Health IT Module. For developers of certified health IT that would have attested ''no'' to our proposed attestation statement, these developers do not supply a Predictive DSI as part its Health IT Module and, therefore, do not have IRM practices or IRM summary information that needs to be reviewed and updated. For developers of certified health IT that would have attested ''yes'' to our proposed attestation statement, these finalized requirements are a reduction in scope given our focus on Predictive DSIs supplied by a health IT developer as part of its Health IT Module, as compared to our proposed scope of Predictive DSIs enabled or interfaced with a Health IT Module. The requirements proposed are the same as the requirements finalized for these developers of certified health IT that must review and update, as necessary, risk management practices described in § 170.315(b)(11)(vi), and summary information provided through § 170.523(f)(1)(xxi).

As for the finalized requirement in § 170.402(b)(4) to review and update source attribute information in § 170.315(b)(11)(v)(A) and (B), we believe this is a clearer articulation of our intention proposed at § 170.315(b)(11)(vi)(A) and (C). This annual review process clarifies expectations that developers of certified health IT must review and update, as necessary, on an ongoing basis the source attribute information that was proposed to be available for user review in § 170.315(b)(11)(vi)(A) and (C).

xiv. Update From Clinical Decision Support to Decision Support Intervention Criterion

At 88 FR 23808, we proposed modifications to the Base EHR definition in § 170.102 to identify that a Health IT Module can be certified to either § 170.315(a)(9) or § 170.315(b)(11) to satisfy the definition for the period up to and including December 31, 2024. We also proposed that § 170.315(a)(9) would no longer be included as part of the Base EHR definition after December 31, 2024. Rather, only § 170.315(b)(11) and not § 170.315(a)(9) will be available as a certification criterion to satisfy the definition of Base EHR beginning January 1, 2025.

Additionally, in § 170.315(a)(9)(vi) we proposed that the adoption of § 170.315(a)(9) would expire on January 1, 2025, for purposes of the Program. Together, these proposals identified the dates when § 170.315(b)(11) replaces § 170.315(a)(9) in the Base EHR definition, and they indicated when Health IT Modules certified to § 170.315(a)(9) will need to be certified to § 170.315(b)(11) to maintain compliance with the Base EHR definition.

Comments. Several commenters were not supportive of the proposed requirement to developers of certified health IT with Health IT Modules certified to § 170.315(a)(9) who wish for those Health IT Modules to continue to meet the Base EHR definition would need to certify those Health IT Modules to § 170.315(b)(11) by December 31, 2024, and requested that the timeframe be extended due to the feasibility of implementation. Specifically, commenters requested a compliance timeframe of 24–36 months from final rule to design, program, test, certify, deploy to customers and real word test any new certification requirements for DSI.

Response. We thank commenters for their comments regarding our proposal to modify the Base EHR definition in § 170.102 to identify the dates when § 170.315(b)(11) replaces § 170.315(a)(9) in the Base EHR definition. As part of a broader timing strategy, and in acknowledgement of the important work related to Predictive DSI transparency that is needed now, we have finalized our proposal that the reference to § 170.315(a)(9) as part of the Base EHR definition in § 170.102, thus its availability as a certification criterion in the Program, would expire January 1, 2025. We have finalized that developers of certified health IT with Health IT Modules certified to § 170.315(a)(9) who wish for those Health IT Modules to continue to meet the Base EHR definition would need to certify those Health IT Modules to § 170.315(b)(11). We also note for purposes of the Program that the certification criterion at § 170.315(a)(9) expires on January 1, 2025.

b. Updates to Real World Testing Condition for CDS Criterion

At 88 FR 23808–23811, we proposed to revise § 170.405(a) to include § 170.315(a)(9) within the list of certification criteria for which a developer of certified health IT with Health IT Module(s) certified to such criteria must successfully test the real world use of those Health IT Module(s) for interoperability in the type of setting in which such Health IT Module(s) would be or are marketed. As proposed, this meant that a developer of certified health IT with a Health IT Module certified to § 170.315(a)(9) would be subject to the requirements set forth in § 170.405(a) (88 FR 23808). We noted that the effects of including Health IT Modules certified to § 170.315(a)(9) in § 170.405(a) and the effect of proposing a revised version of the CDS criterion in § 170.315(b)(11) would require developers of certified health IT certified to § 170.315(a)(9) and § 170.315(b)(11) to follow the testing plans, methods, and results reporting; submission dates; and August 31 deployment deadline requirements in § 170.405(b) similar to the requirements of other applicable certification criteria listed in § 170.405(a) (88 FR 23809). We anticipated that if finalized as proposed this would mean that Health IT Modules certified to § 170.315(a)(9) would be subject to the real world testing Condition and Maintenance of Certification requirements beginning with the 2023 real world testing cycle.

Comments. Commenters were mixed in their support and opposition to our proposal to add § 170.315(a)(9) to the list of applicable certification criteria for the real world testing Condition and Maintenance of Certification requirement in § 170.405(a) and thus requiring developers certified to § 170.315(a)(9) or § 170.315(b)(11) to participate in real world testing plan and results submission. Commenters that did not support including § 170.315(a)(9) in the list of applicable criteria for real world testing Condition and Maintenance of Certification requirements stating that it would be infeasible, and a poor investment of time and resources given the possible timing of this final rule publication in conjunction with requirements for 2024 real world testing plan submissions in November of 2023. Commenters stated that it would create significant developer burden to meet this requirement for a criterion that developers could not certify to after December 31, 2024. Many of these commenters instead said we should limit real world testing requirement to developers of certified health IT with Health IT Module(s) certified to § 170.315(b)(11). Commenters suggested that by only including § 170.315(b)(11) then ONC and developers could focus resources on a revised criterion instead of a retired criterion. Commenters also recommended a phased approach for the inclusion of Predictive DSI into real

world testing given the burden on developers to implement other proposals in the rule, notably the new Insights Condition and Maintenance of Certification requirements.

Commenters who were supportive of the proposal to add § 170.315(a)(9), thus requiring developers certified to § 170.315(b)(11) to participate in real world testing, stated that it would have the benefit of testing predictive models in a diverse range of real world clinical settings, thereby creating a more accurate, comprehensive, and contextual understanding of a model's performance. Commenters noted that including CDS will help ensure implementation of the CDS Criterion, future certification criteria, and other elements discussed in this rule are effective, efficient, minimally burdensome, and beneficial, and would ensure intended performance in practice. One commenter stated that adding CDS to real world testing will give developers an opportunity to determine if the user community is using their interventions, and if so, the ability to determine how the interventions are being used. Lastly, one commenter believed that testing decision support intervention technology and predictive models successfully for real world use enhances interoperability and patient care experience in which certified Health IT Modules would be marketed.

Response. We appreciate comments regarding our proposal to revise § 170.405(a) to include § 170.315(a)(9). Given the mixed support from commenters and finalization of our policy to replace § 170.315(a)(9) with § 170.315(b)(11) as of January 1, 2025, we have not finalized our proposal to modify § 170.405(a) to include Health IT Modules certified to § 170.315(a)(9). We agree with commenters that requiring developers of certified health IT with Health IT Modules certified to § 170.315(a)(9) to engage in real world testing for only the period of time before the revised criterion expires is unnecessary. We continue to believe there is value for developers of certified health IT with Health IT Modules certified to § 170.315(a)(9) to demonstrate how their support of evidence-based CDS and linked referential CDS positively impacts patient care through real world testing plans and results; however, we think it would be more important for developers of certified health IT to spend time and resources conforming to requirements in § 170.315(b)(11) and § 170.402(b)(4) by January 1, 2025.

We note that because all criteria in § 170.315(b) are already subject to real world testing requirements in § 170.405, Health IT Modules certified to § 170.315(b)(11) prior to August 31, 2024, would need to, among other requirements, address each of the elements in § 170.405(b)(1)(iii)(A) through (G) in their real world testing plans by December 15, 2024, and submit results based on those plans no later than March 15, 2026.

We appreciate those commenters who supported our proposals for real world testing because it would have various benefits for more accurate, comprehensive, and contextual understanding of a model's performance. We also appreciate the commenters that stated how real-world testing will give developers an opportunity to determine if the user community is using their interventions, and if so, the ability to determine how the interventions are being used. We agree and we encourage developers of certified health IT to consider ways to demonstrate validity or fairness of Predictive DSIs in local data as a means to fulfill the requirements for real world testing plans and results.

Comments. A minority of commenters did not support including either § 170.315(a)(9) or § 170.315(b)(11) in real world testing and stated neither certification criterion appropriately fit the stated intent for the scope of Real world Testing Condition and Maintenance of Certification. One commenter recommended including § 170.315(a)(9) in real world testing, with the proposed updates, but only if ONC would keep § 170.315(a)(9) as a certification criterion and add § 170.315(b)(11) as a separate certification criterion, noting that requiring real world testing for Predictive DSI immediately after development and implementation is overly burdensome for developers.

Response. We appreciate these comments and we have not finalized our proposal to modify § 170.405(a) to include Health IT Modules certified to § 170.315(a)(9). We note that certification criteria at § 170.315(b) are already subject to real world testing requirements identified in § 170.405; thus, Health IT Modules certified to § 170.315(b)(11) will be subject to the same requirements currently applied to Health IT Modules certified to § 170.315(b)(1), for example. We believe real world testing would not be overly burdensome with the implementation of the DSI requirements under § 170.315(b)(11).

Comments. A few commenters questioned the logistics of real world testing CDS and DSI criteria and sought clarity on how the proposed real world testing plan will be assessed. Specifically, one commenter sought clarity on how real world testing would impact a health plan's existing operations. One commenter suggested that certification testing could be accomplished using a test data set that incorporates synthetic patient records containing a wide range of demographic and health condition information, including rare diseases and conditions, noting that DSI training and testing data should be developed in collaboration with provider, patient, research, and health IT partners and made available to all parties in a standardized, computable format. In the interest of program flexibility, one commenter suggested that real world testing of CDS should allow for some types of survey or questionnaire form for providers to offer feedback on the value and use of CDS in the EHR rather than trying to capture analytics or metrics on CDS use from the EHR as developers are required to do with other real world testing criteria.

Response. We note that we did not propose any changes to the requirements of real world testing plans and results submission, which are currently described in § 170.405(b)(1)–(2). We also invite readers to review discussion in the ONC Cures Act Final Rule at 85 FR 25766 and visit the numerous resources we have developed to support ongoing implementation of the real world testing Condition and Maintenance of Certification requirements at *https://www.healthit.gov/topic/certification-ehrs/real-world-testing.*

6. Synchronized Clocks Standard

We proposed at 88 FR 23811 to remove from 45 CFR 170.210(g) the current named specification for clock synchronization, which is Network Time Protocol (NTP v4 of RFC 5905). However, we proposed to amend 45 CFR 170.210(g) so that Health IT Modules certified to applicable certification criteria continue to utilize any Network Time Protocol (NTP) standard that can ensure a system clock has been synchronized and meets time accuracy requirements. The applicable certification criteria that either reference the NTP standard, revised in § 170.210(g), or cross-reference a provision that references § 170.210(g), include § 170.315(d)(2), § 170.315(d)(3), § 170.315(d)(10), and § 170.315(e)(1) (88 FR 23811).

Comments. Commenters, including health information technology companies, consumer and patient advocacy groups, health IT expert organizations, and professional trade

associations, uniformly agreed with our proposal to remove the named standard in § 170.210(g) and instead require the date and time recorded utilize a system clock that has been synchronized using any NTP standard. Several commenters welcomed the flexibility offered by this approach to use updated versions of NTP or specified versions of NTP, such as Microsoft's MS–SNTP. One commenter noted support for our proposal but urged consistency across organizational networks and systems to ensure that the same network time protocol is used across all servers and platforms.

Response. We appreciate the commenters' support for this proposal. We have finalized the changes as proposed, including the removal of a named standard in § 170.210(g), but we will require Health IT Modules to utilize a system clock that has been synchronized using any NTP standard.

Comments. A health IT expert organization requested ONC comment on the NTP test procedure by either explicitly removing the demonstration requirement or describing a test procedure to demonstrate time server accuracy to accommodate a variation in time services used.

Response. We thank the commenter for the comment. While the request is outside the scope of this final rule because conformance methods, including testing procedures, are not determined as part of notice and comment rulemaking, we will consider updating the test procedures in the future.

7. Standardized API for Patient and Population Services

In the HTI–1 Proposed Rule, we proposed to reorganize § 170.215 to delineate the purpose and scope more clearly for each type of standard or implementation specification (88 FR 23812). We refer readers to the HTI–1 Proposed Rule (88 FR 23812) for additional background history. We proposed to revise the structure of § 170.215 as follows:

Application Programming Interface Standards.

(a) *API base standard.*

(b) *API constraints and profiles.*

(c) *Application access and launch.*

(d) *Bulk export and data transfer standards.*

(e) *API authentication, security, and privacy.*

Comment. We received one comment supporting the revision of the structure of the API related standards.

Response. We thank the commenter for their support. We have finalized the revised structure of § 170.215 as proposed. This restructuring will impact cross-references in the certification criterion at § 170.315(g)(10) in several subparagraphs, including § 170.315(g)(10)(i)(A) and (B); § 170.315(g)(10)(ii); § 170.315(g)(10)(iv)(A) and (B); § 170.315(g)(10)(v)(A)(*1*)(*i*) and (*ii*); § 170.315(g)(10)(v)(A)(*2*)(*i*) and (*ii*); § 170.315(g)(10)(v)(B); and § 170.315(g)(10)(vii).

a. Native Applications and Refresh Tokens

In an interim final rule (IFR) published on November 4, 2020 (85 FR 70064), we addressed an ambiguity regarding how our refresh token requirements, in § 170.315(g)(10)(v)(A), would apply to ''native applications.'' [158] In response to public feedback in the IFR and subsequent interaction with interested parties, a history of which can be found in the HTI–1 Proposed Rule (88 FR 23812), we proposed in the HTI–1 Proposed Rule to remove mention of ''applications capable of storing a client secret'' from § 170.315(g)(10)(v)(A)(*1*)(*ii*) and § 170.315(g)(10)(v)(A)(*2*)(*ii*), as well as to revise § 170.315(g)(10)(v)(A)(*1*)(*ii*) to state, ''A Health IT Module's authorization server must issue a refresh token valid for a period of no less than three months to applications using the 'confidential app' profile according to an implementation specification adopted in § 170.215(c)'' (88 FR 23813). We also proposed to revise § 170.315(g)(10)(v)(A)(*2*)(*ii*) to state, ''A Health IT Module's authorization server must issue a refresh token valid for a new period of no less than three months to applications using the 'confidential app' profile according to an implementation specification adopted in § 170.215(c)'' (88 FR 23813). We stated that these proposed revisions would better reflect a Health IT Module's obligation for first time and subsequent connection refresh tokens using concepts familiar to industry and according to the HL7 FHIR SMART Application Launch Framework Implementation Guide (IG). We noted that existing requirements for Health IT Modules to issue a refresh token to native applications, consistent with § 170.315(g)(10)(v)(A)(*1*)(*iii*), remained unchanged.

We also stated in the HTI–1 Proposed Rule that we would continue to monitor implementation of § 170.315(g)(10), engage with the standards development community, and provide information through existing ONC Certification Companion Guides (CCGs), the ONC API Resource Guide, and other educational materials.

Comments. Many commenters expressed support for our proposal to revise § 170.315(g)(10)(v)(A)(*1*)(*ii*) and (*2*)(*ii*) to reference the ''confidential app'' profile defined in the HL7 FHIR SMART Application Launch Framework IG as part of our refresh token support requirements. Several of these commenters expressed appreciation for our reference to an industry standard and noted the important role of this standard for driving consistent implementations and interoperability.

Response. We appreciate the feedback from commenters. We have finalized our revisions to § 170.315(g)(10)(v)(A)(*1*)(*ii*) and (*2*)(*ii*) as proposed.

Comments. Some commenters raised concerns around the impacts to app developers of breaking API changes, particularly changes that affect refresh token validity. These commenters suggested requirements that app developers be given advance notification of upcoming breaking changes that affect refresh tokens.

Response. We appreciate these commenters' concerns and suggestions. We remind commenters of the scope of our revisions to § 170.315(g)(10)(v)(A)(*1*)(*ii*) and (*2*)(*ii*) in this final rule, and specifically note that our revisions do not change certain previously finalized requirements around refresh tokens, namely that Health IT Modules certified to § 170.315(g)(10) must issue refresh tokens valid for a period of no less than three months.[159] We also remind commenters of our existing API Conditions and Maintenance of Certification requirements at 45 CFR 170.404, which apply to developers of certified health IT with Health IT Modules certified to § 170.315(g)(10). Specifically, at § 170.404(a)(4)(iii), we have ''service and support obligations'' that Certified API Developers must abide by. These obligations include requirements for Certified API Developers to ''make reasonable efforts to maintain the compatibility of its certified API technology and to otherwise avoid disrupting the use of certified API technology in production environments'' by API Users. While we appreciate the specific suggestions from commenters for added requirements, we decline to add these requirements in this final rule. In the circumstance

[158] According to IETF RFC 6749, ''native applications are ''clients installed and executed on the device used by the resource owner (*i.e.,* desktop application, native mobile application).'' See IETF RFC 6749: *https://tools.ietf.org/html/rfc6749.*

[159] See § 170.315(g)(10)(v)(A)(*1*)(*ii*), (*iii*), and (*2*)(*ii*) in 85 FR 70083.

where a Certified API Developer must make a change to their technology that affects refresh token validity, we expect that the Certified API Developer abide by the obligations referenced above to enable the continued and effective production use of their certified API technology.

Comments. Some commenters suggested that refresh tokens for non-patient facing applications should be reviewed on a case-by-case basis for security reasons. One commenter asked that we clarify that apps may, at times, be required to request a new token with new access scopes instead of using a refresh token and that this is not a violation of our refresh token policies. Another commenter suggested that we change the requirements for the duration of refresh tokens and that three months is not always appropriate in all cases.

Response. We appreciate these suggestions from commenters. We do not agree that we should include separate requirements for refresh tokens that apply only in non-patient facing application use cases at this time. We remind this commenter of what we stated in the ONC Cures Act Final Rule at 85 FR 25746—25747 when responding to commenters who similarly raised security concerns and suggested we finalize different requirements for refresh tokens based on patient versus non-patient facing application use cases. Those sections of the ONC Cures Act Final Rule also clarify what implementers of § 170.315(g)(10)-certified Health IT Modules are allowed to do regarding refresh token length and clarify what practices we see as restricted. We stated in the ONC Cures Act Final Rule that ''[r]efresh tokens are commonly used in healthcare and other industries'' and that ''implementers of § 170.315(g)(10)-certified Health IT Modules are not prohibited from changing the length of refresh tokens for users of the API including patients and providers to align with their institutional policies.'' We also stated that ''implementers of § 170.315(g)(10)-certified Health IT Modules should be mindful of information blocking provisions applicable to them and that requiring patients to re-authenticate and re-authorize at a high frequency could inhibit patient access and implicate information blocking'' (85 FR 25747).

Regarding duration of refresh tokens, we again remind commenters of what we clarified in the ONC Cures Act Final Rule where we noted that ''we believe a refresh token valid for a period of three months is sufficient to balance persistent access and security concerns'' (85 FR 25747). We also stated that implementers (*e.g.,* hospitals) ''of § 170.315(g)(10)-certified Health IT Modules are not prohibited from changing the length of refresh tokens for users of the API, including patients and providers, to align with their institutional policies. Further, implementers of § 170.315(g)(10)-certified Health IT Modules are not prohibited from implementing their § 170.315(g)(10)-certified Health IT Modules in accordance with their organizational security policies and posture, including by instituting policies for re-authentication and re-authorization (*e.g.,* providers and/or patients could always be required to re-authenticate and re-authorize after a set number of refresh tokens have been issued)'' (85 FR 25747). Further, we clarify that § 170.315(g)(10)-certified Health IT Modules may require a new authorization request from an application to provision that application with scopes not already granted.

In acknowledgement of the comments received, we have finalized our requirements in § 170.315(g)(10)(v)(A)(*1*)(*ii*) and (*2*)(*ii*) to reference the ''confidential app'' profile defined in the HL7 FHIR SMART Application Launch Framework as proposed.

b. FHIR United States Core Implementation Guide Version 5.0.1

In the HTI–1 Proposed Rule, 88 FR 23813 to 238144, we included a proposal to adopt the FHIR US Core IG v5.0.1 in § 170.215(b)(1)(ii) and incorporate it by reference in § 170.299. We noted that based on the annual US Core release cycle, the FHIR US Core IG v6.0.0 would likely be published between the release of the HTI–1 Proposed Rule and our finalization of this final rule. Assuming the FHIR US Core IG v6.0.0 was published prior to the release of this final rule, we stated that we would consider adopting v6.0.0 rather than v5.0.1. We stated our belief that the FHIR US Core IG v6.0.0 would support the data elements and data classes in USCDI v3, which we also proposed to adopt in the HTI–1 Proposed Rule.

In addition, we proposed to update some of the cross-references to the FHIR US Core IG v3.1.1 in § 170.215(a)(2) in § 170.315(g)(10)(i)(A) and (B), (ii)(A) and (iv)(A) to instead refer to FHIR US Core IG v5.0.1. Finally, we proposed to restructure the standards in § 170.215 to better categorize API standards and to enable simultaneous use of different versions of IGs for a set period. For example, we proposed categorizing the US Core IG v3.1.1 in § 170.215(b)(1)(i) as part of a group of standards for constraining and profiling data elements, and we proposed that the adoption of this standard would expire on January 1, 2025. We proposed to include the US Core IG v5.0.1 in this same group in § 170.215(b)(1)(ii).

Comments. Commenters overwhelmingly supported our proposal to advance the version of the FHIR US Core IG included in § 170.215 and incorporated by reference in § 170.299. Most of the commenters specifically voiced support for including the FHIR US Core IG v6.0.0, which was published in May 2023 and supports the data elements and data classes in USCDI v3. We did not receive any comments in favor of adopting the FHIR US Core IG v5.0.1 rather than v6.0.0. Commenters noted that the FHIR US Core IG v6.0.0 aligns with our proposals elsewhere in the HTI–1 Proposed Rule, including our proposals to adopt USCDI v3 and the SMART v2 IG.

We received only one comment in opposition to the proposal to advance the version of the FHIR US Core IG, which expressed concerns about the limited amount of time for developers to test and implement v5.0.1. While still supportive of advancing the version of the FHIR US Core IG, several other commenters also expressed concerns about the timelines for adoption of the latest version. These commenters urged ONC to acknowledge the development time and effort required to support a newer version of the US Core FHIR IG and consider extending the deadline for certification to a newer version.

Response. We thank the commenters for their support. The HL7 standards development community published FHIR US Core 6.0.0 in May 2023. As anticipated, FHIR US Core 6.0.0 added new and updated FHIR profiles to represent new data elements and classes included in USCDI v3. We considered adopting FHIR US Core 5.0.1 and FHIR US Core 6.0.0 and using the Standards Version Advancement Process (SVAP) to enable developers of certified health IT to use FHIR US Core 6.1.0 to certify Health IT Modules that require support of the USCDI. However, we concluded that this would be insufficient to achieve our policy objectives for improved interoperability and lead to misalignment in the marketplace. This is because use of the SVAP by developers of certified health IT is voluntary and experience to-date indicates that a minority of developers of certified health IT choose to avail their Health IT Modules to use newer standards. Adopting FHIR US Core 6.1.0 establishes a consistent baseline across all Health IT Modules certified to

criteria that reference the USCDI and provides clarity to developers of certified health IT regarding which version of the US Core IG they are expected to use in support of USCDI v3 and which version they can expect to encounter when interacting with other actors in the health IT ecosystem, industry-wide.

After the publishing of FHIR US Core 6.0.0, HL7 found errors with how the guide implemented data elements in USCDI v3 and had to make updates to the specification to align with USCDI v3 and ensure that USCDI v3 can be implemented in Health IT Modules. Adopting FHIR US Core 6.1.0 is necessary for developers of certified health IT to have appropriate implementation guidance to meet the criteria adopted in this final rule that reference USCDI v3. Based on public comments on this and prior rulemakings, we believe that the health IT industry, healthcare standards developers, and health care providers expect and support ONC making such determinations so that the adopted version of standards are the most up-to-date available and are feasible for real world implementation (see, for example, 85 FR 25677 and 25708).

We have finalized the adoption of the FHIR US Core 6.1.0 in § 170.215 and incorporated it by reference in § 170.299. We have also finalized our proposal to restructure the standards in § 170.215 and adopted the FHIR US Core 6.1.0 at § 170.215(b)(1)(ii). Likewise, we have finalized our proposal to categorize the FHIR US Core IG v3.1.1 in § 170.215(b)(1)(i) as part of a group of standards for constraining and profiling data elements and have finalized our proposal that the adoption of this standard would expire on January 1, 2026. With regard to concerns about compliance dates, we refer readers to the discussion in section II.C (General Comments on the HTI–1 Proposed Rule) of this final rule.

c. FHIR Endpoint for Service Base URLs

In the ONC Cures Act Final Rule, we finalized API Maintenance of Certification requirements in 45 CFR 170.404(b)(2) which contain a specific provision requiring Certified API Developers, for Health IT Modules certified to the certification criterion in § 170.315(g)(10), to publicly publish certain ''service base URLs''—otherwise known as ''endpoints''—for all their customers and in a machine-readable format at no charge (85 FR 25764—25765). These electronic endpoints are the specific locations on the internet that make it possible for apps to access EHI at the patient's request.

As we developed these service base URL publication requirements in the ONC Cures Act Final Rule, we acknowledged the importance of industry alignment and standardization in this area by indicating that we ''strongly encourage API Technology Suppliers, health care providers, HINs and patient advocacy organizations to coalesce around the development of a public resource or service from which all interested parties could benefit'' (84 FR 7494). We ultimately did not adopt specific standards for the publication format of these service base URLs in the ONC Cures Act Final Rule to provide industry an opportunity to coalesce on specifications. We finalized § 170.404(b)(2) to require that Certified API Developers must make their service base URLs freely accessible and in a machine-readable format at no charge (85 FR 25765).

However, since the ONC Cures Act Final Rule was published, we have found that developers with publicly discoverable endpoint lists have defined their own bespoke publication approaches and unique formats. This variability across developers of certified health IT in the format they are using to publish their service base URLs indicates the industry has not coalesced around a common framework or approach. Research conducted through ONC's Lantern Project confirms this variability among developers of certified health IT, which is hindering maturation of a vibrant app ecosystem for patients and the healthcare community,[160] a primary objective within the Federal Health IT Strategic Plan.[161]

The inconsistent implementation of our service base URL requirement has also rendered important data meant to facilitate connections to endpoints difficult to access.[162] Specifically, the organization details of the API Information Source associated with a service base URL is not always available, and even when available, is not always available in a format that can be readily used. Patient-facing apps require access to these service base URLs to provide patients access to information maintained by specific provider organizations that deploy certified API technology (*i.e.,* API Information Sources). Without standardized formats and an ability to search for service base URLs, patients are hindered in their ability to find which service base URL(s) refer to their provider. Similar barriers exist for others involved in healthcare seeking to leverage apps for interoperability.

Additionally, it is difficult to map multiple, unique organizations to service base URLs. Experience to-date indicates that the name of the organization associated with a service base URL is typically formatted as free text (*i.e.,* String). A single String is unable to represent the complexity of healthcare systems, where a system can contain many subsystems, or where a FHIR API URL can support a set of systems. Including all organizations that are serviced by a service base URL is important for discovery of which service base URL serves a particular health care provider, which in turn would allow API users to access relevant EHI through that service base URL. Having all healthcare organizations serviced by the service base URL accessible and in a standardized format would help app developers easily fetch information to enable patients and other users to access, exchange, and use information.

To address the inconsistencies in service base URL publication and challenges with mapping, we proposed in the HTI–1 Proposed Rule to revise the requirement in § 170.404(b)(2) to include new data format requirements (88 FR 23814). We anticipated that these new specifications would establish standards for industry adoption and better facilitate patient access to their health information. In the revised § 170.404(b)(2), we also proposed to incorporate the following existing requirements in § 170.404(b)(2)(i) and (ii): a Certified API Developer must publish service base URLs ''[f]or all of its customers regardless of whether the Health IT Modules certified to § 170.315(g)(10) are centrally managed by the Certified API Developer or locally deployed by an API Information Source;'' and publish these service base URLs ''at no charge'' as part of proposed § 170.404(b)(2). We proposed that Certified API Developers publish these standardized details by December 31, 2024.

In § 170.404(b)(2)(i), we proposed to require that service base URLs must be published in ''Endpoint'' resource format according to the FHIR standard adopted in § 170.215(a) (88 FR 23814). Additionally, in § 170.404(b)(2)(ii) and subparagraphs § 170.404(b)(2)(ii)(A) and § 170.404(b)(2)(ii)(B), we proposed to require that organization details such as name, location, and provider identifiers

[160] *https://www.healthit.gov/buzz-blog/healthit-certification/shining-a-light-on-fhir-implementation-progress-toward-publishing-fhir-endpoints.*

[161] See objective 1b in the 2020–2025 Federal Health IT Strategic Plan at *https://www.healthit.gov/topic/2020-2025-federal-health-it-strategic-plan.*

[162] *https://www.healthit.gov/news/events/onc-lantern-workshop.*

(*e.g.,* National Provider Identifier (NPI), CMS Certification Number (CCN), or health system ID) for each service base URL must be published in US Core ''Organization'' resource format according to the implementation specifications adopted in § 170.215(b)(1) (we note that elsewhere in this final rule, in section III.C.7.b, we discuss the proposal to move US Core IGs to § 170.215(b)(1)), with the ''Organization.endpoint'' element referencing the service base URLs managed by this organization.

We proposed the Endpoint and Organization resource formats because they are based on the FHIR Release 4 and US Core IG industry standards that are already adopted for use in the Program in § 170.315(g)(10). We specifically proposed the FHIR ''Endpoint'' resource because it is used for representing technical endpoint details and contains a required ''address'' element that, according to the FHIR R4 standard, contains ''the technical base address for connecting to this endpoint.'' [163] We noted that Certified API Developers would be able to populate this element, in each of their published ''Endpoint'' resources, with a service base URL that can be used by patients to access their EHI.

We additionally proposed the US Core ''Organization'' resource because it can be used to represent important contextual information around a service base URL (88 FR 23814 through 23815). We noted that the US Core ''Organization'' resource contains an optional ''endpoint'' element that can be used to reference ''technical endpoints providing access to services operated for the organization.'' [164] To standardize a link between published ''Endpoint'' resources and organization details relating to the organization that services these endpoints, we proposed to require, in § 170.404(b)(2)(ii)(A), that this optional ''endpoint'' element be populated on publicly published ''Organization'' resources and that they reference the ''Endpoints'' managed by the organization. We noted that ''publicly published'' meant that the information is made publicly available and noted that ONC will host a link to developers' service base URL list on the Certified Health IT Product List (CHPL) or another website hosted by ONC. We stated that this information would give the public a standard way of knowing how published ''Endpoint'' and published ''Organization'' resources are linked and which organization details apply to which service base URLs.

Additionally, we noted in the HTI–1 Proposed Rule that the US Core ''Organization'' resource contains a ''mandatory'' element called ''name'' that contains a ''name used for the organization'' (88 FR 23815). In addition to this required element, we proposed in § 170.404(b)(2)(ii)(B) to require Certified API Developers to make available ''must support'' elements of organization location and provider identifier(s) using the US Core ''Organization'' resource. An organization's location could be an address that is populated in the ''address'' element of the US Core ''Organization'' resource; and a provider identifier could be a National Provider Identifier (NPI), Clinical Laboratory Improvement Amendments (CLIA) number, or other health system ID populated in the ''identifier'' element. We noted that this information helps contextualize service base URLs and enables application developers to more easily and consistently provide patients access to their electronic health information.

Finally, we proposed, in § 170.404(b)(2)(iii), requirements for collection and maintenance of Endpoint and organization resources. Specifically, in § 170.404(b)(2)(iii)(A), we proposed to require that these resources be collected in a ''Bundle'' resource, according to the FHIR standard adopted in § 170.215(a), that the Certified API Developer would publicly publish (88 FR 23815). According to the FHIR specification, a ''Bundle'' acts as ''a container for a collection of resources'' and is widely used in use cases, such as returning search results and grouping resources as part of a message exchange.[165] Given the broad use of the ''Bundle'' resource throughout the FHIR specification (*e.g.,* FHIR search), we noted in the HTI–1 Proposed Rule our expectation that most FHIR clients and FHIR application developers would be familiar with the ''Bundle'' resource and be able to parse ''Bundle'' resources electronically and extract relevant information from them for use in their application. Alternatively, we considered a different format for requiring that the Endpoint and Organization resources be collected for publication. We also considered the Newline Delimited JSON (ndjson) format (88 FR 23815). According to the ndjson specification, this format is convenient for publishing ''structured data that may be processed one record at a time.'' [166] The ndjson format is an efficient way for machines to parse large amounts of data given that the entire file does not need to be read into memory before parsing. As we noted in the HTI–1 Proposed Rule, we expect that these ''Endpoint'' and ''Organization'' JSON resource lists may be large, depending on the developer of certified health IT's client base. We noted our expectation that most Certified API Developers would be familiar with this format because it is included as an underlying standard in the FHIR Bulk Data Access IG required for certification to § 170.315(g)(10). Given the simplicity of the ndjson standard, we also noted our expectation that most FHIR clients and FHIR application developers would easily be able to parse ndjson files electronically and extract relevant information from them for use in their application.

We also proposed, in § 170.404(b)(2)(iii)(B), that Certified API Developers review Endpoint and Organization resources quarterly and, as necessary, update the information (88 FR 23815). We recognized that as customers upgrade and install new health IT, data provided in the Endpoint and Organization resources will change. In the HTI–1 Proposed Rule, we noted that a one-time publication of the developer's current list of endpoints for active customers upon certification to the § 170.315(g)(10) criterion will only meet initial certification requirements, and we proposed to establish in § 170.404(b)(2)(iii)(B) a requirement that Certified API Developers maintain this information over time. We also noted that failure to maintain the service base URLs and ensure the associated organization information remains up to date and free of errors or defects on a quarterly basis would be considered a violation of this Condition and Maintenance of Certification requirement and may result in corrective action. We clarified that any endpoint or organization information that is out of date, incomplete, or otherwise unusable for more than 90-days would be considered in violation of this proposed requirement.

Comments. The majority of commenters support the continued development and standardization of publication formats for FHIR ''service base URLs'' otherwise known as ''endpoints,'' noting that standardization would better facilitate interoperability and address challenges that exist in operationalizing connections to FHIR servers for facilitating patient access. Many of these supportive commenters cautioned that our proposal does not align with the direction of industry and one

[163] *https://hl7.org/fhir/R4/endpoint.html.*

[164] *https://www.hl7.org/fhir/organization.html.*

[165] *http://hl7.org/fhir/R4/bundle.html.*

[166] *http://ndjson.org/.*

commenter raised a particular concern that our proposal is not based in implementation experience and has not been informed by a draft implementation guide. Another commenter noted that since we are proposing that the ''endpoint'' element in the US Core ''Organization'' resource be used to reference FHIR R4 ''Endpoint'' resource(s), we should make specific and clear reference to the applicability of FHIR R4 and its detailed standards on Endpoint. Most of these commenters also offered suggestions on how we should change our proposal by citing the Argonaut implementation guide for Patient-access Brands as standard and the industry driven approach we should consider referencing for this endpoint publication use case.

Response. We thank the commenters for their support of the continued development in this space and suggestions for improvement. The ''Patient-access Brands'' conceptual model, developed by the FHIR community through the Argonaut Project, has advanced significantly since publication of the HTI–1 Proposed Rule. A connectathon, which is an event where the FHIR community gathers and tests emerging FHIR standards, was held in May 2023 and it included developers of certified health IT and app developers who tested the real-world feasibility of the Patient-access Brands model.[167] Additionally, at the September 2023 HL7 Working Group Meeting, the FHIR community discussed and finalized new changes to the Patient-access Brands model.[168] Currently, the Patient-access Brands model is incorporated into a section of the continuous build draft version of the SMART App Launch IG.[169] This indicates that the Patient-access Brands model is now a draft specification and is on track for publication in a future version of the SMART App Launch IG.

We agree with commenters that the Patient-access Brands specification is a key standardized approach for the endpoint publication use case and we are committed to aligning our requirements with industry efforts. In the HTI–1 Proposed Rule, our proposal generally aligned with the current draft Patient-access Brands specification by calling for the use of ''Organization'' and ''Endpoint'' FHIR resources for representing endpoints (*e.g.,* service base URLs) and corresponding organization (*e.g.,* API Information Source) details in a standardized format.

Additionally, in the HTI–1 Proposed Rule, our proposal, similarly to the current draft of Patient-access Brands specification, called for the use of the ''endpoint'' element in the US Core ''Organization'' resource for linking ''Endpoint'' resources and organizational details relating to the organization that services this endpoint.[170] However, our proposal in the HTI–1 Proposed Rule is not an exact match of the underlying construct defined in the Patient-access Brands specification. One key difference that could result in incompatibilities between our requirements and the industry led efforts in the Patient-access Brands specification is that we referenced the US Core profile of the base FHIR ''Organization'' resource, while the Patient-access Brands specification includes its own custom profile of the base FHIR ''Organization'' resource. Both profiles are based off the base FHIR ''Organization'' resource, but they each contain their own sets of constraints to best match their use cases.

Based on commenter feedback, we do not believe it is necessary for us to impose US Core level ''Organization'' resource constraints and reference the FHIR ''Organization'' resource via the US Core IG at this time. We agree with the commenter who recommended a specific and clear reference to the applicability of FHIR R4. We realize that we introduced some unnecessary confusion by referencing two separate but related standards, namely FHIR R4 and US Core, in separate paragraphs of our proposed criterion updates in § 170.404(b)(2). To simplify our requirements and make a more specific and clear reference to FHIR R4, we believe it is necessary to reference one standard, namely FHIR R4. We also agree with the many commenters who emphasized the importance of considering and not conflicting with the standards developed by the FHIR community for the endpoint publication use case, and we believe that referencing the more general FHIR R4 standard for our Program reduces the risk of conflicting requirements.

To generalize our proposal, respond to commenter feedback, and to align our requirements with emerging industry standards for the endpoint discovery use case, we have finalized a modified version of our proposed requirements at § 170.404(b)(2). We have modified the standard referenced in § 170.404(b)(2)(ii) to require the use of the base FHIR ''Organization'' resource instead of the more constrained US Core-profiled version of the base FHIR ''Organization'' resource. Specifically, we have revised § 170.404(b)(2)(ii) to reference the standard adopted in § 170.215(a). We emphasize that subparagraphs of finalized § 170.404(b)(2)(ii)(A) and (B) remain largely unchanged, meaning that Certified API Developers will still be required to reference ''Endpoint'' resources using the ''endpoint'' element in the ''Organization'' FHIR resource and will still be required to publish organization details such as name, location, and facility identifier. With this modification, we have finalized a policy that is less prescriptive than what we proposed. By referencing the base FHIR ''Organization'' resource, instead of the US Core-profiled ''Organization'' resource, Certified API Developers have more flexibility to support the ''Organization'' resource without minimal element constraints and no elements are marked as ''must support.'' We note that when proposing the US Core ''Organization'' resource profile, we referenced certain mandatory and ''must support'' elements contained in that profile, including ''address,'' ''name,'' and ''identifier.'' We did not adopt these constraints; rather, we are leaving it up to the Certified API Developer to determine how best to publish the required organization details using the base FHIR standard instead of the more constrained US Core IG. Overall, this change will provide industry with more flexibility to meet Program requirements as standards evolve. We have finalized our proposal in § 170.404(b)(2) to require Certified API Developers to publish these standardized details by December 31, 2024, as proposed. We clarify that for the time period between when this final rule is effective and December 31, 2024, that Certified API Developers may fulfill their obligations at § 170.404(b)(2) by publicly publishing the service base URLs for all customers in a machine-readable format at no charge.

This modification supports our goal of addressing the inconsistent implementation of our service base URL requirement and better facilitates

[167] More information on this connectathon can be found at *https://confluence.hl7.org/pages/viewpage.action?pageId=90350859#EndpointCallNotes-2023-5-312-5pET:Connectathon.*

[168] See *https://jira.hl7.org/browse/FHIR-42134.*

[169] *https://build.fhir.org/ig/HL7/smart-app-launch/branches/pab/brands.html.*

[170] During the public comment period for the HTI–1 Proposed Rule, the draft Patient-access Brands specification called for the use of the ''managingOrganization'' element in the ''Endpoint'' resource for linking ''Endpoint'' and ''Organization'' resources. At the September 2023 HL7 Working Group Meeting, occurring after the comment period for the HTI–1 Proposed Rule closed, the FHIR community approved a change to use the ''endpoint'' element in the ''Organization'' resource instead of the ''managingOrganization'' element in the ''Endpoint'' resource for linking ''Endpoint'' and ''Organization'' resources. See *https://jira.hl7.org/browse/FHIR-42134.*

patient access to their health information by requiring the use of a consistent data format, while also reflecting feedback received from software developers, technology companies, and standards developer interested parties. This modification also better aligns our requirements with the underlying data format constructs currently defined in the leading, and still emerging, industry specification in this area, namely the Patient-access Brands specification. We hope to give Certified API Developers the option of using the data format structure in Patient-access Brands specification to publish their service base URLs and organization data we require without being in conflict with our data format requirements for the Program. We note that at the time of publication of this final rule, the Patient-access Brands specification is still in draft form and may evolve over time, including the addition of breaking changes. We will consider the Patient-access Brands specification for adoption in future rulemaking as it develops.

Comments. In addition to the Patient-access Brands specification, several commenters noted the Directory IG for TEFCA as a standard to consider for the endpoint publication use case. All but one of these commenters cited the Directory IG for TEFCA alongside the Patient-access Brands specification and advocated for the alignment of TEFCA with the Patient-access Brands specification. One commenter advocated specifically for changes to our proposal based on the Directory IG for TEFCA, stating that we should consider it for defining the format of FHIR ''Organization'' and ''Endpoint'' resources for the endpoint publication use case.

Response. We appreciate the notes from commenters pointing us to other work in the endpoint publication space to consider. The Directory IG for TEFCA is under active development and is being designed to support the TEFCA use case and the participants within that framework. [171] We agree that this IG is an important standard to keep in mind for supporting the endpoint publication use case more broadly but, because it already includes constraints and extensions that go beyond the relatively small set of elements we proposed requiring of developers, we do not agree with the commenter who suggested using it for specifying the format of FHIR ''Organization'' and ''Endpoint'' resources used for publishing endpoints in our Program at this time. However, we note that because we have finalized an approach in § 170.404(b)(2) that references the base FHIR standard, Certified API Developers have the flexibility to consider using ''Organization'' and ''Endpoint'' FHIR resources profiles, such as the profiles in the Directory IG for TEFCA, to meet our requirements.

Regarding the suggestions to align TEFCA with the Patient-access Brands specification, we thank commenters for this suggestion but note that it is outside the scope of the proposals related to TEFCA in the HTI–1 Proposed Rule. We will continue to monitor the development of these standards and may take them into consideration in future rulemaking.

Comments. A number of commenters asked that we clarify the intended use of the organization details we proposed to be published. More specifically, commenters asked that we clarify that we expect organization or facility level identifiers, rather than individual practitioner identifiers, to be published. Many of these commenters noted that the publication of individual practitioner identifiers is out of scope for our intended use case. Additionally, one commenter noted the active work on a National Directory FHIR IG and said that it would be an approach to consider if we intend for practitioner level identifiers to be published.

Response. We appreciate commenters' input and suggestions for clarity. We intend for these additional organization details to be used by app developers to help them map organizations to endpoints which, in turn, helps patients find the organization(s) they want to allow an app to access data from. We clarify that facility or organization level identifiers are sufficient to satisfy our proposed publication requirements. Facility level identifiers, for the purposes of certification to these Endpoint publication requirements, include identifiers such as: a National Provider Identifier (NPI), Clinical Laboratory Improvement Amendments (CLIA) number, CMS Certification Number (CCN), or other health system ID. Support for one of these identifier types is sufficient, meaning Certified API Developers are not required to publish individual NPIs as a floor for certification. Different identifiers may be used depending on the customers a Certified API Developer has. We have updated our regulatory text at § 170.404(b)(2)(ii)(B) to more clearly state that ''[e]ach Organization resource must contain the organization's name, location, and facility identifier.''

For clarity and consistency, we have also updated our regulatory text at § 170.404(b)(2), and the relevant preamble text in this final rule, to replace the word ''organizational'' with ''organization.'' The phrase ''organization details'' more accurately represents the details we are referring to and is a consistent phrase to use in lieu of our mixed use of ''organizational'' and ''organization'' in the HTI–1 Proposed Rule.

Regarding the comment on the active work on a National Directory FHIR IG, we thank this commenter for pointing this out. Because we have not required the publication of individual provider-level identifiers, we are not considering this IG for the endpoint publication use case in our Program. We emphasize again that because we have finalized an approach in § 170.404(b)(2) that references the base FHIR standard, Certified API Developers have the flexibility to consider using ''Organization'' and ''Endpoint'' FHIR resources profiles, such as the profiles in the National Directory FHIR IG, to meet those requirements.

Comments. A couple of commenters asked that we clarify our requirements for elements in the Endpoint and Organization FHIR resources if we are updating to US Core version 6.

Response. We thank the commenters and we note that, given the changes we have made to § 170.404(b)(2)(ii) (see response to comments above), US Core is no longer in scope. We have modified the standard referenced in § 170.404(b)(2)(ii) to require the use of the base FHIR ''Organization'' resource instead of a US Core-profiled ''Organization'' resource.

Comments. A few commenters responded to our invitation for comment on whether we should finalize our proposal to adopt a requirement for FHIR Endpoint and Organization resources to be made publicly available according to the FHIR Bundle format or if we should finalize the requirement to use a ndjson format. These commenters were generally split on which format they prefer. One commenter noted that large FHIR Bundles are challenging to parse. Another commenter suggested that we align with a format that is most compatible with Lantern to support certification.

Response. We appreciate these responses and suggestions from commenters. We have finalized, at § 170.404(b)(2)(iii)(A), our requirement for FHIR Endpoint and Organization resources to be collected in FHIR Bundle resource format. We recognize that large FHIR Bundles may be hard to parse given their size, but we anticipate that app developers will have the technology and access to the tools

[171] *https://rce.sequoiaproject.org/RCEIG/output/index.html.*

needed to parse large machine-readable artifacts. We also note that the current draft Patient-access Brands specification calls for the use of FHIR Bundles to collect FHIR Endpoint and Organization details.[172] We believe that our finalized requirement for publication using the FHIR Bundle resource format sufficiently supports app developers and aligns with industry direction.

We thank commenters for supporting Lantern, which is an open-source tool developed by ONC and the MITRE corporation ''that monitors and provides analytics about the availability and adoption of FHIR API service base URLs (endpoints) across healthcare organizations in the United States.'' [173] We anticipate that Lantern and other FHIR tools will be able to take advantage of our standards-based and machine-readable approach to monitor and discover FHIR endpoints. We also note that the Program will continue to explore ways to support conformance and certification to these requirements to enable patients and other users to access, exchange, and use information via discoverable FHIR APIs.

Comments. One commenter suggested that both human readable and machine-readable Endpoint metadata be made available on the CHPL.

Response. We thank this commenter for their suggestion. We acknowledge that human readable Endpoint metadata may be useful for some use cases, but we do not believe that is a necessary additional requirement to put on Certified API Developers in our Program. We note that by requiring machine-readable publication using a standardized FHIR format, developers can consider developing their own tools or leveraging existing community tools (*e.g.,* Lantern) that render FHIR data into human readable formats.

Comments. One commenter explicitly expressed support for the quarterly review timeline we proposed for Certified API Developers in § 170.404(b)(2)(iii)(B), while two commenters recommended changes to the timeline. The two commenters who recommended changes indicated that a quarterly review minimum was too long given that inaccurate organization details and non-functioning endpoints significantly hinders interoperability. One of these two commenters suggested the review timeline be one week and the other suggested that ONC notify organizations of any inaccurate information after 30 days and find them in violation if no corrective updates are made after 60 days.

Response. We appreciate the feedback and thoughtful suggestions for possible improvement from commenters. We agree that this information needs to remain up to date to ensure application developers can easily and consistently provide patients access to EHI. We also acknowledge the need to consider the burden on Certified API Developers to keep their customers' endpoint information up to date. To balance value and burden, we have finalized the review timeline as proposed and have finalized a quarterly review timeline as the requirement. In response to commenters' suggestion that ONC monitor and notify interested parties of inaccurate information and initiate corrective action after 60 days, we note that we have a defined process to elevate concerns of non-conformity and we urge users or other interested parties to leverage this process.[174]

Comments. Many commenters suggested that ONC work on a process for validating and monitoring these endpoints. Many of these commenters also suggested that we develop a directory of these endpoints. One commenter specifically cited our Lantern tool as a central place where these endpoints could be submitted and validated.

Response. We thank the commenters for their feedback and suggestions. All Certified API Developer published Endpoint and Organization FHIR resource Bundles will be available publicly via the CHPL. Links to these Bundles are collected during the certification process by the ONC-Authorized Certification Bodies (ONC–ACB) and posted on a product's CHPL listing following successful certification. This public data can be used by anyone for collection and monitoring. This includes ONC's open-source Lantern tool. ONC hosts a public instance of this tool at *https://lantern.healthit.gov/* and collects data into this instance from many sources, including the CHPL, to monitor and provide analytics about the availability and adoption of FHIR API endpoints.[175] We encourage interested parties to visit the Lantern tool and we will continue to consider ways to ensure that service base URLs required in the Program continue to support individuals' access to their health information.

Comments. A few commenters expressed concern over the burdens and challenges for EHR developers to collect this information from their customers and be responsible for it being up to date. This included comments that Certified API Developers should not be penalized if and when their customers do not provide this information. One commenter asked that ONC clarify that Certified API Developers can rely on assurances provided by their customers that this information is valid and up to date, because it will not be feasible for developers to independently validate the information, and that Certified API Developers should instead only be expected to publish information for customers that provide details to the Certified API Developers, rather than an expectation that endpoint and organization detail lists are comprehensive. A couple of commenters suggested the introduction of a CMS attestation for providers and hospitals to be responsible for this information and keeping it up to date.

Response. We appreciate the feedback from commenters and acknowledge these concerns from Certified API Developers about gathering endpoint and organization information from their customers and being responsible for its publication. However, we did not propose and have not finalized any changes to our existing policy at § 170.404(b)(2) that requires Certified API Developers to publicly publish the service base URLs for all of their customers regardless of whether the Health IT Modules certified to § 170.315(g)(10) are centrally managed by the Certified API Developer or locally deployed by an API Information Source. As we said in the ONC Cures Act Final Rule with regards to publication of service base URLs, we believe that Certified API Developers will have adequate relationships with API Information Sources in the process of providing Health IT Modules certified to § 170.315(g)(10) to gather the necessary information (85 FR 25765). We believe that these same relationships are adequate for Certified API Developers to be able to collect and publish service base URLs, organization names, organization locations, and facility identifiers on behalf of their customers. We do not agree that it will be infeasible for Certified API Developers to provide validated URLs for customers that locally deploy certified API technology because details related to customer names, organization locations, and facility identifiers should be routinely and readily available during the business process (*i.e.,* a Certified API Developer licensing or selling use of certified API technology to a customer). We remind commenters of our focus for

[172] *https://build.fhir.org/ig/HL7/smart-app-launch/branches/pab/brands.html.*

[173] *https://lantern.healthit.gov/?tab=dashboard_tab.*

[174] *https://www.healthit.gov/topic/certified-health-it-complaint-process.*

[175] *https://lantern.healthit.gov/?tab=about_tab.*

this criterion on service base URLs and related organization details for Health IT Modules certified to § 170.315(g)(10) that can be used by patients to access their EHI. We believe that the effort needed to collect this information is warranted given the critical role it plays in enabling third-party apps to access EHI at a patient's request.

We appreciate the feedback and suggestions from commenters on potential points of intersection between our requirements and CMS requirements. Updates to CMS programs are out of scope of this rule, but we encourage commenters to submit such ideas to CMS.

Comments. A few commenters suggested that we work with CMS and other federal partners to ensure our requirements do not duplicate other efforts and to ensure that the necessary infrastructure is in place to support this requirement. One commenter specifically cited CMS's ongoing effort to develop a national directory.

Response. We appreciate the feedback from commenters. We will continue to coordinate and work with our federal partners, including CMS, on points of intersection for potential future rulemaking.

d. Access Token Revocation

In the ONC Cures Act Final Rule, we established a requirement in § 170.315(g)(10)(vi) that for Health IT Modules certified to § 170.315(g)(10), the Health IT Module's authorization server must be able to revoke an authorized application's access at a patient's direction (85 FR 25945). This required capability is intended to enable patients to ''definitively revoke an application's authorization to receive their EHI until reauthorized, if ever, by the patient'' (85 FR 25747). We noted in the ONC Cures Act Final Rule that we finalized § 170.315(g)(10)(vi) as a functional requirement to allow health IT developers the ability to implement it in a way that best suits their existing infrastructure and allows for innovative models for authorization revocation to develop (85 FR 25747). We understand that a lack of specificity in the current requirement has led to some confusion among health IT developers and application developers.

As part of health IT developers' implementation of these requirements, we have received feedback regarding the implementation of authorization revocation, specifically around the revocation of access tokens. Health IT developers have requested clarification regarding letting access tokens expire in lieu of immediate access token revocation for the purposes of certification testing. The Oauth 2.0 Token Revocation specification, RFC 7009, describes expiration of short-lived access tokens as a design option for authorization servers to revoke an application's access. This design option conforms with industry standard practice and may reduce health IT developer burden as the Health IT Module would not have to perform token introspection for each resource request nor maintain a database of valid access tokens.

In the HTI–1 Proposed Rule, we proposed to revise the requirement in § 170.315(g)(10)(vi) to specify that a Health IT Module's authorization server must be able to revoke and must revoke an authorized application's access at a patient's direction within 1 hour of the request (88 FR 23816). This requirement aligns with industry standard practice of short-lived access tokens as specified in internet Engineering Task Force (IETF) Request for Comments (RFC) 6819,[176] IETF RFC 7009,[177] and Section 7.1.3 of the SMART Application Launch Framework version 1.0.0, which states that ''Access tokens SHOULD have a valid lifetime no greater than one hour. Confidential clients may be issued longer-lived tokens than public clients.'' This policy would provide clarity and create a consistent expectation that developers revoke access within 1 hour of a request, regardless of their internal approach to fulfilling a patient's request to revoke access. This policy would also assure patients that once requested, an application's access to their data would be revoked within 1 hour. This would also support situations where a patient may have an unexpected change in their privacy concerns and seek to curtail access to their information.

Comments. The majority of commenters supported our proposal to revise § 170.315(g)(10)(vi) to specify that a Health IT Module's authorization server must be able to revoke and must revoke an authorized application's access at a patient's direction within 1 hour of the request. Several commenters, including health IT companies, medical software companies, professional trade associations, some healthcare systems, and consumer/patient advocacy groups agreed with our rationale that such a requirement supported patients' direct control over the applications that have access to their EHI, and that the requirement is consistent with industry standards.

Response. We appreciate the feedback from commenters. We believe our proposal would assure patients that once requested, an application's access to their data would be revoked within 1 hour and that such revocation could be supported by all Health IT Modules regardless of their internal approach to fulfilling a patient's request to revoke access. We appreciate the overall strong support for our proposal that, for Health IT Modules certified to § 170.315(g)(10), the Health IT Module's authorization server must be able to revoke and must revoke an authorized application's access at a patient's direction within 1 hour of the request. We have adopted our proposal in § 170.315(g)(10)(vi) without revisions.

Comments. A small number of commenters opposed our proposal, for differing reasons. A healthcare system and a medical software company commented that 1 hour is too long a period of time to execute a revocation request, and a trade organization said 1 hour was too short. Two commenters worried about implications related to information blocking, including a professional trade association that said that providers should be able to request that an app developer delete any data received through the API between when the request was made and when access had been revoked without trigging information blocking concerns, and a medical software company worried about information blocking claims if revocation within 1 hour was not feasible due to technical challenges, such as a network outage at a cloud provider.

Response. We appreciate these commenters' concerns. However, we note that this proposed requirement aligns with industry standard practice of short-lived access tokens as specified in IETF RFCs 6819 and 7009. We also note that this 1-hour requirement does not preclude a Health IT Module from revoking access in a shorter timeframe; rather, it establishes a maximum timeframe for the revocation of access once requested. Based on community feedback, we respectfully disagree with the commenter indicating that 1 hour is not enough time to process such a request; industry consensus, as discussed above with the IETF RFCs, and experience with implementing the Program requirement to-date, indicates that many, if not most, requests can be easily fulfilled within 1 hour. We have established this timeframe to clearly delineate Program expectations, which did not previously exist. Finally, we appreciate commenters' concerns regarding information blocking; however, we currently do not provide

[176] Available at: *https://www.rfc-editor.org/pdfrfc/rfc6819.txt.pdf.*

[177] Available at: *https://www.rfc-editor.org/pdfrfc/rfc7009.txt.pdf.*

an exception specific to access token revocation and we decline to do so at this time. We also invite readers to review the discussion regarding the Infeasibility Exception, finalized by the ONC Cures Act Final Rule in § 171.204 (85 FR 25866–25875), and our discussion of the Infeasibility Exception and its *responding to requests* condition (§ 171.204(b)) discussed in section IV.C.1 of this final rule.

Comments. One commenter from a health system recommends that the ONC liaise with the Federal Trade Commission (FTC) to consider introducing a requirement such that, when consumer apps that access, exchange, or use personal health records experience a breach and are required to notify users of such a breach, those apps also include easy-to-understand instructions about how to revoke access to that application via certified health IT products and the timeframe in which such revocation must occur.

Response. We appreciate the comment and will continue to coordinate and work with our federal partners, including the FTC, on points of intersection for potential future rulemaking.

We appreciate the overall strong support for our proposal that a Health IT Module's authorization server must be able to revoke and must revoke an authorized application's access at a patient's direction within 1 hour of the request and we have adopted our proposal in § 170.315(g)(10)(vi) without revisions.

e. SMART App Launch 2.0

In the ONC Cures Act Final Rule, we adopted the HL7 FHIR SMART Application Launch Framework Implementation Guide Release 1.0.0 (SMART v1 Guide), a profile of the Oauth 2.0 specification, in § 170.215(a)(3) (85 FR 25741). The SMART v1 Guide provides reliable, secure authorization for a variety of app architectures through the use of the Oauth 2.0 standard. This IG defines various capabilities for app support, known as the ''SMART on FHIR Core Capabilities'' (85 FR 25741). As part of adopting the implementation specification in § 170.215(a)(3), the ONC Cures Act Final Rule required support for these ''SMART Core Capabilities,'' which enable applications to securely perform standardized authentication and authorization as part of enabling receipt of patient EHI via a FHIR API.

In the ONC Cures Act Final Rule, the § 170.315(g)(10) ''Standardized API for patient and population services'' certification criterion required support for capabilities from the SMART v1 Guide as described in § 170.215(a)(3) to enable apps to securely perform authentication and authorization with the Health IT Module in a standardized manner. Additionally, the § 170.315(g)(10) criterion included additional requirements for technical capabilities specified in the SMART v1 Guide, requiring support for the issuance of ''refresh tokens'' valid for a period of no less than three months. This requirement was intended to reduce patient and provider burden to receive patient EHI using an application of their choice by potentially reducing the number of re-authorizations of the application. Support for refresh tokens facilitates patient and provider receipt of patient EHI by enabling an application to be authorized to receive data in a persistent manner, without requiring re-authorization of the application while the refresh token is valid. The § 170.315(g)(10) criterion required support for the issuance of refresh tokens valid for a period of no less than three months, so that an application could potentially be authorized to receive patient EHI for at least a three-month period without requiring re-authorization.

As part of the adopted implementation specification, we explicitly required mandatory support of the ''SMART Core Capabilities'' for Program testing and certification, and we stated that by requiring the ''permission-patient'' ''SMART Core Capability'' in § 170.215(a)(3), Health IT Modules presented for testing and certification to § 170.315(g)(10), via cross-references to § 170.215(a)(3), must include the ability for patients to authorize an application to receive their electronic health information (EHI) based on FHIR resource-level scopes (85 FR 25741, 25746). Practically, this means that patients would need to have the ability to authorize access to their EHI at the individual FHIR resource-level, from one specific FHIR resource (*e.g.,* ''Immunization'') up to all FHIR resources necessary to implement the standard adopted in § 170.213 and implementation specification adopted in § 170.215(a)(2). This capability gives patients increased control over how much EHI they authorize applications of their choice to receive.

The SMART App Launch Implementation Guide Release 2.0.0 (SMART v2 Guide) is the next major release of the SMART App Launch IG.[178] The SMART v2 Guide updates the features of the SMART v1 Guide by including revisions aligning with industry consensus to provide technical improvements and reflect security best practices. The SMART v2 Guide technical enhancements improve the authentication and authorization security layer provided by the SMART v1 Guide and enables increased capabilities and functionality for individual control of EHI. Therefore, we proposed to adopt the SMART v2 Guide in § 170.215(c)(2), and we proposed that the adoption of the SMART v1 Guide in § 170.215(c)(1) would expire as of January 1, 2025 (88 FR 23816). We clarified that both the SMART v1 Guide and SMART v2 Guide will be available for purposes of certification where certification criteria reference § 170.215(c) until the expiration date of January 1, 2025, after which time only the SMART v2 Guide will be available for certification.

As part of this proposal, we proposed to adopt several sections specified as ''optional'' in the SMART v2 Guide as ''required'' for purposes of the Program for certification criteria that reference § 170.215(c). Specifically, we proposed to adopt all Capabilities as defined in ''8.1.2 Capabilities,'' which include but are not limited to (1) backward compatibility mapping for SMART v1 scopes as defined in ''3.0.2 Scopes for requesting clinical data;'' (2) asymmetric client authentication as defined in ''5 Client Authentication: Asymmetric (public key);'' and granular scopes as defined in (3) ''3.0.2.3 Finer-grained resource constraints using search parameters.'' Additionally, we proposed to require support for the ''Patient Access for Standalone Apps'' and ''Clinician Access for EHR Launch'' Capability Sets from ''8.1.1 Capability Sets.'' Also, we proposed to adopt token introspection as defined in ''7 Token Introspection.'' Again, we clarified that for the period before January 1, 2025, Health IT Modules certified to certification criteria that reference § 170.215(c) may use either SMART v1 or SMART v2 for certification (88 FR 23817).

Further, we noted that the SMART v2 Guide includes section 3.0.2.3 ''Finer-grained resource constraints using search parameters,'' and associated ''3.0.2.4 requirement for support'' and ''3.0.2.5 experimental features,'' which present concepts for further development within the SMART v2 Guide (88 FR 23817). Together, these optional functionalities will enable more granular control for individuals, clinicians, and other users to share information with apps of their choice in more explicit ways. The granular scope functionality would empower patients and providers to share health data in a

[178] *https://hl7.org/fhir/smart-app-launch/STU2/index.html.*

more granular fashion, which would improve confidence in the use of third-party apps by allowing app users to decide which specific type of EHI they share with the app. These functionalities would help address privacy and security concerns of third-party app access to health data and further patient empowerment by providing the ability to limit an app's access to a granular, minimum set of health data, as determined by the app user. We proposed these sections for adoption as part of SMART v2 Guide with the understanding that either the SMART v2 Guide or another implementation guide such as the US Core Implementation Guide will define more specific requirements for finer-grained resource constraints using search parameters.

Comments. There was near universal support for adoption of the SMART v2 Guide among commenters, including health IT companies, software and IT firms, advocacy organizations, and health systems. Several commenters noted that the SMART v2 Guide would play a crucial role in promoting health data interoperability and facilitating seamless data exchange between healthcare systems and applications. However, there was strong support among many of these interested parties to adopt the newest balloted version of the SMART App Launch Implementation Guide, Release 2.1. (SMART v2.1 Guide), rather than the SMART v2 Guide. Several commenters highlighted the benefits of the SMART v2.1 Guide, including improved FHIR Context management and App State capability. Some commenters also recommended ONC require support for browser-based apps, including requirements from the SMART v2.1 Guide.

Response. We thank the commenters for their support. We have finalized the adoption of the SMART v2 Guide subject to modifications described later in this section. We believe that adoption of the SMART v2 Guide will enable an improved and more secure authorization process for applications to receive EHI from Health IT Modules. We appreciate commenters' input regarding adoption of the subsequent release of the SMART v2.1 Guide. We acknowledge there are noteworthy updates included in the SMART v2.1 Guide. However, given that the SMART v2 Guide has already been an established part of the Program via SVAP and rigorously tested as a result, we believe adopting the SMART v2 Guide as a baseline requirement is more appropriate at this time. We will consider potential ways the SMART v2.1 Guide could be included in the Program in the future, including through SVAP. We also clarify that browser-based apps fitting the definition of ''public clients'', or ''native applications'' as defined in internet Engineering Task Force Request for Comments 6749 (RFC 6749), are required to be supported by Health IT Modules certified to the § 170.315(g)(10) criterion, per the requirements of that criterion. Such relevant requirements for supporting ''public clients'' and ''native applications'' include the data response, search, registration, secure connection, authentication and authorization for patient and user scopes, and authorization revocation requirements in the § 170.315(g)(10) criterion, respectively at § 170.315(g)(10)(i)(A), § 170.315(g)(10)(ii)(A), § 170.315(g)(10)(iii), § 170.315(g)(10)(iv)(A), § 170.315(g)(10)(v)(A), and § 170.315(g)(10)(vi).

Comments. Commenters were mixed in their recommendations on our proposal to expire the use of the SMART v1 Guide as part of the Program on January 1, 2025, effectively requiring use of only the SMART v2 Guide for applicable certification criteria after that date. Among those interested parties that commented, professional associations urged ONC to finalize the timeline as proposed. Health information technology companies and one health system requested additional time, indicating that the proposed expiration timeframe of January 1, 2025, does not give organizations sufficient time to develop, test, and implement necessary changes to systems and processes.

Response. We thank the commenters for their input. We acknowledge the benefits of extending the timeframe in which the SMART v1 Guide is available for certification. Taking this into consideration, we have modified our proposal as suggested by commenters who recommended more time to adopt only the SMART v2 Guide. We have, therefore, finalized our modified proposal that the adoption of the SMART v1 Guide implementation specification expires on January 1, 2026, and we clarify that following expiration of the SMART v1 Guide, the SMART v2 Guide will be the only valid standard for certification criteria that reference § 170.215(c).

i. SMART v2 Guide New and Revised Features Proposed for Adoption

The SMART v2 Guide introduces new or revised requirements to the previous version of the implementation guide, SMART v1 Guide. Major requirements new to the SMART v2 Guide include support for the OAuth 2.0 security extension Proof Key for Code Exchange (PKCE), as well as a revision of the scope syntax. The SMART v2 Guide includes requirements that both the EHR and all apps support the OAuth 2.0 security extension PKCE. PKCE is an industry standard security extension for OAuth 2.0 to mitigate the known security vulnerability of authorization code interception attacks.[179] The requirement of support for PKCE especially improves the security of native apps, or apps that operate from an individual's phone or tablet, which were particularly vulnerable to authorization code interception attacks.

Another major change included in the SMART v2 Guide is revision of the syntax of scopes provided to apps. To align with the FHIR interactions of ''Create,'' ''Read,'' ''Update,'' ''Delete,'' ''Search,'' collectively known as ''CRUDS,'' scopes are constructed to consist of combinations of five types of permissions corresponding to the CRUDS interactions. The use of this CRUDS scope syntax permits improved patient choice for persistent access as more specific combinations of permissions can be granted to apps as opposed to the scope syntax used in the SMART v1 Guide, which only used two permission types of ''read'' and ''write.''

New feature: PKCE

One of the major security improvements in the SMART v2 Guide is the requirement that all apps support the OAuth 2.0 security extension Proof Key for Code Exchange (PKCE). PKCE is designed to mitigate the known security vulnerability of authorization code interception attacks, with native apps especially targeted. According to IETF RFC 7636,[180] the request for comment which defines the PKCE extension, this attack can be used to illegitimately obtain an access token from the authorization server and thus obtain server data in an unauthorized manner. PKCE mitigates this vulnerability by creating cryptographically random keys for every authorization request. The authorization server performs proof of possession of the secret key by the client. This mitigates the vulnerability as an attacker who intercepts the authorization code cannot redeem it for an access token as they do not possess the secret key associated with the authorization request.

Support for PKCE is important because PKCE makes health app access

[179] *https://www.oauth.com/oauth2-servers/pkce/.*

[180] See IETF RFC 7636 at: *https://www.rfc-editor.org/rfc/rfc7636.*

of patient health information more secure in a standardized manner. ONC recognizes healthcare participants and patients are interested in the secure use of health apps, including native apps, to access health information. PKCE support makes the granting of access to health information via health apps more secure by mitigating the known vulnerability of authorization code interception attacks. We believe the support of PKCE would further our goal of secure access of health information without special effort by further securing health app access, especially for native apps. Therefore, we proposed to require the support of PKCE as specified in the SMART v2 Guide (88 FR 23817).

Comments. All comments received from interested parties supported adoption of the OAuth 2.0 security extension PKCE in the SMART v2 Guide. Many commenters noted that adoption and required support for PKCE is aligned with industry best practice and forthcoming updates to OAuth in draft version 2.1.

Response. We thank the commenters for their support. We believe the support of PKCE would further our goal of secure access of health information without special effort by further securing health app access, especially for native apps. Therefore, we have finalized adoption of the SMART v2 guide with inclusion of PKCE. This means that Health IT Modules presented for testing and certification to § 70.315(g)(10) must support PKCE.

New Feature: CRUDS scope syntax

Another major update in the SMART v2 Guide is the revision of the scope syntax to align with the FHIR REST API interactions for FHIR resources. Previously in the SMART v1 Guide, scope syntax for FHIR resources was delineated in terms of combinations of ''read'' and ''write'' permissions. The SMART v2 Guide revises this scope syntax by splitting ''read'' permissions into two types of permissions which correspond to FHIR REST API interactions, ''Read'' and ''Search.'' Similarly, the ''write'' permissions from the SMART v1 Guide are split into ''Create,'' ''Update,'' and ''Delete.'' This alignment of scope syntax to the FHIR REST API interactions permits Health IT Module authorization servers to provide greater specificity regarding which permissions are granted in scopes to apps and has the benefit of improved technical clarity to health IT and application developers. This additional specificity for scopes also improves a patient's control over how an app accesses their health data by clarifying for the patient what specific type of API interactions are permitted to the app. For example, under this new syntax the patient could specifically permit an app ''read'' access to a FHIR resource but deny ''search'' access for the same FHIR resource.

As stated in the ONC Cures Act Final Rule at 85 FR 25742, the § 170.315(g)(10) certification criterion only requires health IT developers to support ''read'' capabilities according to the standard and implementation specifications adopted in § 170.215(a) and in § 170.215(b)(1), including the mandatory capabilities described in ''US Core Server Capability Statement.'' Our proposal aligns with this existing policy for § 170.315(g)(10) by proposing to require that only ''Read'' and ''Search'' permissions as specified in the SMART v2 Guide be supported for certification to the § 170.315(g)(10) criterion.

Comments. Comments from health IT companies supported our proposals to adopt the SMART v2 revised scope syntax of ''Create,'' ''Read,'' ''Update,'' ''Delete,'' and ''Search,'' or CRUDS. They noted that the new syntax supports flexible and patient-friendly user interfaces (UI). One commenter noted that ONC should maintain current policy allowing developers the flexibility to present authorization scopes in a more user-friendly format, such as by logically grouping FHIR resource-level scopes, as long as users are able to grant FHIR resource-level scope authorizations, if requested. We also received a comment recommending against requiring support for wildcard scopes as defined in the SMART v2 Guide due to concerns about data management and security in patient access use cases.

Response. We thank the commenters for their support and comments. In consideration of the comments received, we have finalized as proposed the requirement for Health IT Modules certified to § 170.315(g)(10) to support the SMART v2 scope syntax for the ''Read'' and ''Search'' permissions as specified in the SMART v2 Guide. We clarify that Health IT Modules supporting the SMART v2 Guide scope syntax and the ''permission-patient'' capability from the SMART v2 Guide are not required to support wildcard scopes relating to authorization to receive a single patient's data. Instead, we align with the policy as mentioned in the ONC Cures Act Final Rule (85 FR 25741) that as part of supporting the ''permission-patient'' capability, Health IT Modules presented for testing and certification must include the ability for patients to authorize an application to receive their EHI based on FHIR resource-level scopes.

ii. SMART v2 Optional Features Proposed as Required by ONC

We proposed to require all Capabilities as defined in ''8.1.2 Capabilities'' and the ''Patient Access for Standalone Apps'' and ''Clinician Access for EHR Launch'' Capability Sets from ''8.1.1 Capability Sets'' (88 FR 23817 through 23819). First, the SMART v2 Guide introduces functionality specified as optional in the implementation guide. We proposed to make several of these optional functionalities required as part of the proposed implementation specification, and therefore required for certification criteria that reference proposed § 170.215(c)(2) (88 FR 23818).

Second, the SMART v2 Guide introduces an optional profile for authorization servers to support asymmetric client authentication for confidential clients. We proposed to require Health IT Modules support asymmetric client authentication as an option for confidential clients during the process of authentication and authorization when granting access to patient data.

Third, the SMART v2 Guide also introduces a new optional feature of granular scope constraints using search parameters. This feature uses the FHIR REST API search parameter syntax to specify permissions more granular than the FHIR resource level, which was the maximum granularity of scopes in the SMART v1 Guide. We proposed to require ''3.0.2.3 Finer-grained resource constraints using search parameters'' with the clarification that Health IT Modules certified to § 170.315(g)(10) must minimally be capable of handling finer-grained scopes using the ''category'' parameter for (1) the Condition resource with Condition sub-resources Encounter Diagnosis, Problem List, and Health Concern and (2) the Observation resource with Observation sub-resources Clinical Test, Laboratory, Social History, SDOH, Survey, and Vital Signs. We note that the requirements denoted in ''3.0.2.3 Finer-grained resource constraints using search parameters'' would be required as part of implementing the ''permission-v2'' capability defined in ''8.1.2 Capabilities''. We anticipated that the US Core IG would provide guidance for developers to support a minimum number of search parameters, and this minimum list would be consistent with the optional scopes described in section ''3.8 Future of US Core'' of the US Core IG v6.1.0.

Fourth, the SMART v2 Guide revises how capabilities are categorized. The ''SMART Core Capabilities'' in the

SMART v1 Guide define capabilities supported by the server and are made available to inform clients of supported functionality. ''Capabilities'' are grouped into ''Capability Sets'' to define the functionalities required for a specific use case. The SMART v2 Guide restructures how ''Capabilities'' are organized, and no longer includes ''SMART Core Capabilities.'' Instead, the SMART v2 Guide includes a list of ''Capabilities'' and ''Capability Sets.''

Finally, the SMART v2 Guide introduces a new requirement to support POST-based authorization for the client authorization request. This new requirement in the SMART v2 Guide is adapted from the OpenID Connect Core specification and is related to the requirement in § 170.315(g)(10)(v)(A)(*1*)(*i*), which requires a Health IT Module to support authentication and authorization during the process of granting access to patient data according to the SMART App Launch and OpenID Connect Core standards. The SMART v2 Guide includes the ''authorize-post'' capability under ''Capabilities'' for servers to indicate support for this requirement. To align with this new technical requirement in the SMART v2 Guide and the authorization and authentication requirement in § 170.315(g)(10)(v)(A)(*1*)(*i*), we proposed to require the ''authorize-post'' capability (88 FR 23819).

Comment. Overall, commenters were supportive of ONC's proposals to adopt optional features in the SMART v2 Guide as required for the Program. Several commenters supported adoption of all optional features; several others supported adoption of all optional features except for ''authorize-post'' capability (also referred to as HTTP POST by commenters); and a minority of commenters also commented against including the ''permission-online'' capability. There was a comment recommending revision to the language of the token introspection proposal in § &170.315(g)(10)(vii), since the SMART v1 Guide does not include a guidance section regarding token introspection. We also received a comment requesting clarity regarding requirements to independently support SMART v2 scopes separately from SMART v1 scopes.

Response. We thank the commenters for their support and comments. We believe requiring the proposed optional features will improve the capability of applications to be authorized by users to securely receive EHI. We clarify the ''authorize-post'' capability is not an optional capability and is required as per the SMART v2 Guide as a method to obtain an authorization code from the authorization server. To align with the requirement as per the implementation guide, we have finalized the proposal to require the ''authorize-post'' capability. We encourage interested parties to participate in the development of the SMART App Launch IG if there are enhancements or technological advances regarding this capability. We proposed to require the ''permission-online'' capability, as part of our proposal to require all ''Capabilities'' as defined in ''8.1.2 Capabilities,'' which would enable an application to receive authorization to receive EHI while the user is logged in. In consideration of comments we received, we believe additional clarity is necessary regarding the specific authorization contexts in which this capability would be required. Also, further insight is needed regarding the use cases in which this capability provides utility beyond the ''permission-offline'' capability included in the proposal. Therefore, we are modifying our proposal to exclude the ''permission-online'' capability from the requirements of § 170.215(c)(2). Thus, we have finalized our proposal to require all Capabilities as defined in ''8.1.2 Capabilities'' and the ''Patient Access for Standalone Apps'' and ''Clinician Access for EHR Launch'' Capability Sets from ''8.1.1 Capability Sets'' of the SMART v2 Guide, except for the ''permission-online'' capability. We also note that since we have finalized our proposal to expire use of the SMART v1 Guide as part of the Program on January 1, 2026, that after that date certification to § 170.315(g)(10) would effectively require that token introspection be supported as described in the SMART v2 Guide. Additionally, regarding independently supporting SMART v2 and SMART v1 scopes, we note that this proposal requires the ''permission-v1'' and ''permission-v2'' capabilities as defined in the SMART v2 Guide, which define how such scopes must be supported. We clarify that the SMART v2 Guide scopes must be supported independently of the SMART v1 Guide scopes as per the ''permission-v2'' capability in the SMART v2 Guide, and that the SMART v1 Guide scopes must be supported as per the ''permission-v1'' capability in the SMART v2 Guide. Support for scopes in this manner enables the updated SMART v2 Guide scope syntax to be used by applications while also maintaining backwards compatibility with the SMART v1 Guide scopes for legacy applications.

Comments. We received support from a majority of commenters that addressed ONC's proposals for support of the SMART v2 Guide's optional capability ''3.0.2.3 Finer-grained resource constraints using search parameters,'' including our proposal to use the ''category'' parameter for (1) the Condition resource with Condition sub-resources Encounter Diagnosis, Problem List, and Health Concern and (2) the Observation resource with Observation sub-resources Clinical Test, Laboratory, Social History, SDOH, Survey, and Vital Signs. Multiple commenters appreciated this degree of specificity and encouraged ONC to finalize this approach without further specifying in future rulemaking; instead, many of these commenters said ONC should rely on future versions of the US Core Implementation Guide to instruct further specification of other FHIR resource constraints. One health IT company recommended that we do not align scopes requirements to ''search operations,'' and instead adopt authorization scopes no more granular than the ''category'' level for FHIR resources such as Condition, Observation, Medication Request, and Diagnostic Report.

Response. We appreciate commenters' feedback and have finalized the requirements as proposed. We note that the finalized requirements regarding ''3.0.2.3 Finer-grained resource constraints using search parameters'' are required as part of implementing the ''permission-v2'' capability defined in ''8.1.2 Capabilities''. We also note that the requirements of this proposal to support finer-grained scopes using search parameter syntax and the ''category'' parameter are intended to align with capabilities and guidance as included in the SMART v2 Guide and FHIR US Core 6.1.0 implementation guide. We believe that establishing minimal conformance requirements at the category level for the Condition and Observation resources using specifications and guidance from these implementation guides will both ensure that Health IT Modules are capable of supporting the finer-grained resource constraints capability without being overly prescriptive in setting expectations for how the Health IT Module implements such capabilities.

Comments. Several commenters suggested that ONC adopt capabilities and standards that were outside the scope of our proposals, including ''rich authorization requests,'' ''push authorization requests, as defined by RFC 9126,'' and anti-malware capabilities, identity threat detection and response systems, the adoption of sender-constrained tokens, and OAuth 2.0 Demonstrating Proof-of-Possession

at the Application Layer (DPoP) specification.

Response. We thank the commenters for their recommendations, but we note that these comments are outside the scope of our proposals. We decline to accept the recommendations to adopt these capabilities, but we encourage industry to continue highlighting potential capabilities for future consideration in the Program. We also encourage interested parties to participate in the development and refinement of standards and implementation guides such as the SMART App Launch Implementation Guide.

8. Patient Demographics and Observations Certification Criterion in § 170.315(a)(5)

In the 2015 Edition Final Rule (80 FR 62601), ONC required the recording, capture, and access to a patient's sex, sexual orientation, and gender identity for Health IT Modules certified to the ''Demographics'' certification criterion (§ 170.315(a)(5)) (80 FR 62747). This rule also defined a required set of standardized terminology to represent each of these data elements (80 FR 62618–62620). Since then, ONC has received recommendations through the Health Information Technology Advisory Committee (HITAC) and public feedback that the current terms and terminologies used to represent sex, gender identity, and sexual orientation are limited and need to be updated.

Meanwhile, the healthcare industry had similarly taken note of the need for precision for ideas encompassed in terms such as ''sex'' and ''gender'' and launched the Gender Harmony Project [181] to capture these concepts consistently within healthcare. The Gender Harmony Project introduced for the health IT context the concepts ''Sex for Clinical Use'' (SFCU), ''Recorded Sex or Gender'' (RSG), ''Name to Use,'' and ''Pronouns.'' The Gender Harmony Project defines Sex for Clinical Use as a category that is based on clinical observations typically associated with the designation of male and female; Name to Use provides the name that should be used when addressing or referencing the patient; Recorded Sex or Gender is the documentation of a specific instance of sex and/or gender information; and Pronouns are determined by a patient and used when referring to the patient in speech, clinical notes, and in written instructions to caregivers (*e.g.,* she/her/hers or they/them). Sex for Clinical Use, Name to Use, Recorded Sex or Gender, and Pronouns are currently not present in the certification criteria.

We outline our proposals as discussed in the HTI–1 Proposed Rule to modify the ''Demographics'' certification criterion (§ 170.315(a)(5)) (88 FR 23820):

We proposed to rename § 170.315(a)(5) from ''demographics'' to ''patient demographics and observations,'' to acknowledge that the data elements being proposed are broader than demographics information, as we look to promote a more inclusive healthcare system.

We proposed to add the data elements ''Sex for Clinical Use'' in § 170.315(a)(5)(i)(F), ''Name to Use'' in § 170.315(a)(5)(i)(G), and ''Pronouns'' in § 170.315(a)(5)(i)(H) to the ''patient demographics and observations'' certification criterion (§ 170.315(a)(5)). This addition reflects concepts developed by the HL7 Gender Harmony Project and help promote inclusivity in care delivery.

We proposed to revise the terminology standards specified for ''Sex'' in § 170.315(a)(5)(i)(C). Prior to issuing the HTI–1 Proposed Rule, ONC received significant feedback reflecting the need to be more inclusive in the terminology representing the data element. As such, ONC proposed to revise the fixed list of terms for ''Sex'' in § 170.315(a)(5)(i)(C), which are represented by HL7® Value Sets for Administrative Gender and NullFlavor in § 170.207(n)(1). We proposed to ultimately replace § 170.207(n)(1) with the SNOMED CT® U.S. Edition code set proposed in § 170.207(n)(2). In order to be less disruptive to developers of certified health IT, we proposed to provide flexibility and allow recording the element using the specific codes represented in § 170.207(n)(1) for the time period up to and including December 31, 2025, to provide enough time to transition their health IT systems to SNOMED CT® U.S. Edition by January 1, 2026. By having § 170.207(n)(1) expire at the end of 2025 and adding § 170.207(n)(2) as a requirement for Health IT Modules certified to § 170.315(a)(5) beginning January 1, 2026, we proposed to enable health IT developers to specify any appropriate value from the SNOMED CT® U.S. Edition code set with the standard specified in § 170.207(n)(2). We proposed to require that Sex for Clinical Use must be coded in accordance with, at a minimum, the version of LOINC® codes specified in § 170.207(c)(1).

Additionally, we proposed to replace the terminology standards specified for Sexual Orientation in § 170.315(a)(5)(i)(D), and Gender Identity in § 170.315(a)(5)(i)I. ONC has received significant feedback reflecting the need to be more inclusive in the terminology representing each of these data elements. As such, ONC proposed to revise the fixed list of terms for Sexual Orientation in § 170.315(a)(5)(i)(D), and Gender Identity in § 170.315(a)(5)I(E), which are represented by SNOMED CT® U.S. Edition and HL7® Value Set for NullFlavor in § 170.207(o)(1) and (2), and ultimately replace it with the SNOMED CT® U.S. Edition code set specified in § 170.207(o)(3).

We further proposed to set an expiration date of January 1, 2026, for the adoption of the values sets referenced in § 170.207(o)(1) and (o)(2). This allows the use of either the value sets in § 170.207(o)(1) and (o)(2) or the standard proposed in § 170.207(o)(3) beginning on the effective date of a final rule and transitioning to allow only the use of the adopted standard in § 170.207(o)(3) after December 31, 2025. Consistent with our policies in sections III.A and III.C.11, developers of certified health IT with Health IT Modules certified to criteria that reference § 170.207(o)(1) or (o)(2) would have to update those Health IT Modules to § 170.207(o)(3) and provide them to customers by January 1, 2026.

We also proposed to add Sex for Clinical Use (SFCU) as a new data element in § 170.315(a)(5)(i)(F). SFCU is a category based upon clinical observations typically associated with the designation of male and female. It &ports context specificity, is derived from observable information, and is preferably directly linked to &e information this element summarizes. SFCU represents a patient's sex relevant to a specific clinical setting. This is valuable when providing care for a patient whose condition or treatment is dependent on their sex as determined by observing and evaluating, for example, a patient's hormonal values, organ inventory, genetic observations, or external genital morphology. SFCU may differ from a patient's sex as recorded on a birth certificate or driver's license. We further clarified, that while there may be multiple values of SFCU tied to different events, such as requesting a laboratory test or imaging study, we proposed to require health IT developer be able to record at least one value of SFCU. Additionally, in order to align with current industry practice and to provide flexibility to health IT developers, we proposed that health IT be capable of recording SFCU using the LOINC® terminology code set standard specified in proposed § 170.207(n)(3).

[181] *https://confluence.hl7.org/display/VOC/The+Gender+Harmony+Project.*

We proposed to add new data elements Name to Use in § 170.315(a)(5)(i)(G) and Pronouns in § 170.315(a)(5)(i)(H), respectively, to advance the culturally competent care for lesbian, gay, bisexual, transgender, queer, intersex, asexual, and all sexual and gender minority (LGBTQIA+) people. Multiple values for a given patient may be valid over time. We require at least one value for Pronouns and Name to Use be recorded. Additionally, in order to align with current industry practice and to provide flexibility to health IT developers, we proposed that health IT be capable of recording Pronouns using the LOINC® terminology code set standard specified in proposed § 170.207(o)(4).

In addition to the other data elements proposed, the HL7 Gender Harmony Project created an element named Recorded Sex or Gender (RSG). RSG documents a specific instance of sex and/or gender information. RSG is considered a complex data element that includes provision for a sex or gender value, as well as reference to the source document where the value was found, whereas Sex is a simple data element. RSG provides an opportunity for health IT developers to differentiate between sex or gender information that exists in a document or record, and from Sex for Clinical Use (SFCU) which is designed to be used for clinical decision-making. In the HTI–1 Proposed Rule, ONC asked commenters to evaluate two options and provide feedback regarding whether Recorded Sex or Gender as defined by the HL7 Gender Harmony Project should be incorporated into 170.315('')(5) ''patient demographics and observations'' (88 FR 23820).

Comments. Some commenters did not support the proposed deadline and instead suggested a deadline of 24 months after the effective date of the final rule as this would be in line with the proposed ''timeliness'' provisions of the Assurances Condition and Maintenance of Certification requirements. Other commenters specifically proposed December 31, 2025, for the adoption of new and updated certification criteria.

Response. We thank the commenters for the comments suggesting an extension to the proposed effective dates. In assessing the overall burden and proposed timeframes, we have revised the compliance dates to allow for 24 months for compliance and finalized the adoption of § 170.315(a)(5) with a compliance date of January 1, 2026. We have also revised the ''timeliness'' requirement in the Assurances Condition to avoid confusion.

Comments. Most commenters supported the addition of Sex for Clinical Use, Name to Use, Sex, and Pronouns to § 170.315(a)(5) ''patient demographics and observations.'' Some commenters noted that comprehensive demographic data supports holistic understanding of patients' background, leading to culturally competent and patient-centered care. Commenters also encouraged ONC to continue collaborating with the HL7 Gender Harmony Project to provide more detail regarding the definitions and supporting terminologies—supporting the ability for people to provide more nuanced information about themselves to best inform care. Commenters also suggested that ONC explore how Sex for Clinical Use could be expanded to incorporate organ inventory and hormone levels. One commenter suggested that ONC promote Sex for Clinical Use as a repeatable set of observations. Another commenter suggested that the addition of Pronouns, Name to Use, and Sex for Clinical Use would create unnecessary confusion, increased medical risk, and religious conscience concerns. Other commenters expressed concern that it will be difficult to collect Sex for Clinical Use as the clinician interacting with the patient may not have the information necessary to provide a value. Some commenters expressed concern about the complexities of dealing with context-specific Sex for Clinical Use data.

Some commenters expressed concern that there is not sufficient information or guidance for programs and health IT to implement Sex for Clinical Use, therefore it should not be included in § 170.315(a)(5) ''patient demographics and observations.'' Several commenters suggested that ONC wait to add any data elements to ''patient demographics and observations'' until the data elements are part of USCDI. Other commenters supported the addition of Sex for Clinical Use, Name to Use and Pronouns to the ''patient demographics and observations'' criterion rather than USCDI, as adding to USCDI and then SVAP would greatly slow adoption since SVAP is optional.

Response. ONC thanks the commenters expressing support for Name to Use, Pronouns, and Sex for Clinical Use. Including ''patient demographics and observations'' criterion in this final rule provides time for Health IT Modules to incorporate support for capture of this important data prior to requiring exchange.

ONC collaborates closely with the HL7 Gender Harmony project team and as a result has finalized the descriptive data name change of ''Sex for Clinical Use'' to ''Sex Parameter for Clinical Use'' in § 170.315(a)(5)(i)(F). ONC will continue to support efforts to expand the scope of the HL7 Gender Harmony Project to explore how more specific information about a person's physical characteristics (*e.g.,* organ inventory and hormone levels) can be collected and exchanged to inform Sex Parameter for Clinical Use. We have finalized as proposed (88 FR 23820) that the Health IT Module must be able to record at least one value for Sex Parameter for Clinical Use for each patient and note that there may also be multiple values tied to different events, such as requesting a laboratory test or imaging study, allowing for and encouraging more than one. We recognize that the Sex Parameter for Clinical Use data element may be a new concept to some. However, we note that developers of certified health IT have the flexibility to configure their user interface and to capture and display these data in clinical workflows consistent with their own design decisions.

ONC appreciates the concerns expressed by some commenters about lack of guidance to implement Sex Parameter for Clinical Use (formerly Sex for Clinical Use); however, at the time of this final rule, HL7 has published updated specifications that provide specific exchange guidance that may then inform incorporation into health IT workflows. ONC has identified Sex Parameter for Clinical Use, Name to Use, and Pronouns as key to implementing ONC's priorities to support health equity and access for LGBTQIA+ communities. We have also finalized what was proposed to specify that at least one Name to Use and Pronouns must be recorded for each patient.

With regards to the comment suggesting that collection of these data elements would create unnecessary confusion, increased medical risk, and religious conscience concerns, ONC believes that these data elements are critical to supporting healthcare, health equity, and access for LGBTQIA+ communities. Our adoption of these data elements will help to advance the capability of certified health IT to exchange these data elements for use by patients and health care providers. Our adoption of these data elements does not establish a requirement for health care providers or patients to record or disclose this information, or use these capabilities. As stated above, these data elements may be new concepts to some, and ONC encourages developers of certified health IT to work with providers to develop appropriate workflows.

The ''patient demographics and observations'' criterion focuses on data capture and storage and not the exchange of this data, which is the focus of USCDI. Therefore, we did not accept the comment suggesting that ONC not include the data elements in § 170.315(a)(5) ''patient demographics and observations'' until they are included USCDI.

Comments. Commenters suggested that ONC remove Sex and retain Sex for Clinical Use because Sex for Clinical Use paired with Gender Identity provides clear information to distinguish between a clinical categorization of a person's sex used for clinical decision making and a person's self-reported Gender Identity.

Response. ONC thanks commenters for their input suggesting that Sex be removed and Sex Parameter for Clinical Use (as we have renamed Sex for Clinical Use) be retained. However, more analysis by the health IT community is necessary to determine the impact of removing Sex. Therefore, ONC declines to remove Sex.

Comments. Some commenters did not support changing the title from patient demographics to patient demographics and observations, noting that all data described within are considered demographics. Other commenters noted that the title change is confusing as the criterion now includes statistical characteristics of human populations used to identify population segments and attributes associated with a diagnostic test or procedure.

Response. We disagree with the stated concerns and do not believe that the certification criterion name change will be confusing to most in the healthcare ecosystem. The addition of the word ''observations'' signals that some of the data elements in this data class may not be statistical characteristics of human populations by all people evaluating the certification criterion. Accordingly, we have finalized the criterion title change as proposed.

Comments. Multiple commenters expressed concern about changing the requirement for specific code set concepts for Sexual Orientation and Gender Identity to a more general reference to SNOMED CT U.S. Edition. They also questioned whether health IT developers would be compliant if other values are exchanged such as ''unknown'' or ''asked but did not answer.'' Other commenters supported ONC's plans to move value set definitions out of regulatory text and delegate to industry groups. One commenter suggested referencing specific value sets defined in the Value Set Authority Center.

Response. ONC thanks the commenters for their input and assures them that ONC collaborates with health IT developers to develop specific values that may be exchanged, including those that indicate a standard value is not available, such as ''unknown'' or ''asked but did not answer''. The resulting value sets may be defined in the Value Set Authority Center. Removing specific code set concepts from regulation allows health IT developers to provide options that are culturally relevant and may change on a cycle that is different from regulation.

Comments. Some commenters did not support the addition of Sex with the requirement that data values be drawn from SNOMED CT U.S. Edition. Others expressed concern that the addition of Sex may increase confusion among senders and receivers about the various data elements currently in use—administrative sex, administrative gender, and sex (assigned at birth).

Response. ONC thanks the commenters for their input regarding Sex. Health IT Modules may continue to record and exchange Sex (assigned at birth). Historically, Sex (assigned at birth), administrative sex, and administrative gender have been used to communicate sex which may be used for clinical decision making when the values were obtained from a document at some point in a patient's life or were not based on clinical observations and should not be used for clinical decision making. The addition of Sex allows health IT developers to exchange Sex without relying on document context.

Comments. Some commenters suggested that ONC remove the ''patient demographics and observations'' criterion entirely and rely on USCDI to promote the capture, use, and exchange of patient demographic data elements. Others suggested that all data elements listed in the ''patient demographics and observations'' criterion should be in USCDI prior to inclusion in regulation. These commenters referenced cases where ONC withdrew certification criteria (*e.g.,* Problem List, Medication List, Smoking Status).

Response. ONC thanks the commenters and acknowledges that certification criteria have been withdrawn in the past. ONC declines to remove the ''patient demographics and observations'' criterion or change the scope of USCDI to include data capture and use.

The ''patient demographics and observations'' certification criterion includes important data elements supporting underserved communities and health equity. The USCDI scope is focused on the exchange of data element values, whereas this certification criterion focuses on health IT capabilities to collect and record certain data. In some cases, the data required to be collected and recorded is not yet in USCDI.

Comments. In the HTI–1 Proposed Rule, proposals for § 170.315(a)(5), ONC asked commenters to provide feedback regarding whether Recorded Sex or Gender as defined by the Gender Harmony Project should be incorporated into the § 170.315(a)(5) ''patient demographics and observations'' criterion. Responses indicate there is not agreement among interested parties, and many open issues remain related to how and when these data should be collected. One commenter suggested that ONC remove the Sex data element entirely and add Recorded Sex or Gender to delineate administrative information from Sex for Clinical Use, which is to be used when making clinical decisions.

Response. ONC thanks commenters for their thoughtful input and will not finalize the addition of Recorded Sex or Gender to § 170.315(a)(5) due to lack of community consensus. ONC will continue to support maturation of this data element through the Gender Harmony Project at HL7.

Comments. Some commenters encouraged ONC to work with interested parties to provide clarity on the differences between related data elements to ensure patients' identities are respected while important information for clinical care is captured correctly. Specifically, sharing this information via a patient access API, such as those required by the CMS quality programs for health care providers under Medicare, may cause confusion or distress to a patient. Commenters also noted that care must be taken to ensure privacy controls are in place to protect sensitive, granular health data. This information may be sold or disclosed by an application developer if agreed to in the consumer terms and agreement.

Response. We thank the commenters for their comments regarding privacy concerns and recognize the importance of addressing the privacy and confidentiality of sensitive information. Recognizing this, the Program establishes the standards, implementation specifications, and functional requirements for health IT to manage and exchange data but does not control the collection or use of data. For more on patient requested restrictions on sharing of their health information, we refer readers to section III.C.10 on modifications to the ''view, download, and transmit to 3rd party'' certification

criterion in § 170.315(e)(1), which addresses patients' (and their authorized representatives') ability to use an internet-based method to request a restriction to be applied for any data expressed in the standards in § 170.213.

Base EHR Definition

We proposed to revise and update the ''demographics'' certification criterion (§ 170.315(a)(5)), to rename as ''patient demographics and observations,'' and which is included in the Base EHR definition in § 170.102 (88 FR 23821). This means Health IT Modules would need to be updated to accommodate the additional requirements in the ''patient demographics and observations'' certification criterion in order to meet the Base EHR definition. We did not receive comments related to updating the Base EHR definition to include the additional requirements in the ''patient demographics and observations'' certification criterion, so we have finalized this revision as proposed.

In addition, because December 31, 2022 has passed, we proposed to revise the Base EHR definition by removing the reference to § 170.315(g)(8) in § 170.102 Base EHR Definition (3)(ii) and replacing the references to § 170.315(g)(10) in § 170.102 Base EHR Definition (3)(ii) and (iii) with a single reference to § 170.315(g)(10) in § 170.102 Base EHR Definition (3)(i). We did not receive comments on this proposal, so we have finalized this revision as proposed.

9. Updates to Transitions of Care Certification Criterion in § 170.315(b)(1)

We proposed to replace the fixed value set for the USCDI data element ''Sex'' and instead enable health IT developers to specify any appropriate value from the SNOMED CT U.S. Edition code set with the standard specified in § 170.207(n)(2) (88 FR 23821). We proposed that health IT developers can continue using the specific codes for Sex represented in § 170.207(n)(1) for the time period up to and including December 31, 2025. We note that these dates were proposed for the adoption of the associated standards in § 170.207(n), including the expiration of the adoption of the standard in § 170.207(n)(1) on January 1, 2026. As discussed in sections III.A and III.C.11, developers of certified health IT with Health IT Modules certified to criteria that reference § 170.207(n)(1) would have to update those Health IT Modules to § 170.207(n)(2) and provide them to customers by January 1, 2026. We note that, in the proposed rule regulation text in § 170.315(b)(1)(iii)(G)(*3*), we inadvertently included a reference to § 170.213 (88 FR 23909) instead of including § 170.207(n)(2) as discussed in our proposal (88 FR 23821). ONC has not finalized § 170.213 as proposed in § 170.315(b)(1)(iii)(G)(*3*), as § 170.213 references a version of SNOMED CT U.S. Edition that is older than the one referenced in § 170.207(n)(2). We have finalized the reference to § 170.207(n)(2) in § 170.315(b)(1)(iii)(G)(*3*) to include the most recent version of SNOMED CT U.S. Edition available at the time of publication of this final rule. Health IT developers may update to a newer version if one exists at effective date of the criterion.

We also proposed a conforming update to § 170.315(b)(1) to update the listed minimum standard code sets for Problems in § 170.315(b)(1)(iii)(B)(*2*) (88 FR 23821). We proposed that Health IT Modules certified to § 170.315(b)(1) use, at a minimum, the version of the standard specified in § 170.207(a)(1).

Comments. All commenters agreed with the proposal to update the transitions of care certification criterion § 170.315(b)(1)(iii)(G)(*3*) to include the adoption of USCDI v3 in § 170.213(b). Some commenters noted that the updated criterion will allow better inpatient—outpatient transitions, especially for community health centers.

Response. ONC thanks commenters for their support to update the transitions of care certification criterion to include the adoption of USCDI v3. We have finalized the adoption of this proposal in this final rule.

Comments. One commenter encouraged ONC to work across HHS to enforce existing CMS and ONC requirements across products and healthcare organizations. The commenter suggests that HHS should extend transition of care data elements for claims data from payers to healthcare organizations offering primary care.

Response. ONC thanks the commenter for their input. ONC will continue to work with federal partners to promote alignment for these data concepts.

Comments. Some commenters suggested that the date to support USCDI v3 in Transitions of Care documents should be changed to December 31, 2025, or 24 months after the rule is finalized to allow health IT developers time to incorporate and test USCDI v3 data elements into Health IT Modules and develop appropriate safeguards for sensitive personal health information.

Response. ONC appreciates concerns expressed about the proposed date to allow for USCDI v3 adoption prior to including USCDI v3 data elements in transition of care documents. We have finalized the adoption of updates to § 170.315(b)(1) with a compliance date of January 1, 2026.

Comments. Some commenters expressed concern about USCDI data element Sex and its inclusion in patient matching algorithms, suggesting that time of birth is a better matching parameter than Sex. Other commenters suggested that mother's maiden name (in a child's record), birth order, and multiple birth indicators be added to the patient matching requirement.

Response. ONC thanks commenters for their input concerning appropriate data to include in patient matching algorithms. The transitions of care criterion define the minimum set of data elements to use for patient matching and does not inhibit health IT developers from using other additional data elements.

10. Patient Right To Request a Restriction on Use or Disclosure

In the HTI–1 Proposed Rule, we noted that under the HIPAA Privacy Rule, covered entities, as defined in 45 CFR 160.103, are required to allow individuals to request a restriction on the use or disclosure of their PHI for treatment, payment, or health care operations, although it does not require covered entities to accept such requests, except in certain limited circumstances (See 45 CFR 164.522(a)(1)) and 164.530(i)) (88 FR 23821). The HIPAA Privacy Rule also requires covered entities to implement policies and procedures with respect to PHI that are designed to comply with the standards, implementation specifications, or other requirements of the HIPAA Privacy Rule, including the individual right to request restrictions (See 45 CFR 164.530(i)(1)). We stated that we believe that certified health IT should support covered entities so they can execute these processes to protect individuals' privacy and to provide patients an opportunity to exercise this right to the extent feasible. However, we also noted that patient-directed privacy of data the patient deems sensitive requires attention to specific technology and policy challenges, which we recognize are not easily solved (88 FR 23821).

We proposed a new certification criterion in § 170.315(d)(14), an addition to ONC's Privacy and Security Framework under the Program in § 170.550(h), and a revision to an existing ''view, download, and transmit to 3rd party'' certification criterion in § 170.315(e)(1) to support additional tools for implementing patient requested privacy restrictions (88 FR 23822 through 23824).

We proposed to adopt a new certification criterion ''patient requested restrictions'' in § 170.315(d)(14) to enable a user to implement a process to restrict uses or disclosures of data in response to a patient request when such restriction is agreed to by the covered entity (88 FR 23822). This criterion was proposed specifically in support of the HIPAA Privacy Rule's individual right to request restriction of certain uses and disclosures (See also 45 CFR 164.522(a)). We proposed that this new criterion in § 170.315(d)(14) would be standards-agnostic, allowing health IT developers seeking to certify a Health IT Module to the criterion flexibility in how they design these capabilities as long as they meet the functional requirements described for certification. We specifically intended the proposed § 170.315(d)(14) to advance the technological means to support clinicians and other covered entities when honoring patient requests for the restriction of uses or disclosure of PHI through certified health IT.

We proposed to add the following in § 170.315(d)(14) for this new criterion ''patient requested restrictions'':

- For any data expressed in the standards in § 170.213, enable a user to flag whether such data needs to be restricted from being subsequently used or disclosed; as set forth in 45 CFR 164.522; and
- prevent any data flagged pursuant to paragraph (d)(14)(i) of this section from being included in a subsequent use or disclosure for the restricted purpose.

We proposed that ''enabl[ing] a user to flag'' means enabling the user of the Health IT Module to indicate that a request for restriction was made by the patient and that the user intends to honor the request. We noted that in the case of integration with a Health IT Module certified to the revised criterion in § 170.315(e)(1), that request made by the patient could be in part automated for requests made through an internet-based method. However, the functionality under the proposed new criterion in § 170.315(d)(14) would include the ability for the user to indicate a request made via other means. We noted that such ''flags'' may leverage use of security labels like those included in the HL7 data segmentation for privacy (DS4P) implementation guides discussed in section III.C.10.b of the HTI–1 Proposed Rule, or other data standards such as provenance or digital signature specifications.[182] We also noted that the use of such standards or specifications would be at the discretion of the health IT developer, and they would have the flexibility to implement the ''enable a user to flag'' functionality in the manner that works best for their users and systems integration expectations.

We proposed that the developer of a certified Health IT Module, under the proposed standards-agnostic approach, would have the flexibility to implement the restriction on the inclusion in a subsequent use or disclosure via a wide range of potential means dependent on their specific development and implementation constraints (*e.g.,* flagged data would not be included as part of a summary care record, not be displayed in a patient portal, or not be shared via an API). We proposed and sought comment on several alternatives which would add standards to the proposed new criterion and would specifically leverage HL7 dS4P IGs for the new criterion in § 170.315(d)(14). We also proposed and sought comment on alternate proposals that looked exclusively at the HL7 Privacy and Security Healthcare Classification System (HCS) Security Label Vocabulary within the HL7 dS4P IGs for a source taxonomy for the ''flag'' applied to the data (88 FR 23822).

We also proposed to modify the Privacy and Security Framework in § 170.550(h) to add the proposed new criterion. Specifically, we proposed to modify § 170.550(h)(iii) in reference to the certain of ''care coordination'' certification criteria in § 170.315(b); § 170.550(h)(v) in reference to the ''view, download, and transmit to 3rd party'' certification criterion in § 170.315(e)(1); and to § 170.550(h)(viii) in reference to the § ''application access'' certification criteria at § 170.315(g)(7) through (g)(9) and the ''standardized API for patient and population services'' certification criterion at § 170.315(g)(10).

We proposed that the new ''patient requested restrictions'' certification criterion in § 170.315(d)(14) would be required for the Privacy and Security Framework by January 1, 2026.

We also proposed a modification to the ''view, download, and transmit to 3rd party'' certification criterion in § 170.315(e)(1) to support patients' ability to leverage technology to exercise their right to request restrictions of uses and disclosures under the HIPAA Privacy Rule. We proposed that a Health IT Module certified to the criterion in § 170.315(e)(1) must also enable an internet-based approach for patients to request a restriction of use or disclosure of their EHI for any data expressed in the USCDI standards in § 170.213. Specifically, we proposed to modify § 170.315(e)(1) to add a paragraph (iii) stating patients (and their authorized representatives) must be able to use an internet-based method to request a restriction to be applied for any data expressed in the standards in § 170.213.

We proposed that conformance with this update to the ''view, download, and transmit to 3rd party'' certification criterion in § 170.315(e)(1)(iii) would be required by January 1, 2026, for Health IT Modules certified to § 170.315(e)(1). Consistent with our proposals in sections III.A and III.C.11 of the HTI–1 Proposed Rule, developers of certified health IT with Health IT Modules certified to § 170.315(e)(1) would have to update those Health IT Modules to § 170.315(e)(1)(iii) and provide them to customers by January 1, 2026.

We did not propose any changes to the current certification criteria for ''security–tags—summary of–care—send'' and ''security–tags—summary of care—receive'' in § 170.315(b)(7) and § 170.315(b)(8) respectively; however, we noted that the inclusion of the proposed new certification criterion in § 170.315(d)(14) into the Privacy and Security Framework in § 170.550(h) would mean that the proposed new certification criterion would be applicable for Health IT Modules certified to the ''security tags—send'' and ''security tags—receive'' certification criteria as well (88 FR 23822–23823). We sought comment on whether those certification criteria should also be directly modified in alignment with the proposals described in this section (88 FR 23823).

We sought comment on the capabilities we have proposed for the new criterion in relation to the HIPAA Privacy Rule individual right to request restriction of uses and disclosures of PHI. We specifically sought comment on whether the proposed new criterion should include additional functions to better support compliance with the HIPAA Privacy Rule individual right to request restriction of uses and disclosures of PHI. We also sought comment on whether the proposed new criterion should, for example, include capabilities to support HIPAA Privacy Rule provisions for emergency disclosures in § 164.522(a)(1)(iii) and (iv) or termination of a restriction under § 164.522(a)(2).

[182] For example, the USCDI v3 includes a provenance data class (*https://www.healthit.gov/isa/uscdi-data-class/provenance#uscdi-v3*) and submissions in ISA include digital signature as a potential addition to provenance within the USCDI: *https://www.healthit.gov/isa/uscdi-data/signature.* Further specifications for provenance data and digital signatures in the context of FHIR-based transactions are also referenced in ISA: *https://www.healthit.gov/isa/representing-data-provenance.*

We sought public comment on each part of this proposal—the new criterion in § 170.315(d)(14), the inclusion of the request capability for patients in § 170.315(e)(1), and the requirements with the Privacy and Security Framework in § 170.550(h)—both separately and as a whole. We specifically sought comment on the feasibility of each part in terms of technical implementation and usefulness for patients and covered entities using these capabilities. We sought comment on the health IT development burden associated with implementation of the capabilities including for the individual certification criterion referenced in the Privacy and Security Framework in § 170.550(h).

In addition, we sought comment on any unintended consequences that the new criterion in § 170.315(d)(14) or the addition to the Privacy and Security Framework in § 170.550(h) might place on patients, clinicians, or other covered entities using certified health IT. We sought comment on whether, and by how much, the use of this criterion as part of broader privacy workflows might represent a reduction in manual effort for covered entities, a positive impact on uptake by patients, or other benefits such as supporting documentation of restrictions as required under the HIPAA Privacy Rule in § 164.522(a)(3).

Finally, we sought comment on methods by which we might quantify the development burden and costs as well as the potential benefits or future cost savings for the new criterion in § 170.315(d)(14), the new functionality in the existing criterion in § 170.315(e)(1), and the addition to the Privacy and Security Framework in § 170.550(h).

Comments. Overall, in response to our new proposal for Patient Requested Restrictions Criterion in § 170.315(d)(14), we received mixed input for our proposals and our alternative proposals from interested parties. Comments ranged from full support to limited support expressing various technical and policy considerations all the way to full opposition because of technical, policy, and patient care concerns. Multiple commenters expressed support for the intent behind the proposal, noting its potential to empower patients to take ownership of their data, while ensuring that providers are not engaging in information blocking for automated data flows and expressed support for the development and implementation of data segmentation technology. Multiple commenters supported giving patients a reasonable opportunity and the technical capability to make informed decisions about the collection, use, and disclosure of their EHI, noting that the functionality is increasingly necessary for ensuring patient trust.

However, in most instances where support was indicated, it was conditional. In these instances, commenters indicated concern with the implementation of the proposal, noting that if ONC were to finalize the proposal then it should be mindful of numerous considerations and challenges. Concerns ranged across many broad policy and technical topics including but not limited to implementation feasibility, unintended consequences such as impacts on patient safety and provider burden, implementation timeline and approach, importance of patient education, and intersections with existing information blocking policy as well as the Trusted Exchange Framework and Common Agreement (TEFCA).

Multiple commenters questioned the readiness of real-world tested, national standards and specifications for this proposal. One commenter suggested that developers should be given flexibility in implementing the criterion, given the breadth of activities, workflows and features in which patient data is used. Some suggested that adopting a standards-agnostic approach will allow health IT developers to determine appropriate implementation in their own systems and could lead to the future development of new, consensus-based standards informed by robust real-world implementation experience across a broad set of developers and health care provider organizations. However, multiple commenters recommended the criterion be standards-based, as based on past examples, a standards-agnostic approach would likely not successfully lead the private sector to come to consensus on their own. Some commenters indicated support for HL7 FHIR DS4P IG but felt it was not clear that it has been adequately tested and deployed in the field. Such commenters stated that ONC should move forward with support for implementations and test them before deploying as a requirement. One commenter indicated ONC should instead look at FHIR for future rulemaking. Multiple commenters recommended that we focus on establishing, with the relevant Standards Development Organizations (SDOs) as well as other relevant groups, a common infrastructure that enables patients to only document their consent rules once, while having a common definition of all relevant privacy rules across US jurisdictions. Multiple commenters recommended federally funded connectathons and other policy-driven approaches to stimulate the developer community to implement toward a particular use case with the purpose of advancing standards development.

We also received comments indicating strong opposition to the new proposal for patient requested restrictions criterion in § 170.315(d)(14). Commenters opposing the proposal shared a similar sentiment to those supporting the proposal provided certain conditions were met. These commenters stated that it is not feasible for developers to support every permutation on the use of data that a patient might request and that the proposed criterion may not provide enough control to help patients manage the complexities of their information. Commenters highlighted the complexity of managing and scaling a consent management infrastructure, especially across all the data sources where the patient's data is available. Others noted this proposal runs a high risk of allowing for a wide variety of misaligned implementation, and some felt it would increase burden and undermine benefits of interoperability.

Multiple commenters suggested that, if adopted, the new proposed criterion in § 170.315(d)(14) should be optional and that adoption of the criterion within the privacy and security framework in § 170.550(h) should not be required before CY 2030. Commenters noted that significant work would be required by health IT developers, including reconfiguration of existing EHR systems as well as other interconnected systems related to treatment, payment and operations and that ONC should allow for a 3-year implementation cycle, 2 years to develop, test and certify, and at least 1 year to roll-out the proposed criterion to customers and update workflows. In response to our request for comment related to the development burden (88 FR 23823), commenters estimated up to one-million hours for preliminary development and rollout, plus additional ongoing maintenance requirements.

We received several comments regarding how to achieve policy goals through alternative approaches and factors that should be taken into consideration—including several that are out of scope of ONC authorities, but informative of the need for alignment to related privacy laws. Several commenters stated ONC should better align with other regulators and have more explicit workflows on privacy and patient consent before adopting this proposed certification criterion in § 170.315(d)(14). One commenter also

suggested that this criterion's functionality support providers implementing information sharing practices in compliance with potential future policies to protect sensitive health information regarding ''highly politicized lawful health care services.'' Multiple commenters recommended introducing a functional requirement aligning with the HIPAA right to request corrections and amendments to erroneous information to ensure patients have an easy path to requesting corrections or amendments to their PHI through patient portals and APIs. They also felt that this would drive participation in standardization efforts through independent patient-led governance bodies. One commenter suggested that this work be funded and supported by the institutions sharing the data and driving these exchanges, and the commenter encouraged use of established patient-created resources to evaluate fairness of engagement with patient communities. Several commenters focused on our proposals in relation to other related regulations. These commenters indicated that ONC should work with other agencies to focus on ensuring there are streamlined and complementary privacy regulations. They additionally commented that any new privacy related regulation gets compared and cross referenced across existing and pending ones to support policy alignment.

Response. We thank the commenters for their thoughtful input addressing both the entirety of the proposals and specific areas of concern. As noted in the HTI–1 Proposed Rule (see, for example, 88 FR 23821), we proposed requirements for Health IT Modules certified under the Program to support workflows and specifications that would enable an individual to exercise their right to request restriction of uses and disclosures under the HIPAA Privacy Rule. We expressed our concerns about feasibility, timelines, and the overall complexity of the workflows and the related capabilities associated with this right as well as our intent to propose several options for consideration by the healthcare and health IT communities. Based on the mixed input we received on the proposed new criterion in § 170.315(d)(14) and the inclusion of the criterion in the privacy and security framework in § 170.550(h), and the strong concerns regarding its implementation feasibility by interested parties opposing these proposals, we have concluded that we should not finalize the proposals at this time. Our decision to not finalize the criterion in § 170.315(d)(14) is informed by the range of comments expressing concern with successfully implementing the proposal. In particular, there was no clear consensus on whether and how to proceed either with immature and untested standards or without the required use of specific standards for the certification criterion at § 170.315(d)(14). We agree with the concerns on the high risk of allowing Health IT Modules to implement a wide variety of misaligned standards and implementation specifications, as well as increased burden on developers of certified health IT, care providers, health information exchange networks, and a high probability of confusion for patients.

We note that those supporting our proposals for § 170.315(d)(14) did so to varying degrees, often extending conditional support while raising the same broad technical and policy considerations and concerns as those opposed to the proposal. Outright support on § 170.315(d)(14) as proposed, or for the various alternate proposals, was not as common as conditional support or opposition. The specific suggestions for such conditional support were varied and would introduce substantial additional detailed specification well beyond the scope of our proposal and the standards in the alternate proposals. Based on this input, there is no clear and consistent approach at this time to effectively address all commenter concerns. Therefore, we have not finalized the specific proposal to adopt a new certification criterion in § 170.315(d)(14). We also have not finalized corresponding modifications related to this proposed criterion's in ONC's Privacy and Security Framework in § 170.550(h). We will continue to encourage and engage with industry and standards development community efforts to advance standards supporting privacy workflows and to monitor the continued evolution of the HL7 DS4P IGs to consider new criteria in future rulemaking.

In consideration of those commenters who articulated full support, we recognize the importance of empowering patients to take ownership of their data and continue to support efforts to develop the technical capability for patients to leverage certified health IT to take affirmative action regarding the collection, use, and disclosure of their EHI. We note that we have maintained the existing criteria in § 170.315(b)(7) and § 170.315(b)(8) which support the application and persistence of security labels for document-based exchange and reference the standards adopted in § 170.205(o)(1), the HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1 (HL7 CDA DS4P IG) incorporated by reference in § 170.299. These two criteria require a Health IT Module to (1) enable a user to create a summary record that is tagged as restricted and subject to restrictions on re-disclosure and (2) enable a user to receive a summary record that is tagged as restricted and subject to restrictions on re-disclosure and to preserve privacy markings. The use of Health IT Modules certified to these two criteria can support privacy and security labels based on consent and with respect to sharing and re-disclosure restrictions. As noted, these existing criteria utilize the HL7 CDA DS4P IG, and include the use of the taxonomy of reference (HCS Security Label Vocabulary) for the purposes of applying and identifying standardized security labels on health information at the document, segment, or data element level. These existing certification criteria can be leveraged during transitions of care and sending/receiving summary of care records (*i.e.,* combined with Health IT Modules certified to § 170.315(b)(1)) and we encourage purchasers of certified health IT to explore the use and incorporation of these capabilities in their Health IT Modules.

We recognize the concerns of both commenters supporting the application of standards and those identifying a lack of readiness and gaps in the standards for the disposition of a disclosure request based on our proposed new criterion. We also recognize those commenters who advised a longer implementation timeline to refine and test standards. While we considered delaying the implementation of our proposal to 2030, or beyond, we believe that Health IT Modules certified to § 170.315(b)(7) and (b)(8) that use the HL7 CDA DS4P IG may serve as a balanced approach to address these disparate concerns by applying the standard where feasible, while allowing broad flexibility for health IT developers to implement functionalities where the standard is silent on core processes. We will continue to monitor uptake of the existing certification criteria at § 170.315(b)(7) and § 170.315(b)(8), as well as continue to work with the healthcare, health IT, and standards community to advance and evaluate the readiness and potential adoption in future rulemaking of the related HL7 FHIR DS4P IG, which is intended to support the same security label taxonomy (HCS Security Label Vocabulary) for health information

exchange via standards-based APIs using the FHIR standard.

Comments. We received many comments in relation to our proposal to update the existing ''view, download, and transmit to 3rd party'' certification criterion in § 170.315(e)(1), to add § 170.315(e)(1)(iii) to support additional tools for implementing patient requested privacy restrictions (88 FR 23822 through 23824) through the inclusion of an ''internet-based'' method for patients to request a restriction. Commenters were overwhelmingly supportive of the proposal to provide a means for patients to make a restriction request via Health IT Module. However, commenters expressed a wide range of related concerns ranging from the documentation of the request to potential consequences to consider when processing a patient's requests for restriction.

One commenter expressed concern that the HIPAA Privacy Rule does not (with certain exceptions) require a covered entity to restrict disclosure of an individual's PHI if so requested. Instead, the covered entity is required to have a process for approving or denying the request, and that decision is not under the individual's control. One commenter recommended that the certification criterion respect the individual's request for privacy regardless of the covered entity's perspective. However, another commenter noted that requiring the covered entity's approval ensures that important health information is still available when medically necessary while balancing patient privacy and security concerns. One commenter stated that clinicians may have a better understanding than individuals regarding which health data is relevant for their care. Commenters also expressed concern regarding an obligation to accept an individual's request for restriction. One commenter questioned how the lack of restriction on timelines for the request—such as the lookback period for the data or the length of time for which the restriction would be applicable—could impact the clinician's ability to make a reasoned judgment. Another commenter expressed a number of legal concerns relating to concerns that clinicians may have to defend refusals to comply with a patient's request for restriction, or that compliance with the patient's request which could place them in legal jeopardy for fraud, professional misconduct, or criminal charges.

Response. We thank the commenters for their input and support of our proposal to include an internet-based method for an individual to request restriction of uses and disclosures consistent with their right under the HIPAA Privacy Rule. We have finalized this proposed revision to the existing ''view, download, and transmit to 3rd party'' certification criterion in § 170.315(e)(1) to support additional tools for implementing patient requested privacy restrictions (88 FR 23822 through 23824) through the inclusion of an ''internet-based'' method for patients to request restriction. Specifically, we have finalized in § 170.315(e)(1)(iii) a requirement that Health IT Modules support patients (and their authorized representatives) to use an internet-based method to request a restriction to be applied for any data expressed in the standards in § 170.213. We have also finalized that conformance with this paragraph is required by January 1, 2026.

In response to comments on whether a patient or health care provider may be best suited to determine if data should be private, or a covered entity's obligation to accept a patient's request, we reiterate our statement from the HTI–1 Proposed Rule that our intent is to advance technologies that support requirements already extant under the HIPAA Privacy Rule (88 FR 23821). In the HTI–1 Proposed Rule, we described that the HIPAA Privacy Rule provides individuals with several rights intended to empower them to be more active participants in managing their health information. These include the right to access certain health information maintained about the individual; the right to have certain health information amended; the right to receive an accounting of certain disclosures; the right to receive adequate notice of a covered entity's privacy practices; the right to agree or object to, or authorize, certain disclosures; the right to request restrictions of certain uses and disclosures; and provisions allowing a covered entity to obtain consent for certain uses and disclosures. Under the HIPAA Privacy Rule, covered entities as defined in 45 CFR 164.530(i) are required to allow individuals to request a restriction on the use or disclosure of their PHI for treatment, payment, or health care operations and to have policies in place by which to accept or deny such requests (See 45 CFR 164.522(a)(1)(i)(A) and (B)). The HIPAA Privacy Rule does not specify a particular process to be used by individuals to make such requests or for the entity to accept or deny the request. However, we believe that certified health IT should—to the extent feasible—support covered entities so they can execute these processes to protect individuals' privacy and to provide patients an opportunity to exercise this right (88 FR 23821).

We further stated that identifying which health data are defined as ''sensitive'' may vary across federal or state laws and may further vary based on an individual's perspective. Thus, the concept of ''sensitive data'' is dynamic and specific to the individual. Patient populations that have historically been subject to discrimination may identify a wide range of demographic information as sensitive, including race, ethnicity, preferred language, sex, sexual orientation, gender identity, and disability status—or patients may want to restrict health data that they view as sensitive, such as behavioral health or reproductive health-related data. These considerations from an individual's perspective may not always coincide with a health care provider's perspective. However, we believe that facilitating the ability of a patient to request such a restriction, in addition to addressing patient considerations, may also provide additional context for health care providers engaged in discussions with patients about their health information, sensitivities, and related concerns.

In response to commenters expressing concerns with timelines associated with requests, we decline to specify any limitations and note that a health care provider might include an option for an individual to specify such information as a part of the internet-based method for requests in § 170.315(e)(1).

For commenters expressing concerns related to legal liabilities, we reiterate that ONC certifies capabilities of Health IT Modules to perform specific functions, in many circumstances using specific standards. These are generally restricted to technical standards and capabilities. The user of the technology may also need to comply with certain requirements established by federal, state, territory, local or tribal law. Our intent for finalizing a technical means for individuals to request a restriction on their data is to advance tools that support privacy laws, including the HIPAA Privacy Rule right to request a restriction of certain uses and disclosures.

We note that the revision adding an internet-based method to make a request that we have finalized as part of § 170.315(e)(1) only supports one component of the HIPAA Privacy Rule. As noted in the HTI–1 Proposed Rule, we emphasize that use of a Health IT Module certified to revised criterion in § 170.315(e)(1) would not, by itself, fully discharge a covered entity's obligations

under the HIPAA Privacy Rule to allow an individual to request restriction of the use or disclosure of their PHI for treatment, payment, or health care operations or to have policies in place to address such requests (88 FR 23826). Further, use of any such certified Health IT Module would not discharge the obligations of a covered entity to meet any other requirements under 45 CFR 164.522. In addition, there may be other applicable laws that affect the exchange of particular information, and those laws should be considered when developing policies that provide individuals with more granular control over the use or disclosure of their PHI.

Comments. Several commenters expressed support for a patient's ability to manage various aspects related to their restriction requests. Multiple commenters noted that patients should be able to allow data use/exchange with some parties but not others and be able to decide the timing to safeguard patient autonomy and mitigate criminalization risk. Commenters also suggested that the patient should be able to define when a treatment relationship exists with a provider and only allow exchange with those providers who qualify, without explicit consent from the patient. One commenter noted that patients should be able to group data by type or encounter/procedure date or any criteria the patient wishes to impose on data use and exchange. Another commenter recommended allowing patients to decide how long they would like to restrict sensitive data from being shared. Another commenter suggested that we introduce certification requirements focused on granting health care providers the option to segment entire discrete sensitive notes, which allow clinicians to limit access to notes that patients consider sensitive, in a fully self-contained way.

With regards to recording patient requests for restriction, we received comments related to the inclusion of additional, relevant information. One commenter sought clarification on whether the requirement includes providing a standard way for a patient to state the purpose for a particular restriction. One commenter highly recommended that we include a certification criterion for the ''tracking of patient privacy and disclosure requests'' and another suggested that the concepts ''request for restriction was made'' and ''request for restriction was granted'' be separated in the requirements, recorded, and permanently associated with the related data. They also recommended that if a request is denied, a rejection reason should be required, retained, and exchanged alongside the related data so the next recipient of the data could potentially decide how to respond to the patient request.

Response. We thank the commenters for their input and advocacy on behalf of patients. In the HTI–1 Proposed Rule, we did not include proposals for § 170.315(e)(1) to add specific requirements on the format of the ''internet-based method'' individuals to request restrictions. We also did not specify additional functionality beyond the capability for patients (and their authorized representatives) to use an internet-based method to request a restriction to be applied for any data expressed in the standards in § 170.213. For example, we did not propose that the function must enable individuals to specifically identify different access roles for individual care team members or that patients be enabled to group health information in different ways, such as by type or encounter/procedure, or that patients be provided the option to segment entire discrete sensitive notes. We proposed an approach that, at minimum, would support a method for patients to request restrictions on PHI uses and disclosures through means related to the function supporting their ability to view, download, or transmit to a 3rd party their health information using certified health IT. We also did not propose specific terminologies to be used for the recording, disposition or notification of acceptance or denial of such requests. We appreciate the insights into enhanced functionalities and the related recording of data associated with such request, but such additional requirements would constitute a significant deviation from the proposed functionality. We do not believe that our proposals represent sufficient notice of the intent to add such requirements in this final rule. However, we will continue to engage with the health IT, standards, health care provider, and patient advocacy communities and to encourage innovative approaches to implementation of the adopted criteria and standards, as well as advancement of additional interoperable privacy standards and functionality. We will also monitor and analyze approaches by health IT developers for real world implementation of the revised criterion, and will consider such information to inform further modifications in future rulemaking.

We further note that, while we have not finalized the inclusion of additional capabilities or the application of a specific standard, there are obligations imposed on covered entities under the HIPAA Privacy Rule, if they agree to the requested restrictions, which this functionality may partially support, that health IT developers may consider supporting in related capabilities. For example, the HIPAA Privacy Rule prohibits a covered entity that agrees to a restriction request to use or disclose PHI in violation of such restriction except in certain limited circumstances. We encourage developers of certified health IT certifying Health IT Modules to the revised criterion in § 170.315(e)(1) to consider if there are methods that additional health IT tools could integrate with such Health IT Modules to facilitate these processes. In addition, while we did not propose and have not finalized the use of a standard for the use of security labels, we note that the HL7 CDA DS4P IG adopted in § 170.205(o) and the HCS Security Label Vocabulary that is referenced as part of the HL7 CDA DS4P IG are valuable health IT implementation resources for these purposes. As described in the HTI–1 Proposed Rule (88 FR 23824), the HCS Security Label Vocabulary could serve as the basis for a format-agnostic and transport-mechanism-agnostic standard for the application of security labels and to define the general instructions for security labels for a wide range of use cases including patient requested restrictions. While we are not requiring the use of the HCS Security Label Vocabulary within the revised criterion in § 170.315(e)(1), we recommend health IT developers consider its applicability for this purpose. We further note that the existing criteria ''security tags- summary of care send and receive'' in § 170.315(b)(7) and (b)(8) for sending and receiving summary of care records with security labels applied at the document, segment, or data element level would potentially support the capabilities commenters describe, including, for example, the ability to label a clinical note in the C–CDA as sensitive.

Comments. ONC also received several comments related to health equity and the need for patient-specific education about privacy restrictions. Multiple commenters recommended explaining specific aspects of the proposed functionality to patients such as, how it facilitates individual rights under the HIPAA Privacy Rule, how data is used to improve individual and population outcomes, and the proper role of health IT in protecting the security and privacy of health information. Multiple commenters also recommended providing counseling to patients regarding benefits and risks of restricting data and the impact on their

healthcare outcomes and safety. These comments focused on empowering patients with more granular privacy controls while noting that health literacy is an important part of such control in order to avoid disparities in privacy protection and on overall care quality. These commenters also identified that a person may not share sensitive health data if they do not understand the options for data sharing. One commenter suggested that we clarify if and how patients should be informed about functionality, specifically regarding the ability to request a restriction in multiple ways and with different levels of granularity (rather than just having the binary choice to either share or to not share data globally). Some commenters expressed concern that, if presented with complex data-element sharing options, patients may get confused and simply decide against sharing any data. Another commenter suggested that patients also need to be informed that their requests may be denied. Multiple commenters recommended that we add a requirement that patient-facing certified Health IT Modules include the capability to provide educational materials regarding the patient's options about disclosure and instructions regarding how to change disclosure limitations. Other commenters additionally highlighted the importance of patient education and health literacy, particularly for older-adult and disabled patients who may struggle with cognitive impairments or behavioral health issues. Finally, commenters sought clarification on whether the patient will be informed about who will be notified of restriction requests, as some may be concerned about negatively impacting their relationship with their providers and/or healthcare institutions.

In addition to patients, multiple commenters suggested that we provide education and guidance to providers, developers, and the industry as a whole. One commenter noted that provider organizations often do not have a clear mechanism for making patient restriction requests or know how to process/adjudicate/implement them if they do receive requests. Another commenter suggested that the industry will also need significant additional guidance and infrastructure. One commenter suggested that health IT developers should receive guidance regarding standards for developing a process for patient restriction requests. Another commenter noted that without a robust communication, education, and engagement effort, many entities essential to implementing the final rule at medical practices, hospitals, and health systems will be left out. Another commenter recommended that we consider the use of an implementation guide in future rulemaking, and one commenter requested that we provide full guidance on what different types of information should be flagged and how such flags would be addressed in FHIR resources.

Some commenters indicated ONC should provide education and work to clarify how this proposal is balanced with information blocking requirements. One commenter noted that confusion about information blocking often results in compliance officers, administrative personnel, in-house attorneys, and policy consultants misinterpreting regulations. They relayed feedback that some health IT developers refuse to provide patients or physicians granular controls over medical information. The commenter noted that compliance with the information blocking regulation is overriding compliance with other, more protective laws and rules, and they recommend that we adequately educate those involved in interpretating, implementing, and operationalizing our policies. Another commenter also requested that we address overlaps with information blocking, how and when to implement Notices of Privacy Practices by providers, and other healthcare workflow considerations that could allow this criterion to be misinterpreted and potentially abused. A commenter also stated that patients should be educated about information blocking and that patient facing tools should be held to similar requirements for access, privacy, and security as certified health IT products.

Response. We thank the commenters for the thoughtful consideration of the impacts of our proposals. As we noted in the HTI–1 Proposed Rule (see, for example, 88 FR 23748), health equity considerations are a driving force behind our proposals. We described the importance of expanding the interoperability of health data that is essential to identifying health disparities, measuring quality, addressing gaps in care access and outcomes, providing patient-specific preventative care and intervention, and supporting researchers in their ability to address the risk of unintended bias in clinical guidelines that may exacerbate disparities (88 FR 23821). We also described how important it is to ensure that with the expansion of exchange of granular health equity data comes expanded needs for thoughtful and deliberate privacy policies to support and protect patients (88 FR 23821). We discussed how ONC has specifically focused on how health IT can support efforts to reduce healthcare disparities and provide both insights and tools for the purposes of measuring and advancing health equity. This includes specific steps to expand the capabilities of health IT to capture and exchange data that is essential to supporting patient-centered clinical care that is targeted to supporting a patient's unique needs (88 FR 23821). We believe that patients should be empowered to make such decisions for themselves, and that support or education from clinicians might most appropriately be based on clinical impacts and considerations rather than a perceived lack of patient understanding or competency to make informed decisions.

We appreciate commenters suggestion that to fully implement the range of potential rights afforded by the HIPAA Privacy Rule, additional guidance, infrastructure, and standards development is needed to process for patient restriction requests. While we agree with the need for future work on technical specifications and implementation guides, we note that the behavior of covered entities and their role in patient education related to the HIPAA Privacy Rule or other privacy laws is outside the scope of ONC Certification Criteria for Health IT. We encourage covered entities using certified health IT to review and follow the obligations defined under the HIPAA Rules and other applicable laws and programs. We likewise encourage all actors who are required to comply with the HIPAA Rules, whether as HIPAA covered entities or business associates, to know and to comply with all of their obligations under the HIPAA Rules. In response to the comment indicating concern for ONC to extend adequate education on information blocking, we note our deliberate focus on developing accessible, user-friendly resources to help inform the effective implementation of these policies. This includes, but is not limited to, Frequently Asked Questions, recorded national webinars, and infographics all accessible on the ONC website.[183] For discussion of the relationship of privacy laws, including the HIPAA Rules and other laws, to the information blocking regulations, please see section IV.A of this final rule.

Finally, we appreciate commenters' suggestions about ONC's role in educating patients about health IT capabilities and standards as they relate

[183] ONC website: *HealthIT.gov* ''Information Blocking''. *https://www.healthit.gov/topic/information-blocking.*

to the privacy and security of health information. We are committed to continued public engagement for that purpose.

Comments. We received mixed feedback on the implementation timeline proposed for health IT developers to comply with any new or revised criteria. In general, commenters (both those opposed to and those supportive of the implementation timelines proposed) address the proposed timelines for updates to the criterion in § 170.315(e)(1) within the context of the implementation burden for that proposed revision and the proposed new criterion in § 170.315(d)(14) together. Multiple commenters expressed concerns that the overall implementation timeline is too aggressive. One commenter noted that if the scope of the proposed new and revised criteria were not narrowed and a holistic effort to also address updates to consent policies is not pursued, a significantly longer implementation period will be required (*i.e.,* four years or longer). Commenters consistently noted that a development project for the revised criterion in § 170.315(e)(1) in addition to the proposed new criterion in § 170.315(d)(14) would likely require two to three years to code and test and another one to two years for healthcare organizations to implement.

Some commenters shared feedback regarding how to make the proposed implementation timeframe more feasible. Multiple commenters suggested that if we narrow the scope to a limited set of USCDI v3 data elements in § 170.315(e)(1) for which restrictions can be requested and clearly and narrowly define the set of restrictions that certified health IT must support (*e.g.,* restricting the specified data from being accessed by proxy users of the patient portal) in the proposed criterion in § 170.315(d)(14), two years from the publication of a final rule would be feasible. Another commenter requested that we take an incremental approach and start with a low risk, target use case for the effective date of January 1, 2026. This would allow developers and providers to test, learn from and build on this capability over time at both the developer and user levels to address potential issues and risks.

Conversely, some commenters felt the timeframe would be difficult to operationalize and expressed concerns regarding the implementation timeline as being too aggressive. Multiple commenters noted that the proposed criterion would not be finalized until after the development and finalization of the USCDI v3, which ONC released July 2022, so there would not be perfect alignment between the use of USCDI v3 and the applicability of our proposed new and revised criteria. Some commenters recommended that ONC should have a constrained scope of USCDI subject to the tagging and to start with a more focused set of the most relevant data elements in the USCDI thus excluding certain sensitive data from what is shareable from within the USCDI until the criterion is fully operationalized. Commenters encouraged ''control'' or ''consent'' as an over-arching principle to be timed along with USCDI's expansion to more person-centered information and concepts. Commenters noted this alignment is essential for EHR developers to have the incentive to give users control over their preferences and for physicians be able to honor patients' expressed preferences related to sensitive, life-changing, or abnormal results. In one instance, a commenter also indicated that if ONC were to finalize this proposal then it should reconsider implementation to an earlier requirement date of January 1, 2024, to ensure that operationalizing patient requested restrictions is an immediate priority for software developers if finalized.

Response. We thank the commenters for their input and consideration of implementation needs and challenges. As previously noted, we have not finalized the proposed new criterion at § 170.315(d)(14) nor the corresponding changes to § 170.550(h). We have only finalized the revisions to the criterion in § 170.315(e)(1). We believe that the reduced scope of the changes we have finalized—focusing on the revised criterion in § 170.315(e)(1) and outlining our commitment to encourage the further adoption, use, and advancement in support of numerous care settings and use cases of the existing criteria in § 170.315(b)(7) and (b)(8) for sending and receiving health information with security labels—should help mitigate the concerns over scale, implementation timeframes, and feasibility. We also believe this approach is appropriate to supporting the advancement of health IT for privacy workflows that place importance on the need to empower patients with agency and control of their data, while acknowledging real challenges, including but not limited to scale and feasibility, as described earlier including from those in support of our proposals. We also agree with commenters that the revisions to the criterion in § 170.315(e)(1) for use of the USCDI v3 are finalized to occur at the same time as the revisions to the criterion in § 170.315(e)(1) described in this section. We have finalized that these revisions to the criterion in § 170.315(e)(1) align with the updates made to USCDI, as discussed in section III.C.1 of this final rule, so that the functionality is synchronized with the USCDI v3 including any new or updated data elements.

We have finalized our proposal to revise the criterion in § 170.315(e)(1) as proposed, with the specific revision in § 170.315(e)(1)(iii). Pursuant to other policy decisions discussed elsewhere in this final rule on compliance timing, we have adopted our proposal that conformance with this new paragraph will be required for Health IT Modules certified to § 170.315(e)(1) by January 1, 2026.

11. Requirement for Health IT Developers To Update Their Previously Certified Health IT

In the HTI–1 Proposed Rule, we proposed to make explicit in the introductory text in § 170.315 that health IT developers voluntarily participating in the Program must update their certified Health IT Modules—including when new standards and capabilities are adopted—and provide that updated certified health IT to customers in accordance with the timelines defined for a specific criterion or standard where included, such as via cross-reference, in § 170.315 (88 FR 23827). We proposed that health IT developers with health IT certified to any of the certification criteria in § 170.315 would need to update their previously certified Health IT Modules to be compliant with any revised certification criterion adopted in § 170.315 (please see section III.A.2 of this final rule for discussion of the adopted definition of revised certification criterion (or criteria)), including any certification criteria to which their Health IT Modules are certified that reference new standards adopted in 45 CFR part 170 subpart B, and capabilities included in the revised certification criterion. Health IT developers would also need to provide the updated health IT to customers of the previously certified health IT according to the timelines established for that criterion and any applicable standards (88 FR 23827).

We noted that in addition to supporting the goals of the Program, we believe this approach will help to advance interoperability. We stated that requiring health IT developers who voluntarily participate in the Program to update Health IT Modules to revised certification criteria (including new and revised standards) can help to advance capabilities for access, exchange, and

use of EHI for authorized use under applicable State or Federal law. In addition, we explained that ensuring health IT developers voluntarily participating in the Program provide such updates to customers will help to enable the secure exchange of EHI with, and use of EHI from, other health information technology without special effort on the part of the user. We also stated that the proposed timelines serve to support clear and transparent benchmarks for furthering interoperability throughout the health IT infrastructure (88 FR 23827).

We explained that the updates to criteria may include technical capabilities such as security enhancements or additional electronic transactions not previously supported for a criterion. These updates may also include an expansion of the data supported by content, vocabulary, and format standards to increase the scope of interoperable EHI (88 FR 23827). The adoption of USCDI v3 and its incorporation into certification criteria through updates to those criteria, as finalized in this rule, means that certified health IT systems will be able to support representation of this health information in a standardized computable format. Updating current systems to incorporate these data elements and providing updated certified health IT to customers would allow users of certified health IT to begin to access, exchange, and use such data without special effort. Over the long term, this advancement of interoperability for certified health IT systems may also have a positive impact on the availability of this essential data and the capability to access, exchange, and use this data across a nationwide health IT infrastructure—including for purposes not yet specifically supported by certified health IT such as clinical research (88 FR 23827).

Comments. Commenters outlined concerns regarding the definition of ''provide'' and, specifically, the preamble language that states, ''[we] propose that to 'provide' the product means the developer must do more than make the product available and there must be demonstrable progress towards implementation in real-world settings.'' Commenters expressed confusion about what ''demonstrable progress towards implementation in real-world settings'' means and suggested ONC clearly define this phrasing. Commenters also mentioned concerns about how the responsibility of implementing or upgrading to health IT meeting the revised certification requirements ultimately lies with the provider and not the developer.

Response. We thank commenters for their input. We appreciate that the responsibility of implementing a Health IT Module is not solely on the developer. With this final rule, as discussed below, we recognize the potential for variation in how implementation of certified health IT proceeds, including implementation consistent with the agreements, contracts, and licenses that exist between health IT developers and their customers of certified health IT. Overall, our proposed approach is not new or exclusive to the proposed updates in the HTI–1 Proposed Rule, but rather is consistent with the approach ONC adopted for the ONC Cures Act Final Rule updates to the 2015 Edition certification criteria (85 FR 25664). From the effective date of the ONC Cures Act Final Rule through December of 2022, and based on the programmatic technical assistance, developers of certified health IT successfully updated their technology and provided it to customers.[184] However, as discussed in the HTI–1 Proposed Rule, ONC used the terms ''provide'' and ''make available'' interchangeably in the ONC Cures Act Final Rule, and subsequent technical assistance (including through correspondence and via public forums) was required to support clarity and achieve that transition (88 FR 23828). We also noted in the HTI–1 Proposed Rule that ''provide'' does not imply that the Health IT Module must be in production use across all customers (88 FR 23828). Under this clarification for the term ''provide,'' we have finalized as proposed that ''provide'' does not mean that the Health IT Module must be in production use across all customers. We encourage developers of certified health IT to provide updated Health IT Modules to their customers—and support them in their implementation of such updated modules—in the manner most appropriate to support safety, security and interoperability across settings and systems.

It is beneficial or necessary to further define ''demonstrable progress toward implementation in real world settings'' as the phrasing or concept is not part of the finalized regulatory definition of ''provide.'' As noted by commenters, the phrasing/concept introduces additional confusion over what might constitute demonstrable progress and whether implementation includes production use.

We stated in the HTI–1 Proposed Rule, and continue to maintain, that we do not intend for ''provide'' to mean either that customers who no longer wish to use a certified Health IT Module must be provided the update or that customers who do choose to use an updated certified Health IT Module must have the updated Health IT Module in production use by the timelines established for the health IT developer (88 FR 23828). We note that there are a number of instances in which a health IT developer will have updated the Health IT Module, but the customer may have declined the update. This can occur when the customer is not yet ready to implement new functionalities, standards, and/or workflows, or when the customer decides that the functionalities, standards, and/or workflows are not relevant to their clinical practice.

With consideration of the above explanations, we have finalized the term ''provide'' with a further clarification that ''provide'' is binary. That is, the updated Health IT Module is either provided to customers (respective of customer choice) by the timeline established, or it is not. Further and accordingly, we have also finalized that a health IT developer must update a Health IT Module as described and provide customers with updated Health IT Modules in order to maintain certification of the Health IT Module. Consistent with the definition of interoperability and the Assurances Condition and Maintenance requirements discussed in section III.D, the certified Health IT Module must be able to support all the capabilities to which it is certified, and such capabilities must be provided to the customer for use without special effort by the end of the regulatory specified timelines.

We also note that we proposed to include the definition of ''provide'' in § 171.102, which stated that ''*Provide* is defined as it is in § 170.102.'' We did not intend to define ''provide'' in part 171 of the HTI–1 Proposed Rule. Therefore, in this final rule, we have not finalized the revision to add the definition of ''provide'' in § 171.102.

We have finalized in § 170.315 for all revised certification criteria and in 45 CFR part 170 subpart B for each applicable standard, as proposed, that a Health IT Module may be certified to either the existing certification criterion or the revised certification criterion until the end of the transition period when the prior standard(s) and/or certification criterion no longer meet certification requirements. During this time period, existing customers may

[184] See ONC *Achieving a Major Milestone: Health IT Developers Certify to Cures Update https://www.healthit.gov/buzz-blog/health-it/achieving-a-major-milestone-health-it-developers-certify-to-cures-update.*

continue to use the certified health IT they have available to them and can work with their developers to implement updates in a manner that best meets their needs consistent with the established regulatory timeframes. Finally, as with the 2015 Edition Cures Update, in order to support effective communication of the updates, we will implement a practical approach to facilitate transparency using the Certified Health IT Product List (CHPL),[185] which is the tool that health care providers and the general public may use to identify the specific certification status of a certified health IT product at any given time, to explore any certification actions for a product, and to obtain a CMS Certification ID for a product, which is used when participating in some CMS programs.

Comments. Commenters voiced concerns about how the HTI–1 Proposed Rule aligns with CMS's Promoting Interoperability Program—specifically, the impact on the timing of when hospitals and clinicians implement or upgrade an EHR in order to comply with CMS regulations.

Response. We thank commenters for their feedback. We have worked closely with CMS for more than a decade to ensure alignment between our Program and CMS programs, including the Medicare Promoting Interoperability Program and the Quality Payment Program (these programs incorporate the programs previously known as the EHR Incentive Payment Programs, or ''Meaningful Use'') and we will continue to do so moving forward. For example, CMS finalized in the CY 2021 PFS final rule (85 FR 84815 through 84828) that health care providers participating in the Medicare Promoting Interoperability Program and eligible clinicians participating in the Quality Payment Program must use certified health IT that satisfies the definitions of CEHRT at 42 CFR 495.4 and 414.1305, respectively, and is certified under the Program, in accordance with the 2015 Edition Cures Update, as finalized in the ONC 21st Century Cures Act Final Rule (85 FR 25642).

As part of the CY 2024 PFS Final Rule, CMS finalized revisions to the definitions of CEHRT in §§ 495.4 and 414.1305 for the Medicare Promoting Interoperability Program and for the Quality Payment Program (88 FR 78308 through 79312) in a manner consistent with the ''edition-less'' approach to health IT certification that we proposed in the ONC HTI–1 Proposed Rule. This included removing references to the ''2015 Edition'' in the CEHRT definition, and that in order to meet the CEHRT definitions, technology must meet ONC's certification criteria in 45 CFR 170.315 ''as adopted and updated by ONC.'' CMS stated that these revisions would ensure that updates to the 2015 Base EHR or subsequent Base EHR definition at § 170.102, and updates to applicable health IT certification criteria in § 170.315, would be incorporated into CEHRT definitions, without requiring additional regulatory action by CMS. CMS noted in its final rule that it will continue to determine when new or revised versions of measures that require the use of certified health IT would be required for participation under the Medicare Promoting Interoperability Program and the Quality Payment Program. In determining requirements for any potential new or revised measures, CMS stated it will consider factors such as implementation timelines and provider readiness to inform when CMS proposes requiring participants to complete measures that rely on the use of certified health IT (88 FR 79310). We will continue to work with CMS as we finalize timeline requirements for developers of certified health IT to update and provide certified health IT to their customers so that their customers (*e.g.,* health care providers) can meet CMS requirements for the use of such certified health IT. We also note that, historically, CMS has included additional guidance for program participants within CMS proposed or final rules (see, for example, 85 FR 84818–84828).

Comments. Commenters in general agreed that if a Health IT Module is not updated to new or revised certification criteria, then the Health IT Module should be retired at the ''expiration date'' of the certification criterion and/or standard. One commenter expressed confusion about using the term ''shall update'' when it is up to the developer to determine if they want to update their health IT to comply with new or revised certification criteria.

Response. We thank commenters for their input. Participation in the Program is voluntary and, therefore, any ''shall'' statements within the Program only apply to a health IT developer that is participating and plans to continue to participate in the Program. If a developer participating in the Program intends to no longer support a specific certified Health IT Module, but intends to continue to participate in the Program, previously finalized policies relating to the withdrawal of a Health IT Module or modification of a certificate would remain applicable (88 FR 23828). Otherwise, if a health IT developer participates in the Program and intends to maintain certification of a Health IT Module, the developer will need to comply with the requirements of the Program, including the finalized requirement in the introductory text to § 170.315 stating ''[f]or all criteria in this section, a health IT developer with a Health IT Module certified to any revised certification criterion, as defined in § 170.102, shall update the Health IT Module and shall provide such update to their customers in accordance with the dates identified for each revised certification criterion and for each applicable standard in 45 CFR part 170 subpart B.''

D. Assurances Condition and Maintenance of Certification Requirements

In the HTI–1 Proposed Rule, we proposed to establish a new Condition of Certification and accompanying Maintenance of Certification requirements under the Assurances Condition of Certification (88 FR 23828 through 23830). These new requirements would serve to provide the assurances to the Secretary that Congress sought in the Cures Act and further clarify Program requirements that are established under the authority Congress provided in section 3001(c)(5) of the PHSA, as amended by the Cures Act, and discussed in detail in the HTI–1 Proposed Rule (88 FR 23826).

1. Condition of Certification

We proposed in § 170.402(a)(5), that, as a Condition of Certification, a health IT developer must provide an assurance that it will not inhibit a customer's timely access to interoperable health IT certified under the Program (88 FR 23829). To support this assurance, we proposed accompanying Maintenance of Certification requirements, which are discussed below. The Maintenance of Certification requirements define the scope of this Condition of Certification and provide clarity in terms of what it would mean to take the action of ''inhibiting,'' what constitutes ''timely access,'' and what is ''interoperable health IT certified under the Program'' (88 FR 23829).

Comments. In general, commenters supported the establishment of a new Condition of Certification and the accompanying Maintenance of Certification requirements. Commenters identified multiple benefits of the proposed requirements such as ensuring timely access to interoperable health IT and promoting the adoption of advanced technologies and capabilities that can enhance patient care and

[185] ONC Certified Health IT Product List: *https://chpl.healthit.gov.*

workflow efficiency. One commenter noted how these requirements will positively impact the community of health centers by ensuring they have access to the latest capabilities and standards.

Response. We thank commenters for their support. As noted above and discussed in detail in the HTI–1 Proposed Rule (88 FR 23826), these new requirements will serve to provide the assurances to the Secretary that Congress sought and further clarify Program requirements. Interoperable health IT is an underpinning of the Program and particularly the conditions of certification found in the Cures Act and implemented in 45 CFR part 170 subpart D. Congress established support for health IT interoperability beginning with the authority provided in section 3001(c)(5) of the HITECH Act to adopt standards (including implementation specifications and certification criteria) and establish the Program.

For purposes of certification and the maintenance of such certification under the Program, a health IT developer will need to provide an assurance that its health IT is certified to the most recently adopted certification criteria and such certified health IT is made available to its customers in a timely manner. These actions are essential because certification criteria, and in particular revised certification criteria (as defined in this final rule), include standards, implementation specifications, and capabilities that support and improve interoperability as that term is defined by the Cures Act and incorporated in 45 CFR part 170. Since the inception of the Program, ONC has updated certification criteria to include the most recent versions of standards and implementation specifications that most appropriately support and improve interoperability at the time of adoption. We do this because as standards and implementation specifications evolve, they, by their very nature, improve interoperability by allowing for more complete access, exchange, and use of all electronically accessible health information. Further, the interoperability definition also focuses, in part, on the secure exchange and use of EHI from other health IT without special effort on the part of the user. The Assurances Condition of Certification is an important piece to supporting and achieving these goals because it seeks assurances from health IT developers that they will not take any actions to inhibit the appropriate access, exchange, and use of EHI. We, therefore, have finalized in § 170.402(a)(5), as proposed that, as a Condition of Certification, a health IT developer must provide an assurance that it will not inhibit a customer's timely access to interoperable health IT certified under the Program.

Comments. A handful of commenters expressed concern about how the Maintenance of Certification requirements may be interpreted as mandatory when the decision to participate in the Program is voluntary. One commenter identified the use of the term ''shall update'' as possibly being misunderstood as an obligation for developers to continue to participate in the Program when, in fact, it is up to the developer to determine if they want to pursue certification or to allow the module to be retired.

Response. We thank the commenters for their input. Participation in the Program is voluntary. Health IT developers do not have an obligation to continue to participate in the Program. However, as discussed under section III.C.11 ''Requirement for Health IT Developers to Update their Previously Certified Health IT,'' if a health IT developer does participate in the Program, it needs to comply with the requirements of the Program, including the finalized Assurances Condition and Maintenance of Certification requirements.

Comments. Two commenters identified difficulties in navigating between the different requirements for certified health IT for ONC and CMS. Both commenters recommended CMS delay the effective date of changes to the definition of CEHRT referenced within CMS programs until the next reporting period or performance year. The commenters stated that this proposed modification would eliminate confusion and promote cross-agency collaboration.

Response. We thank the commenters for their feedback. We recognize that certain CMS programs, including the Medicare Promoting Interoperability Program and the Quality Payment Program, require the use of technology meeting the CEHRT definitions in 42 CFR 495.4 and 42 CFR 414.1305. The CEHRT definitions cross-reference health IT certification criteria in 45 CFR 170.315, including relevant dates within the certification criteria which define the requirements of the certification criterion.

While changes to the definition of CEHRT maintained by CMS are outside the scope of this final rule, we note that, as part of the CY 2024 PFS Final Rule, CMS finalized revisions to the definitions of CEHRT in 42 CFR 495.4 and 414.1305 for the Medicare Promoting Interoperability Program and for the Quality Payment Program (88 FR 78308 through 79312), including specifying that in order to meet the CEHRT definitions, technology must meet the 2015 Base EHR or subsequent Base EHR definition (as defined at 45 CFR 170.102) and other certification criteria in 45 CFR 170.315 ''as adopted and updated by ONC.'' CMS stated that these revisions would ensure that updates to the 2015 Base EHR or subsequent Base EHR definition at § 170.102, and updates to applicable health IT certification criteria in § 170.315, would be incorporated into the CEHRT definitions, without requiring additional regulatory action by CMS. We also note that CMS stated that it did not agree with separate effective dates in the CEHRT definitions for the use of updated certified health IT products within the Medicare Promoting Interoperability Program or the Quality Payment Program, as recommended by commenters (88 FR 79311). CMS stated that emphasizing the timelines ONC adopts through notice and comment rulemaking for health IT developers to update and provide certified technology to their customers will reduce burden on participants in the Medicare Promoting Interoperability Program and the Quality Payment Program. CMS further stated that it will continue to determine when new or revised versions of measures that require the use of certified health IT would be required for participation under the Medicare Promoting Interoperability Program and the Quality Payment Program and will consider factors such as implementation time and provider readiness to determine when to require reporting on these measures. We agree with CMS' statements on these topics.

In order to support effective communication of the updates, we intend to implement a practical approach to supporting CMS program participants and other certified health IT users through the Certified Health IT Product List (CHPL) in the same manner as was implemented for the 2015 Edition Cures Update. As also discussed under section III.C.11 ''Requirement for Health IT Developers to Update their Previously Certified Health IT,'' the CHPL is the tool that health care providers and the general public may use to identify the specific certification status of a certified health IT product at any given time, to explore any certification actions for a product, and to obtain a CMS Certification ID for a product, which is used when participating in some CMS programs. We note that historically, CMS has included additional guidance for such

program participants within CMS proposed or final rules (see, for example, 85 FR 84818–84828).

2. Maintenance of Certification Requirements

We proposed, in § 170.402(b)(3)(i), that a health IT developer must update a Health IT Module, once certified to a certification criterion adopted in § 170.315, to all applicable revised certification criteria, including the most recently adopted capabilities and standards included in the revised certification criterion (88 FR 23829).

We also proposed, in § 170.402(b)(3)(ii), that a health IT developer must provide all Health IT Modules certified to a revised certification criterion to its customers of such certified health IT. We clarified that a customer, for this purpose, would be any individual or entity that has an agreement to purchase or license the developer's certified health IT (88 FR 23829).

We proposed separate ''timely access'' or ''timeliness'' Maintenance of Certification requirements for each of the two proposed Maintenance of Certification requirements above that would dictate by when a Health IT Module must be updated to revised certification criteria, including the most recently adopted capabilities and standards; and by when a Health IT Module certified to a revised certification criterion, including the most recently adopted capabilities and standard, must be provided to the health IT developer's customers. We proposed, in § 170.402(b)(3)(iii), that unless expressly stated otherwise in 45 CFR part 170, a health IT developer must complete the proposed ''update'' and ''provide'' requirements according to the following proposals. First, we proposed, in § 170.402(b)(3)(iii)(A), that a health IT developer must update and provide a Health IT Module by no later than December 31 of the calendar year that falls 24 months after the effective date of the final rule adopting the revised certification criterion or criteria. Second, we proposed that the ''provide'' requirement would need to be completed within this same timeframe for customers of the previously certified health IT that must be updated under the ''update'' proposal. However, we proposed deviations to this timeframe because the ''provide'' requirement applies to all Health IT Modules that are certified to a criterion that meets the revised certification criterion definition (*i.e.,* not just health IT previously certified to a 'prior version' of a revised certification criterion) and to *new* customers of health IT certified to revised certification criteria (88 FR 23829 through 23830).

In all the above circumstances, we proposed that health IT certified to revised certification criteria must be provided to all customers, including new customers (*i.e.,* new to the capabilities), of health IT developers under the Program within reasonable timeframes (88 FR 23830).

Comments. Multiple commenters supported the Assurances Condition and Maintenance of Certification requirements. One commenter suggested health IT developers be required to provide all current and new customers with the most current version of a certified Health IT Module. Additionally, the commenter recommended that all health IT developers who have chosen not to comply with new or revised certification standards send a communication to customers in order to better inform such customers.

Response. We thank commenters for their support. We have finalized in § 170.402(b)(3)(i), as proposed, that a health IT developer must update a Health IT Module, once certified to a certification criterion adopted in § 170.315, to all applicable revised certification criteria, including the most recently adopted capabilities and standards included in the revised certification criterion. For clarity, '*applicable* revised certification criteria' includes those certification criteria to which the Health IT Module was previously certified that meet the definition of a revised certification criterion as finalized in this rule (please see section III.A.2 of the preamble, including Table 1, and ''revised certification criterion (or criteria)'' under § 170.102 of the regulation text for the definition of revised certification criterion (or criteria)). Equally important, and, as stated above, to meet the requirement, the Health IT Module will need to be updated to the most recently adopted capabilities and standards included in the revised certification criterion. Second, we have finalized, in § 170.402(b)(3)(ii), that a health IT developer must provide all Health IT Modules certified to a revised certification criterion to its customers of such certified health IT. As noted above, a customer, for this purpose, is any individual or entity that has an agreement to purchase or license the developer's certified health IT.

In response to the comment about sending a communication to customers by a health IT developer not complying with the ''update and provide'' requirements, we note that the developer would, under the commenter's described circumstances, violate these new Maintenance of Certification requirements and the Condition of Certification we have finalized at § 170.402(a)(5), by *inhibiting* a customer's timely access to interoperable health IT certified under the Program. As such, the developer will have committed non-conformities under the Program, unless the health IT developer did so for a permissible reason as described in section III.C.11 (for example, a developer of certified health IT would not be required to provide updated certified health IT to any customer that elected to decline the update for any reason; or a health IT developer's exercising its ability to reduce the scope of a certification while not under ONC–ACB surveillance or ONC direct review). Because we did not propose a requirement that health IT developers who have chosen not to comply with new or revised certification standards send a communication to customers in order to better inform providers and hospitals, we have not accepted this recommendation. However, if the developer committed a non-conformity, the Program process for correcting the non-conformity may involve notification to all customers.

Comments. Commenters requested additional information regarding when, as proposed, a regulatory exception (''unless expressly stated otherwise in 45 CFR part 170'') to the 24-month criteria might be applied by ONC in § 170.402(b)(3)(iii)(A). Commenters outlined how a possible exception creates additional timelines in an environment where competing priorities between meeting deadlines associated with ONC requirements and the requirements under CMS regulations already exist. A few commenters requested ONC provided explicit guidelines about when a regulatory exception to the ''24 months plus X'' requirement might be applied. One commenter expressed concern about how this proposed regulatory exception may negatively impact development roadmaps and the ability to fulfill requests falling outside of non-regulatory functionality. Further, multiple commenters expressed concerns about the proposed deadlines and the implications these timeframes have on developers and providers. Commenters stressed the importance of having 18–24 months to address any new or revised certification requirements and identified the December 31st date outlined in the HTI–1 Proposed Rule as a specific concern. One commenter specifically stated

''[g]iven requirements on the implementation end of the cycle, vendors must have 24 months prior to general availability to properly develop and certify their solutions.''

Response. We appreciate commenters' feedback. For purposes of regulatory clarity, we have revised the proposed ''timeliness'' provision in § 170.402(b)(3)(iii)(A). We have modified the proposed timeliness requirement to state, ''a health IT developer must complete the ''update'' and ''provide'' requirements consistent with the timeframes specified in part 170'' (§ 170.402(b)(3)(iii)(A)). This means that the compliance dates included in the certification criteria in § 170.315 and standards in subpart B will establish when health IT developers need to comply with these Maintenance of Certification requirements. In § 170.402(b)(3)(iii)(B), we have finalized the provision that health IT developers will still have up to 12 months, at a minimum, to provide *new* customers with health IT certified to revised criteria. Specifically, we have finalized that for health IT developers that obtain new customers after the effective date of a final rule, the health IT developer must provide health IT certified to revised certification criteria either in the timeframe identified in part 170 or not later than 12 months after the purchasing or licensing relationship has been established between the health IT developer and the new customer for the health IT certified to the revised criterion.

The timeframe, as noted above, will offer health IT developers no less than 12 months to provide health IT certified to revised certification criteria to new customers (*i.e.,* customers new to the capability). Based on the timeframe, a health IT developer has the ability to plan both the certification to revised certification criteria and the execution of contracts and agreements with new customers to ensure that it can meet the above timeline for new customers. To note, we have also finalized a conforming revision to the Real World Testing Maintenance of Certification requirements in § 170.405(b), as proposed at 88 FR 23830, in that we removed most of the ''update and provide'' requirements currently found in § 170.405(b)(3) through (7) and (b)(10) because they will be moot based on the effective date of this final rule (*e.g.,* many timelines expired on December 31, 2022). Therefore, in § 170.405, we removed and reserved paragraphs (b)(3) through (7) and (b)(10).

E. Real World Testing—Inherited Certified Status

In the ONC Cures Act Final Rule, we finalized requirements in § 170.405(a) that a health IT developer with Health IT Module(s) certified to § 170.315(b), (c)(1) through (3), (e)(1), (f), (g)(7) through (10), and (h) must: successfully test the real world use of the technology for interoperability in the type(s) of setting(s) in which such technology would be marketed. We established in § 170.405(b) that each developer's annual real world testing plan is required to be published by December 15 of a given year and would need to address all of the developer's Health IT Modules certified to criteria listed in § 170.405(a) as of August 31 of that year (85 FR 25769). We also finalized that the annual real world testing plan would pertain to real world testing activities to be conducted in the year following the December 15 plan publication due date, with an annual real world testing results report to be published by March 15 (§ 170.405(b)(2)(ii) of the year following the year in which the real world testing is conducted) (85 FR 25774).

Many health IT developers, however, update their Health IT Module(s) on a regular basis, leveraging the flexibility provided through the Program's Inherited Certified Status (ICS) option.[186] Because of the way that ONC issues certification identifiers, this updating can cause an existing certified Health IT Module to be recognized as new within the Program. All updates to certified health IT must be tracked and recorded to support program integrity and transparency within the Program. When a certified health IT developer leverages ICS for Health IT Modules that have been updated, they receive a new certification date for the newer version of the certified Health IT Module. When an ICS certification is issued, a new certification date is issued by the ONC–ACB to reflect these updates. Regular updating, especially on a frequent basis such as quarterly or semi-annually, creates an anomaly that could result in existing certified Health IT Modules being inadvertently excluded from the real world testing reporting requirements because of those updates.

In order to ensure that all developers test the real world use of their certified health IT, as required, we proposed in the HTI–1 Proposed Rule to eliminate this anomaly by requiring health IT developers to include in their real world testing results report the most recent version of those certified Health IT Module(s) that are updated using Inherited Certified Status after August 31 of the year in which the plan is submitted (88 FR 23831). This approach would ensure that health IT developers fully test all applicable Health IT Modules as part of their real world testing requirements. This policy would also prevent a developer from avoiding, or delaying conducting or reporting, real world testing specifically on the updated versions of Health IT Modules certified through Inherited Certified Status after August 31 of a given year. This policy would not change the underlying requirement that a developer with one or more Health IT Modules certified to any criterion listed in § 170.405(a) must plan, conduct, and report on real world testing of each of those Health IT Modules on an annual basis.

Comments. A significant number of commenters supported our proposal to require developers of certified health IT to include in their real world testing results report newer versions of those certified Health IT Module(s) that are updated using Inherited Certified Status after August 31 of the year in which the plan is submitted. Many commenters reiterated the importance of real world testing and expressed appreciation for ONC's efforts to address the anomaly that could result in existing certified Health IT Modules being inadvertently excluded from the real world testing reporting requirements when updated using Inherited Certified Status before their real world testing results reports are due. Several commenters praised the requirement to demonstrate conformity in a production environment and the assurance gained from testing results that reflect the most recent version of the certified health IT used to meet real world testing requirements. A commenter in support of this proposal suggested that ONC make real world testing mandatory for all health IT developers. Overall, commenters in support of this proposal recognize real world testing as a critical component to verifying certified health IT, eligible for real world testing, works in real world scenarios and use cases, and appreciate ONC's efforts to advance real world testing requirements by requiring health IT updated using Inherited Certified Status to be included in health IT developers' real world testing results reports. One commenter requested that ONC clarify in rulemaking which versions of the certified Health IT Module, after updating using ICS, are required to be included in real world testing results report.

Response. We appreciate these comments and agree with the need to

[186] *https://www.healthit.gov/sites/default/files/policy/public_applicability_of_gap_certification_and_inherited_certified_status.pdf.*

ensure newer versions of certified Health IT Modules updated after the August 31 deadline using Inherited Certified Status are accounted for in real world testing and results reporting. We have issued *public resources* that provide clarity on what versions of certified health IT should be included in real world testing results reports and believe that the guidance is sufficient for developers to determine, for their unique circumstances, which versions of their certified health IT should be included in their results reports.[187] Currently, certification criteria identified in § 170.405(a) are required to adhere to the Real World Testing Condition and Maintenance of Certification requirements, and this final rule does not change the applicable criteria (§ 170.315(b), (c)(1) through (3), (e)(1), (f), (g)(7) through (10), and (h)).[188] ONC will continue to collaborate with interested parties to ensure all required certified health IT continues to function in real-world scenarios and workflows as intended by certification requirements for interoperability and data exchange. We have finalized our requirements at § 170.405(b)(2)(ii) for health IT developers to include in their real world testing results report the newer version of those certified Health IT Module(s) that are updated using Inherited Certified Status after August 31 of the year in which the plan is submitted.

Comments. One commenter was not supportive of this proposal and the requirement for health IT developers to conduct real world testing on their certified health IT and expressed concerns that it adds no value to health IT certification. This commenter suggested that if available functionality is not being implemented in production environments it should not be required for real world testing.

Response. We did not propose any substantive changes or updates to the real world testing requirements in § 170.405. Congress required the real world testing of certified health IT for interoperability in the Cures Act (PHSA § 3001(c)(5)(D)(v)). We have implemented this requirement through the Real World Testing Condition and Maintenance of Certification requirements. The real world testing of certified health IT has value to the Program and users of certified health IT. Since December 2022, more than 500 real world testing plans and results have been submitted by developers of certified health IT with applicable certification criteria. The plans and reports have provided insight into how developers of certified health IT think about framing and measuring the interoperability of their certified Health IT Modules in production use. The plans and reports also provide interested parties with information they can use to understand how a specific certified Health IT Module is demonstrating real world interoperability.[189] We are aware of the challenges faced by health IT developers when establishing approaches to meet their real world testing requirements. ONC has released several public resources to assist the developer community in developing real world testing plans and navigating unique circumstances such as low adoption of specific certified health IT capabilities.[190] Among numerous points of guidance, the Real World Testing Resource Guide includes information on how developers of certified health IT should treat Health IT Modules that do not have functionality or that have not yet implemented functionality in production environments. We also reiterate that the Aug 31 deadline for eligible certified health IT supports developer preparation activities well before entering the applicable calendar year of real world testing.

Comments. Several commenters raised concerns that are out of scope for the proposal, including suggestions for additional certification and real world testing requirements to improve interoperability, none of which are addressed in this rulemaking. Some made recommendations for how ONC may enhance certification and real world testing requirements by further defining measures, data elements, and how health IT should be assessed for data augmentation solutions. A number of these commenters expressed the need for additional real world testing requirements, such as more rigorous testing of data segmentation, standards and implementation guides, and required standard code sets. Some commenters requested more focus on public health data and the use of standard code sets to improve data quality for real world testing, stating that clinical and laboratory partners require data inputs that are high quality, correctly coded, and not reliant on human readability or narrative text to provide critical information. Commenters asserted that these additions to real world testing requirements would diminish mapping burden, improve data entry, facilitate improvements to data quality, and lessen administrative burden on clinical staff. One commenter requested that ONC require real world testing of certified health IT before the sale and implementation of the certified health IT in clinical settings. Another commenter requested that ONC not consider standards mature until they have been real world tested with publicly available comprehensive testing reports. Lastly, one commenter raised issues related to human research protocols when conducting real world testing using real patient data and the need to protect this data from misuse.

Response. We thank commenters for the input. Because these recommendations for certification and real world testing requirements are out of scope for the HTI–1 Proposed Rule in that we did not propose to change any related real world testing conformance requirements, we decline to finalize any such changes. ONC previously finalized requirements, through the ONC Cures Act Final Rule, for real world testing plans and results reports, the required elements to be included, and developers' responsibilities for establishing measure(s) for their approach to assessing their health IT in real world settings (see 85 FR 3580). We reiterate that the proposal finalized in this final rule specifically addresses health IT developers who update their certified Health IT Modules using Inherited Certified Status after the August 31 deadline and before results reports are due for a particular year of real world testing. We also note that the Inherited Certified Status flexibility is specifically designed for updates to certified Health IT Modules that do not adversely impact certified capabilities.

F. Insights Condition and Maintenance of Certification

1. Background and Purpose

The Cures Act specified requirements in section 4002(c) to establish an EHR Reporting Program to provide reporting on certified health IT in the categories of interoperability, usability and user-centered design, security, conformance to certification testing, and other categories, as appropriate to measure the performance of EHR technology. Data collected and reported would address information gaps in the health IT marketplace and provide insights on the use of certified health IT.

[187] See Real World Testing Resource Guide and other resources at: *https://www.healthit.gov/topic/certification-ehrs/real-world-testing.*

[188] Please see the Real World Testing Fact Sheet, page 3, for a list of certification criteria at: *https://www.healthit.gov/sites/default/files/page/2021-02/Real-World-Testing-Fact-Sheet.pdf#page=3.*

[189] *https://chpl.healthit.gov/#/collections/real-world-testing.*

[190] See Real World Testing Resource Guide and other resources at: *https://www.healthit.gov/topic/certification-ehrs/real-world-testing.*

To develop the EHR Reporting Program, ONC contracted with the Urban Institute and its subcontractor, HealthTech Solutions, to engage the health IT community for the purpose of identifying measures that developers of certified health IT would be required to report on as a Condition and Maintenance of Certification under the Program. Detailed background and history on the overall process, and the Urban Institute's reports, can be found in the April 18, 2023 Proposed Rule titled, ''Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing'' (88 FR 23832). For clarity purposes, we refer to the Condition and Maintenance of Certification associated with the ''EHR Reporting Program'' as the ''Insights Condition and Maintenance of Certification'' (also referred to as the ''Insights Condition'') throughout this final rule. We believe this descriptive name captures a primary policy outcome of this requirement.

2. Insights Condition and Maintenance of Certification—Final Measures

In the HTI–1 Proposed Rule (88 FR 23831), we stated that the proposed measures associated with the Insights Condition related to and reflected the interoperability category in section 3009A(a)(3)(A)(iii) of the PHSA. We further stated that these measures related to four aspects or areas of interoperability, which we referred to as measurement ''areas:'' individuals' access to EHI, public health information exchange, clinical care information exchange, and standards adoption and conformance, as discussed in further detail below (88 FR 23831). We explained that the majority of our proposed measures were data points derived from certified health IT. The measures generally consisted of numerators and denominators that would help generate metrics (*e.g.,* percent across a population), which were further detailed in each measure, but the measures could also serve as standalone values. We noted that in some cases we planned to generate multiple metrics by using different denominators for the same numerator or using different numerators with the same denominator. For each proposed measure, we included information on the rationale for the proposed measure, proposed numerators and denominators, and key topics for comment.

As stated in the HTI–1 Proposed Rule, we proposed to modify measures developed by the Urban Institute to reduce ambiguities and to address potential costs and burdens. Based upon public comment and interested party input consistent with section 3009A(a)(3)(C) and (D) of the PHSA, we proposed to modify the measures the Urban Institute developed, as well as the proposed minimum reporting qualifications, to ensure that small and startup developers are not unduly disadvantaged by the measures.[191]

We also stated that in future rulemaking we anticipated proposing additional measures for future iterations of the Insights Conditions and Maintenance of Certification requirements under the Program and that through this first set of measures we intended to provide insights on the interoperability category specified in the Cures Act (as codified at section 3009A(a)(3)(A)(iii) of the PHSA). We also stated that we intended to explore the other Cures Act categories (security, usability and user-centered design, conformance to certification testing, and other categories to measure the performance of EHR technology) in future requirements (88 FR 23832).

In the HTI–1 Proposed Rule (88 FR 23832), we stated that we explored various pathways on how to make it easier for the public to view and comment on the detailed technical specifications supporting the measures. We directed readers to consult our website *healthIT.gov* and provide comment on the technical specifications for measure calculation. We received numerous comments regarding the information described in the technical specifications for the measures, including the definitions of various measurement-related terms such as encounters and duplicate C–CDAs. We have included summaries of these comments within their respective measure sections in this final rule. While the substantive requirements for each measure are defined in this final rule, we determined that measure specification sheets are a logical and accessible method for the public to also view the technical specifications that support those requirements. The finalized specification sheets accompanying this final rule are available at *www.healthit.gov/hti-1.* This is consistent with the approach used by other HHS programs related to measure technical specifications (*e.g.,* CMS Electronic Clinical Quality Measures (CMS eCQMs)).[192] [193] This approach of publishing technical specification separately allows for more effective viewing of the technical details, including supporting public comment on those specifications in a transparent manner. We welcomed comments on the measure specifications sheets accompanying the HTI–1 Proposed Rule and noted in the HTI–1 Proposed Rule (88 FR 23832) that such public comment will be used to further refine the technical specifications. We also stated that we intended to keep these measure specification sheets up to date. We also note that if regulatory baselines associated with the metrics change in the future—such as a revision to a criterion through notice and comment rulemaking—the measure specification would also be changed to ensure alignment with the revised criterion.

Comments. Commenters, including health care provider specialty organizations, technology advocates, health information exchanges, healthcare quality organizations, and some health IT developers, were generally supportive of our proposals to implement the new Insights Condition, and of the measures and reporting processes described. A few commenters emphasized the potential of information gleaned from the Insights Condition to drive transparency in the health IT marketplace and, in particular, to highlight ways for patients to access and use their data. One commenter noted that ONC's development of the Insights Condition demonstrates commitment to improving interoperability, and encouraged ONC to envision a future state of health information exchange capabilities that include patient-requested restrictions, outcomes tracking, and integration of data from other sources such as Prescription Drug Monitoring Programs. Commenters also lauded the potential of the Insights Condition to clarify trends in current capabilities for interoperability services such as APIs that will allow the market to address gaps and improve interoperability. One commenter noted that they believe public health programs and safety net providers could particularly benefit from the Insights Condition and encouraged ONC to work with community health centers to ensure that its implementation supports the populations they serve.

Response. We thank commenters for the feedback and appreciate their support for the potential of the Insights Condition to address information gaps in the marketplace and improve interoperability. We also appreciate comments taking note of our efforts to improve interoperability and continue to explore avenues to increase efficient information exchange for use in improving health and healthcare. As

[191] Urban Institute. See *https://www.urban.org/policy-centers/health-policy-center/projects/ehr-reporting-program.*

[192] *https://ecqi.healthit.gov/.*

[193] *https://mmshub.cms.gov/get-involved/public-comments/overview.*

stated in the HTI–1 Proposed Rule (88 FR 23831), data collected and reported under the Insights Condition will address information gaps in the health IT marketplace and provide insights on the use of certified health IT. We also agree that public health and safety net providers can benefit from increased market transparency that the Insights Condition can provide. We will continue to engage with public health professionals and safety net providers in our implementation of the Program.

Comments. Some commenters suggested that information gained from the Insights Condition will not benefit current users of certified health IT, and some commenters questioned the value of the data in furthering interoperability.

Response. We fundamentally disagree with this perspective offered by some commenters. In the Cures Act, Congress established the requirement to create an EHR Reporting Program and we believe that submission of specific measures pursuant to the Insights Condition under the Program will provide transparent reporting, address information gaps in the health IT marketplace, and provide insights on the use of certified health IT. The adopted metrics are specifically meant to provide insights on how certified health IT enables various aspects of interoperability, including individuals' access to EHI, public health information exchange, clinical care information exchange, and standards adoption and conformance. These metrics help address gaps in information in the health IT marketplace by providing data on key aspects of interoperability that are neither directly nor publicly available from other sources. As described in greater detail within this final rule, the metrics will be shared with the public in a transparent manner on ONC's website.

Comments. A few commenters expressed support and understanding of the use of numerators and denominators by ONC. One professional society expressed support of all proposed measures and numerator/denominator combinations. One commenter specifically voiced support for all the various numerator/denominator combinations proposed as a key opportunity to provide market transparency on various aspects of how information is being exchanged and used by patients and health care providers, and another commenter specifically supported requiring health IT developers to report on the measures. Further, the commenter highlighted the potential of the various combinations to help ONC provide market transparency on various aspects of how information is being exchanged and used by patients and health care providers.

On the other hand, a number of commenters expressed confusion related to the terms numerator and denominator. One commenter requested ONC establish more succinct separation and definition of numerators and denominators for the Insights Condition. Further, the commenter stated measure definitions for numerators and denominators are confusing and overlap. Another commenter found the terms numerator and denominator confusing and requested that ONC use different ones. One commenter encouraged ONC to maximize reuse of collected data, such as allowing a given measure to be submitted once and tagged to count for all relevant metrics where it can be reused. One commenter suggested that ONC state in the overview section for the Insights Condition that developers will be required to submit raw data, and metrics will be calculated after submission. Another commenter suggested removing expected metrics from the specification sheets and only focusing on counts or metrics to be collected by health IT developers.

Response. To reduce confusion, we have replaced the terms ''numerator'' and ''denominator'' with ''metric'' throughout the Insights Condition. Numerator and denominator were terms meant to identify how the metrics would be used to generate various statistics, but given the confusion expressed through public comments related to these terms, we have simplified and replaced these terms. Thus, instead of a list of numerators and denominators that would be submitted, health IT developers shall be responsible for submitting a list of metrics. This applies across all the finalized measures. This represents a change in terminology and does not represent a substantive change. Developers of certified health IT are responsible for reporting on the metrics, not calculating the derived statistics. We would like to reiterate that ONC will be responsible for calculating any derived statistics from the reported metrics using various combinations of the metrics (previously known as numerators and denominators). In other words, this final rule focuses on listing the metrics that developers of certified health IT would be collecting and reporting, rather than the derived statistics which ONC will calculate.

Comments. Some commenters requested clarification on the information that would be required for submission by health IT developers. One commenter requested ONC establish detailed, clear, and consistent specifications for reporting and attestation under the Insights Condition.

Response. As stated earlier in this preamble and in the HTI–1 Proposed Rule (88 FR 23832), we explored various pathways on how to make it easier for the public to view the detailed technical specifications supporting the measures. We determined that measure specification sheets were a logical and accessible method for the public to view the technical specifications supporting those requirements in a clear and consistent manner and that measure specification sheets have been used successfully by other agencies such as CMS for detailing their measures. The information in this preamble and in the measure specification sheets provides the list of metrics and specifications for reporting and attestation under the Insights Condition. We intend to provide up to date measure specification sheets to assist with the community's understanding of the finalized measures and metric calculations. The measure specifications provide granular definitions and other information needed to operationalize the metrics to ensure they are implemented in a consistent manner across health IT developers. The updated measure specification sheets that reflect the final set of metrics will be available for download and viewing on ONC's website at *www.healthit.gov/hti-1.* We believe that the measure specification sheets provide a more user-friendly format that is more easily accessible. For example, given that not all metrics may be applicable to all health IT developers, developers can select which metrics they wish to review and download. We also intend to publish educational materials on ONC's website that include graphics and other visual displays to help explain the metrics and the reporting process.

Measurement Area: Individual Access to Electronic Health Information

In the HTI–1 Proposed Rule, we proposed in § 170.407(a)(1) a measure within the individuals' access to their EHI measurement area to require that any developer of certified health IT with Health IT Modules certified to the criteria specified in the measure to report on the different methods individuals use to access their health information. We refer readers to the HTI–1 Proposed Rule (88 FR 23833) for detailed background associated with the ''individuals' access to electronic health information supported by certified API technology'' measure.

Comments. Many commenters expressed support for the proposed

measure noting the importance of patients' engagement in their own healthcare and the need to further understand how individuals access their health data. Most commenters indicated support of the general intent and focal points of the proposed measure, while including recommendations to simplify the measure. Some commenters indicated this measure would pose a high level of burden, particularly related to encounter-based metrics. Another commenter stated the proposed measure should not present a significant regulatory burden as the data can be collected in real-time using established technologies.

Response. We have made revisions in response to public comment in an effort to reduce burden and simplify reporting as further described below. We note for readers that we have revised some of the measure names (including the name of this measure, which we updated to individuals' access to electronic health information through certified health IT) for additional clarity and consistency. The revisions to the measure names do not inherently reflect substantive changes to the measure. We have used the phrase ''certified health IT'' across our measures to provide clarity and consistency across the Program. We thank commenters for expressing support for the proposed measure and agree that it will contribute valuable insight into the methods that individuals use to obtain access to their EHI. This information can help ONC and others build an understanding of where EHI is available for usage so that individuals can make informed decisions about their healthcare.

Individuals' Access to Electronic Health Information Through Certified Health IT Measure

We proposed (88 FR 23833) to adopt the ''individuals' access to electronic health information supported by certified API technology'' measure within the ''individuals' access to electronic health information'' area in sect; 170.407(a)(1). We proposed (88 FR 23833 and 23834) to require that any developer of certified health IT with Health IT Modules certified to either the ''view, download, and transmit to a 3rd party'' certification criterion (§ 170.315(e)(1)), or the ''standardized API for patient and population services'' certification criterion (§ 170.315(g)(10)), report the numbers of unique patients that used each of the specified methods to access their EHI.

We proposed two distinct numerators and three denominators as part of the measure (88 FR 23834) in § 170.407(a)(1) and noted that we planned to generate multiple metrics from a combination of different numerators and denominators. We proposed (88 FR 23834) the first numerator to be the number of unique individuals who had an encounter and accessed their EHI at least once during the reporting period via at least one of three types of methods: (1) third-party app using technology certified to ''standardized API for patient population services'' certification criterion under § 170.315(g)(10); (2) patient portal using technology certified to the ''view, download, and transmit to 3rd party'' certification criterion under § 170.315(e)(1) only; or (3) app offered by the health IT developer or health care provider using technology certified to the API criterion under § 170.315(g)(10) (if applicable). We proposed (88 FR 23834) a second numerator to be the number of unique individuals who accessed their EHI regardless of an encounter during the reporting period using at least one of the same three types of methods identified above. We stated that each of these numerators would be stratified or reported by type of method. For detailed background on the proposed measure, we refer readers to the HTI–1 Proposed Rule (88 FR 23834).

We proposed (88 FR 23834) the first denominator for this measure to be the total number of unique individuals who had an encounter during the reporting period. We proposed (88 FR 23834) the second denominator to be the total number of unique individuals who used at least one of the types of methods referenced above to access their EHI who had an encounter during the reporting period. We proposed (88 FR 23834) the third denominator to be the total number of unique individuals who used at least one of the three types of methods referenced above to access their EHI during the reporting period (regardless of whether the individual had an encounter or not).

Comments. Commenters representing EHR developers stated that the proposed measure would result in medium to high qualitative ratings of burden, particularly for the encounter-based measures, and shared suggestions to modify its structure. Several commenters representing health IT developers recommended separating the measure into two measures: (1) a measure applicable to Health IT Modules certified to the § 170.315(g)(10) criterion; and (2) a measure applicable to Health IT Modules certified to the § 170.315(e)(1) criterion. These commenters also expressed concern that the structure of the measure did not align with product level reporting and could create issues and inconsistencies in reporting and interpreting its results. These commenters further stated that many Health IT Modules are certified either to § 170.315(g)(10) or 170.315(e)(1), but very few are certified to both. They suggested that ONC revise the measure to report on patient access (view, download, and transmit) via patient portal versus FHIR via apps and reported at the developer level.

Commenters also recommended removing the third access method that was proposed in the HTI–1 Proposed Rule (88 FR 23834) referred to as ''App offered by the health IT developer or health care provider using technology certified to the API criterion under § 170.315(g)(10) (if applicable).'' They explained that, per the API Condition and Maintenance of Certification requirements, developers of certified Health IT Modules shall treat all (similarly situated) app developers as the same. Therefore, they would be unable to distinguish whether an app is offered by a developer of certified health IT or by a health care provider. Two commenters stated that they would be able to distinguish between access via apps that they developed versus others, but they did not see the relevance of it.

Commenters also requested clarification on the measure structure for numerators and denominators.

Response. We appreciate the assessment from commenters on the level of effort to develop this measure. Considering the medium to high burden ratings from health IT developers that commented on the measure, we have made three modifications intended to simplify and reduce the burden of implementing the measure while establishing a starting place for initial reporting that can be expanded in the future.

First, given that commenters indicated that it would be difficult to distinguish whether an app is offered by a developer of certified health IT or by a health care provider, we have removed the third method of access to EHI from the measure that we had proposed in the HTI–1 Proposed Rule (88 FR 23843), referred to as, ''App offered by the health IT developer or health care provider using technology certified to the API criterion under § 170.315(g)(10) (if applicable).'' Second, we have simplified the metrics (formerly referred to as numerators and denominators) by removing the stratification related to methods of access, and instead incorporated the stratification in the metrics. This now aligns the metrics to each associated criterion and addresses the concern that very few Health IT Modules are certified to both criteria

(§ 170.315(g)(10) or § 170.315(e)(1)). Third, as suggested by commenters, we have removed the metrics related to encounters from this measure. We acknowledge that health IT certified to one criterion only, particularly to § 170.315(g)(10), would not be able to report encounters. By removing the requirement around unique individuals with encounters, we expect that developers of products certified to only one criterion will be able to report access to EHI via the applicable method. We also finalized this measure without encounter-based metrics as we considered how an encounter-based measure would apply to health IT developers who offer and implement integrated systems across ambulatory and inpatient settings, as well as developers who offer and implement only ambulatory systems and only inpatient systems. For developers offering integrated systems, an individual might have an ambulatory visit and an inpatient visit within the reporting period and access their EHI. However, the proposed construction of the encounter-based metrics would have required developers to determine the unique individuals and reconcile their encounters and EHI access across ambulatory and inpatient value sets, which would be a complex endeavor. Therefore, this measure does not include encounter-based metrics in efforts to reduce both complexity and burden of implementing the measure.

We will use a third metric, which counts the number of unique individuals who access their EHI during the reporting period using any method, to assess trends in individuals' use of the two methods of access. This will allow ONC to evaluate as developers of certified health IT continue to make more APIs available under § 170.315(g)(10), and it will also provide insight into individuals' use of methods beyond those required for certification that are facilitating patient access to their electronic health information.

Comments. A commenter requested clarification on whether individuals were expected to have both an encounter during the reporting period and access their EHI during the reporting period, or whether the reporting period refers only to the encounter. The commenter also requested clarification on whether the individual has ever accessed their EHI should be counted. A couple of commenters expressed concern about whether deduplication is expected, noting that most denominators and numerators are feasible if developers of certified Health IT Modules are not expected to deduplicate individuals' access counts. They suggested ONC should either change counts to be transaction-based and avoid unique patient measurement, or clarify that unique patient count will be unique only within each instance of the EHR software and cannot be deduplicated across instances.

Response. We have revised the encounter-based approach for the measure so that encounters are no longer included. With regards to the concern related to deduplication, we require unique patient counts of access during the reporting period. However, we recognize that the counts would only be unique within each instance of the EHR software. To clarify, the measure should report on whether individuals accessed their data during the reporting period; this is not a measure of an individual ever accessing their EHI.

Comments. Several commenters requested that ONC clearly state whether the scope is for patients accessing their own records, exclusive of authorized representative access events. Most commenters requested that the measure not include access by authorized representatives. One commenter requested that ONC should include access by an individual's authorized representative in the measure count.

Response. We thank commenters for their feedback on whether patient-authorized representatives should count in the measure when they access EHI and note that there was no consensus. While we agree with the commenter suggesting that ONC should include access by an individual's authorized representative, we did not propose this distinction for our measure. As such, we may incorporate patient-authorized representatives in future rulemaking, noting that it would be beneficial to align this measure with the CMS Promoting Interoperability (PI) Measure for patient access, which similarly counts patients and their authorized representative in the numerator for providing access to patient-authorized representatives for view, download, and transmit (VDT), and apps of the patients' choice.[194] The finalized measure only counts individuals.

Comments. We received comments indicating the need to clarify the definition for access to EHI. Some commenters sought further clarification on the proposed methods of portal and API access for this measure. One commenter asked, in cases where the patient portal may display several electronic health information elements on the log-in landing page, if such a scenario counts as a patient accessing their EHI via a patient portal. One commenter asked whether patient portal access should count any use of the patient portal or specifically a view, download, or transmit to a 3rd party activity. Regarding individual access via a developer's app, a commenter requested clarity on whether an app using different technology than what is included in § 170.315(g)(10) should be counted. For an API, one commenter requested clarity on whether the measure should record the submission of a request for information or the response to the request.

Response. We appreciate the opportunity to clarify how access to EHI is defined for the finalized measure. The definitions associated with this measure (as noted earlier) are described in detail in the measure specifications. Access to EHI via patient portal using technology certified to the ''view, download, and transmit to 3rd party'' certification criterion under § 170.315(e)(1) is counted as a patient log-in with the access credential belonging to the individual at least once during the reporting period. Access to EHI via technology certified to the ''standardized API for patient population services'' certification criterion under § 170.315(g)(10) is counted as the individual's authorization, as indicated by an access token, at least once during the reporting period. To summarize, access to EHI is based upon an individual logging into a system (whether that be a portal or third-party app or other system) within the reporting period and is not based on accessing any specific piece of information or performing any specific action within the system itself such as view, download and transmit activities.

Comments. We received some comments suggesting expanding the proposed measure. One commenter suggested that the data should report on whether individuals are accessing their health information more than once in the same reporting period. Another suggested that the data should report those individuals who tried to access their health information via the proposed methods and failed. Another commenter suggested reporting ''percentage of use'' similar to what was proposed for the ''use of FHIR bulk data access through certified health IT'' measure to measure the adoption of API-based means of access by single users in a developer's client base. One commenter noted that the most common

[194] CMS. 2022 MEDICARE PROMOTING INTEROPERABILITY PROGRAM FOR ELIGIBLE HOSPITALS AND CRITICAL ACCESS HOSPITALS. Provider to Patient Exchange Objective Fact Sheet *https://www.cms.gov/files/document/2022-provider-patient-exchange-objective-fact-sheet.pdf.*

method for authenticating users of third-party health apps is via their patient portal account and that some patients may only use their portal to access their app of choice. They suggested ONC provide an additional metric to determine whether the portal is being used to access health information directly or to access health information via a third-party app. Finally, one commenter suggested collecting additional data for this measure to support health equity, suggesting the measure include a patient's language.

Response. We appreciate comments suggesting expanding the measurement of individual access to EHI and agree that there are several important dimensions of access to EHI to explore. Given that we also received numerous comments related to the burden associated with reporting the current proposed measures, we have not added the suggested additional requirements at this time, though they may provide further insights. Our intent is to balance the value of the information we now require to be collected with the burden of doing so. We may consider these suggestions in future iterations of the measure through rulemaking.

Comments. One commenter expressed concern and requested clarification about how the measure may reflect on the quality of a developer of certified Health IT Modules' products. The commenter stated that health care providers have the relationships with patients and provide the instructions to access their health information, while developers have no influence on these activities.

Response. We acknowledge that there are many factors that influence how and to what degree individuals access their EHI, including those mentioned by commenters. While the results do not solely reflect on the performance of the health IT developers, the methods health IT developers provide to access EHI may vary in usability, implementation of functionality, and robustness of functionality, which may influence patient and provider use of EHI. The measure intends to shed light on the role that health IT plays in facilitating access to EHI through different methods.

Comments. One commenter asked about the entity that would be responsible for reporting on the measure in a situation where the health IT developer relies upon a different certified Health IT Module (owned by a separate entity) in order to meet the certification criteria associated with the Insights Condition (in this case § 170.315(e)(1). Specifically, the commenter sought clarity on whether the developer of the certified health IT module using the relied upon software would be responsible for reporting, or if the developer of that relied upon software would be responsible for reporting.

Response. We appreciate the request for clarification. In these instances, similar to how this is addressed through the Real World Testing requirements,[195] we would expect a health IT developer using relied upon software in its Health IT Module to meet the certification requirement associated with § 170.315(e)(1) to report on this Insights Condition measure on its own accord. The health IT developer may work with its relied upon software vendor, if necessary, to report on the metrics.

Finalization of Measure

We have finalized the measure as ''individuals' access to electronic health information through certified health IT'' in § 170.407(a)(3)(i). We have revised the proposed measure based on public comments received. Specific metrics to support this finalized measure are listed below and described further in the accompanying measure specification sheets located on ONC's website. We also note that if regulatory baselines associated with the metrics change in the future—such as a revision to a criterion through notice and comment rulemaking—the measure specification would also be changed to ensure alignment with the revised criterion. The reporting period for the measure and related metrics below consists of one calendar year. Data collection for the measures and associated metrics will begin during the first phase of reporting (which is described later in the preamble):

(1) Number of unique individuals who accessed their EHI during the reporting period using technology certified to the ''standardized API for patient population services'' certification criterion under § 170.315(g)(10).

(2) Number of unique individuals who accessed their EHI during the reporting period using technology certified to the ''view, download, and transmit to 3rd party'' certification criterion under § 170.315(e)(1).

(3) Number of unique individuals who accessed their EHI using any method. The methods are not limited to third-party apps using technology certified to ''standardized API for patient population services'' certification criterion under § 170.315(g)(10) or patient portals using technology certified to the ''view, download, and transmit to 3rd party'' certification criterion under § 170.315(e)(1) during the reporting period.

Measurement Area: Clinical Care Information Exchange

In HTI–1 Proposed Rule (88 FR 23834), we proposed two measures under the ''clinical care information exchange'' area in § 170.407(a)(2) and (3) titled, ''C–CDA documents obtained using certified health IT by exchange mechanism'' and ''C–CDA medications, allergies, and problems reconciliation and incorporation using certified health IT.'' These measures primarily focused on characterizing the state of information exchange between health care providers who are customers of health IT developers with certified health IT, in contrast to other measures that capture exchange with individuals, public health agencies, and other entities.

Comments. Numerous commenters indicated general support for both clinical care information exchange measures. Commenters representing health care providers valued the reconciliation and incorporation measure because effective reconciliation and incorporation of medication, allergy, and problem information through certified health IT benefits patient safety and care coordination. Some commenters suggested that examining volume alone would not be a good indicator of interoperability advancement or quality. Rather, measures that focus on the efficiency of reconciliation in combination with volume measures would provide better insights into the advancements in interoperability. One commenter suggested removal of both measures.

Response. We appreciate the support expressed for both clinical care exchange measures. We believe measuring volume is important as it provides the means to assess the extent that patient information is moving between providers to facilitate high value care. Furthermore, patient and encounter volume measures help contextualize and interpret other measures designed to assess progress related to interoperability. Current measures to understand the magnitude of information exchange and use are fundamentally limited. For example, as noted in the HTI–1 Proposed Rule (88 FR 23835), publicly available information from some health information networks can be difficult to interpret without also knowing the

[195] ONC Health IT Certification Program. Real World Testing Guide. (Last updated: May 23, 2023). See p. 18. *https://www.healthit.gov/sites/default/files/page/2021-08/ONC-Real%20World%20Testing%20Resource%20Guide_Aug%202021.pdf.*

number of encounters occurring at sites using these methods, the number of patients being treated, and other measures of volume. Measures intended to provide insight into the volume of information exchanged across the nation are not feasible to collect from end users through clinical surveys, and the CMS PI Program measure is reported by a subset of providers that participate in that program.

We agree with commenters that measures of efficiency and effectiveness of health IT to support deduplication and reconciliation alongside measures of volume of clinical care documents received and incorporated will provide valuable insight on interoperability trends. Both measures are discussed more fully below.

Consolidated Clinical Document Architecture (C–CDA) Documents Obtained Using Certified Health IT by Exchange Mechanism Measure

We proposed (88 FR 23834 and 23835) to adopt the ''C–CDA documents obtained using certified health IT by exchange mechanism'' measure in § 170.407(a)(2). We stated that this measure would report on the volume of C–CDA documents obtained using certified health IT by exchange mechanism relative to patient volume, and that a developer of certified health IT with Health IT Modules certified to the ''clinical information reconciliation and incorporation'' certification criterion in § 170.315(b)(2) would be required to report the proposed numerators and denominators for this measure. We refer readers to the HTI–1 Proposed Rule (88 FR 23834 through 23836) for detailed background on the proposed measure.

We proposed four numerators and four denominators for this measure (88 FR 23835). We noted in the HTI–1 Proposed Rule (88 FR 23835 and 23836) that we planned to generate multiple metrics from different combinations of these numerators and denominators. We proposed to adopt the following numerators for this measure: (1) number of unique C–CDA documents obtained (which we defined for the purpose of this proposal as either C–CDAs that are received—that is, C–CDAs that have been sent or 'pushed' by others and received using certified health IT or C–CDAs that are queried—that is, C–CDAs that were found or 'pulled' from a network or central repository using certified health IT) using certified health IT and Direct Messaging during the reporting period; (2) number of unique C–CDA documents obtained (received or queried) using certified health IT and a local/regional health information exchange (HIE) or national health information network (HIN) during the reporting period; (3) number of unique C–CDA documents obtained (received or queried) using certified health IT and a developer-specific HIN (*i.e.,* a network that facilitates exchange between entities using the same health IT developer's products) during the reporting period; and (4) number of unique C–CDA documents obtained (received or queried) using certified health IT and a method not listed above and not including electronic fax during the reporting period.

We proposed (88 FR 23835) to adopt the following denominators for this measure: (1) number of encounters during the reporting period; (2) number of unique patients with an encounter during the reporting period; (3) number of unique patients with an associated C–CDA document during the reporting period; and (4) number of unique C–CDA documents obtained (received or queried) using certified health IT during the reporting period. We proposed (88 FR 23835) to include denominators for the number of encounters during the reporting period and the number of unique patients seen (*i.e.,* with an encounter) during the reporting period to provide a sense of the volume of C–CDA documents exchanged relative to the number of instances when a C–CDA document might be useful.

Comments. While numerous commenters expressed general support for this measure, some commenters raised concerns. Their major concerns related to: (1) burden associated with the measure and the overall program; potentially including health care providers as they may need to map their exchange partners to different types of networks for reporting purposes; (2) rethinking the mechanisms which include a mix of methods and standards that are not mutually exclusive; (3) measuring beyond standards that reflect the current state such as FHIR, which may become dominant in the future; (4) better defining and specifying the selected exchange mechanisms; and (5) potentially including mechanisms that do not result in structured, interoperable data, such as e-fax, to more fully measure the totality of exchange, including exchange across the care continuum with providers who do not possess electronic exchange capabilities.

Response. We thank commenters for their feedback and agree with the concerns raised by commenters related to the potential burden of some metrics, including impacts on providers, the need to reduce overall burden associated with the Insights Condition, and the ability to meaningfully distinguish between the proposed exchange mechanisms given the overlap between the use of standards and methods of exchange. Therefore, we have not finalized the ''C–CDA documents obtained using certified health IT by exchange mechanism'' measure. Although we value measuring exchange mechanisms, the ecosystem for HIE methods is evolving, particularly with the launch of TEFCA. The evolving landscape for exchange calls for a measure that tracks trends related to the adoption and use of each mode of exchange to better inform ONC's policy making and health care providers' operational decisions. We may consider proposing a revised version of this measure in a future rulemaking with the intent of capturing trends in how clinical information is being exchanged, inclusive of FHIR-based exchange.

Consolidated Clinical Document Architecture (C–CDA) Problems, Medications, and Allergies Reconciliation and Incorporation Through Certified Health IT Measure

We proposed (88 FR 23836) to adopt the ''C–CDA medications, allergies, and problems reconciliation and incorporation using certified health IT'' measure in § 170.407(a)(3), which would capture the number of C–CDA documents that are reconciled and incorporated (as defined in § 170.315(b)(2)(iii)) as part of a patient's record by clinicians or their delegates. We proposed (88 FR 23836) that a developer of certified health IT with Health IT Modules certified to the ''clinical information reconciliation and incorporation'' certification criterion in § 170.315(b)(2) would be required to provide information on how data in C–CDA documents are used, focusing on the reconciliation and incorporation of medications, allergies and intolerances, and problems.

We proposed (88 FR 23836) the numerator to be the total number of C–CDA documents of the Continuity of Care Document (CCD), Referral Note, Discharge Summary document types that are obtained and incorporated across all exchange mechanisms supported by the certified health IT during the reporting period. The numerator would increment, or increase in number, upon completion of clinical information reconciliation of the C–CDA documents for medications, allergies and intolerances, and problems, as described in the certification criterion in § 170.315(b)(2).

We proposed (88 FR 23836) the denominators for this measure, using

the definition of ''encounter'' described earlier in the preamble of the HTI–1 Proposed Rule (88 FR 23832), as the following: (1) number of encounters during the reporting period; (2) number of unique patients with an encounter during the reporting period; (3) number of unique patients with an associated C–CDA document during the reporting period; and (4) number of unique C–CDA documents obtained using certified health IT during the reporting period. For this fourth denominator, we indicated that we were aware that in the current landscape, some clinicians and hospitals are able to receive C–CDA documents through multiple methods and it is possible to receive multiple copies of the same C–CDA (*e.g.,* via Direct Messaging and an HIE). We sought to only include unique C–CDA documents in both the numerator and denominator because we believed that clinicians were unlikely to reconcile multiple copies of the same C–CDA and that by eliminating these duplicates, we would avoid undercounting reconciliation (88 FR 23837).

Comments. Several commenters who indicated general support for the measure also expressed concerns about the burden associated with the measure. These commenters noted that their reports for clients on a similar measure for the CMS PI Program do not necessarily create efficiencies in aggregating the data across their clients. One commenter indicated the value of the measure did not outweigh the burden because many of their clients do not regularly reconcile and incorporate documents they obtained.

Commenters representing EHR developers also provided qualitative ratings of burden associated with these measures. They indicated that the data points (*e.g.,* numerators/denominators) ''number of encounters'' and ''number of unique patients with an encounter'' would be low level of effort; whereas ''number of unique patients with an associated C–CDA document'' and ''number of C–CDA documents of the Continuity of Care Document (CCD), Referral Note, Discharge Summary document types that are obtained and incorporated across all exchange mechanisms'' would be a high level of effort. The rest of the clinical care exchange numerators and denominators were rated as medium level of effort. The commenter expressed that the ''number of unique patients with an associated C–CDA document'' was rated as high in burden because greater clarification was needed related to what the term ''associated'' meant.

Response. We appreciate the feedback from commenters. In response to public comments, we have revised metrics to reduce burden associated with the measure as further discussed in this section below. We appreciate that aggregating data across clients at the product level requires additional effort even if the incorporation and reconciliation measure is similar to the CMS PI measure, but we maintain that the existence and use of the similar data structures to generate reports for clients creates efficiencies for developers relative to the counterfactual, in which no such data structures currently exist. We believe the measure will provide value commensurate with the burden described by commenters. As noted earlier, commenters representing health care providers expressed value in the proposed incorporation and reconciliation measure. If providers are not engaging in these activities, it would be useful to make that information more widely known to healthcare organizations, payers, and other interested parties involved with patient safety through this measure. Providers may find the measures useful to evaluate their workflows and health IT configuration to optimize functionality that supports incorporation and reconciliation.

The version of the metric included in the measure specification is described in more detail below and in the measure specification itself. We have included the following metrics described at 88 FR 23835 in the measure specification: number of encounters during the reporting period, number of unique patients with an encounter during the reporting period, and number of unique patients with an associated C–CDA document during the reporting period. These metrics are included as described at 88 FR 23835, except for a revision to the measure of encounters described further in this preamble.

We have revised the metrics, ''number of unique C–CDA documents obtained (received or queried) using certified health IT during the reporting period'' (88 FR 23835) and ''the total number of C–CDA documents of the Continuity of Care Document (CCD), Referral Note, Discharge Summary document types that are obtained and incorporated across all exchange mechanisms through the certified health IT during the reporting period'' (88 FR 23836) to better capture how health IT functions and to reduce requirements specific to the Insights Condition. The revisions are further described later in this section.

Comments. Numerous commenters requested clarification on whether duplicate documents should be counted and asked how duplicates should be defined. Some commenters recommended that all documents be counted, whether duplicative or not, because all documents must be managed. Furthermore, one commenter recommended that ONC require that all documents are counted, whether considered duplicates or not, because whether documents are duplicates or not, all must be processed, deduplicated, and reconciled. Comments also indicated that deduplication may not be necessary if the intended purpose is to examine trends over time. Commenters noted that there is not necessarily industry consensus on what it means for information to be duplicative. Numerous commenters noted that examining the full content of documents to verify if documents are duplicates may not be feasible. Most commenters indicated that ONC should limit its definition to duplicates based upon document identifiers as that was the most feasible option, though these commenters acknowledged that relying on document identifiers alone to identify them may not fully capture all duplicative documents.

Response. We appreciate the input from commenters on how the measures should manage duplicate C–CDAs. In response to feedback, the approach to identifying duplicate C–CDAs to support metrics related to unique C–CDA documents, as included in the measure specifications accompanying the HTI–1 Proposed Rule, has been revised. We have removed the requirement for health IT developers to identify C–CDAs that ''otherwise contain substantially identical data as identified by developers of certified health IT.''[196] In the measure specification accompanying this final rule, we have provided a definition for ''unique C–CDAs'' so that duplicate C–CDAs shall be identified based upon document identifier only, and only one of multiple C–CDAs with the same document identifier will be included in a count of unique C–CDAs. For example, if an HIE receives a C–CDA from a health care provider and regenerates the C–CDA, the content of the document does not change, but the document may have a new document ID. In this instance, we will not require health IT developers to undertake the effort to analyze the content to determine if it is identical to the original C–CDA's content, and we recognize that

[196] ONC Health IT Certification Program Insights Condition: Consolidated Clinical Document Architecture (C–CDA) Medications, Allergies, and Problems Reconciliation and Incorporation Using Certified Health IT *https://www.healthit.gov/sites/default/files/2023-04/3.Measure_Spec_CCDA_Reconcile_1.3.pdf.*

C–CDAs containing identical information would not be counted as a duplicate if they have different document IDs.

We agree with the commenters who highlighted the work necessary to process, deduplicate, and reconcile both non-duplicative and duplicative C–CDAs, and the importance of capturing the totality of all C–CDAs processed. In response to this comment, we have added a metric as the number of total C–CDA documents obtained, inclusive of potential duplicate documents as described in the measure specification. This reflects the totality of documents measured by health IT developers, irrespective of document identifier. This metric relates directly to the proposed metric ''number of unique C–CDA documents obtained using certified health IT during the reporting period'' (88 FR 23835) and would represent the count of C–CDAs before deduplication processes were applied. Given the substantial comments we received on the deduplication process as described in the measure specification, we believe that this permutation on the underlying metric was both anticipated by and supported by public comment.

We have also retained the metric counting the unique number of C–CDAs and have made a revision by modifying the approach to identifying duplicate C–CDAs underlying this metric. The metric, as described in the measure specification accompanying the final rule, is the number of unique C–CDA documents obtained. We clarify that unique C–CDAs are identified by document ID and only one of multiple C–CDAs with the same document identifier counted. This metric relates directly to the proposed metric following revision of the deduplication process. The difference between these two metrics represents the volume of duplicate C–CDAs obtained, determined by document ID. This is critical to track as health care providers have identified the potential negative downstream impacts of duplicate documents exchanged on the complexity of exchange and usability of the data.

Comments. Numerous commenters indicated that the proposed metric did not explicitly include important automated aspect of the reconciliation process, which includes deduplication through automated means. Commenters pointed out that reconciliation by human users can be assisted by underlying automation and that there was variation in these practices. For instance, as noted above, commenters expressed concern that there was not industry consensus on how to deduplicate information contained within a C–CDA. The HITAC specifically noted that new tools and automated processes are advancing to reduce the human burden involved in reviewing exchanged information.[197] Numerous commenters also noted that the measure is specifically based on reconciliation actions occurring at the C–CDA document level, whereas many developers aggregate data across individual documents for consolidated or ''bundled'' clinical reconciliation for a more user-friendly workflow to deduplicate C–CDAs. Commenters noted the measure should be modified to better account for bundled reconciliation, and that doing so would align this measure further with the CMS PI Program measures. Numerous commenters recommended that ONC include documents reconciled not only by human users, but those documents automatically reconciled via electronic tools that reduce the need for manual review and reconciliation of data. A commenter expressed that the metric was rated as high in burden because auto-reconciliation was not included in the proposed measure.

Response. We appreciate considerations from commenters on the range of evolving practices to automate and support reconciliation and incorporation of C–CDAs, which can reduce burden on end-users. As noted above, given this range of practices, we have specified in the measure specification accompanying this final rule that the identification of unique C–CDAs for the purpose of the Insights Condition depends only on document identifier.

In proposing within the measure specification to define duplicates based on the inclusion of substantially identical information as identified by health IT developers, we intended to reflect what we understood to be wide variation in developers' approaches to determining whether information was duplicative.[198] However, public comments further highlighting variation in approaches to deduplication, particularly automated processes to do so, coupled with comments about similar automated processes that some developers use to reduce burden, indicate that it is essential to measure automated processes to meaningfully capture how information in C–CDAs is used. Without including metrics on these processes, we believe the metrics as proposed may have led to invalid inferences. For instance, the proposed metrics may have inappropriately conflated fully automated processes identifying no new information with processes involving clinician review and resulting in new information incorporated into the Health IT Module. This was confirmed by commenters indicating that it might be infeasible or of little value to implement the proposed metrics in cases where documents were bundled or otherwise pre-processed.

We further agree with commenters that changes in health IT systems that reduce provider burden are vital. The metrics described in the measure specification accompanying the final rule will facilitate insight into the extent to which health IT systems employ automated processes to streamline reconciliation and incorporation of clinical information and result in greater use of information in C–CDAs and reduced burden. As a result, the measure will properly reflect the success of developers with approaches that create efficiency for the healthcare delivery system.

To support the final measure and to capture the range of methods that support the reconciliation and incorporation process, we use several terms in the measure specification sheets accompanying the final rule. For purposes of clarity, we note the terms have the following meanings:

- ''Pre-Processes for Reconciliation and incorporation'' is any automated process that (1) deduplicates C–CDAs, for instance, based on document identifier, the information contained within multiple C–CDAs, or other means; (2) removes information for user review that is identical to information in the Health IT Module; (3) aggregates data across documents for bundled reconciliation; or (4) uses another means to process C–CDAs to facilitate manual (by a clinician or their delegate) or fully automated reconciliation and incorporation of information into the Health IT Module.
- ''Reconciled and Incorporated via Any Method'' is any approach to reconciling and incorporating information in the Health IT Module, including but not limited to manual processes performed by a clinician or their delegate only; a mix of manual and automated processes; or fully automated

[197] HITAC recommendation: HTI–1–PR–TF–2023_Recommendation 33 in Recommendations on the Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing (HTI1) Proposed Rule *https://www.healthit.gov/sites/default/files/page/2023-06/2023-06-15_HTI-1-PR-TF-2023_Recommendations_Report_Final_508.pdf.*

[198] ONC Health IT Certification Program Insights Condition: Consolidated Clinical Document Architecture (C–CDA) Medications, Allergies, and Problems Reconciliation and Incorporation Using Certified Health IT *https://www.healthit.gov/sites/default/files/2023-04/3.Measure_Spec_CCDA_Reconcile_1.3.pdf.*

processes. This includes an affirmative action to (1) reconcile new information from the C–CDA into the Health IT Module, for instance, by comparison of medication information in the Health IT Module and information in the C–CDA; or (2) indicate that no new information needs to be incorporated into the Health IT Module.

- ''Fully automated processes for reconciliation and incorporation'' is any process by which problems, medications, or allergies and intolerances contained within C–CDAs are automatically reconciled with information within certified health IT and incorporated into health IT without an action by a clinician end-user or their delegate. These processes include (1) reconciling new information from the C–CDA into the Health IT Module, for instance, by comparison of medication information in the Health IT Module and information in the C–CDA; or (2) determining that no new information needs to be incorporated into the Health IT Module.
- ''Determined to have no new problems, medications, or allergies and intolerances information'' is any pre-process or fully automated process that determines that the C–CDA contains no new information.

In consideration of public comment received on the proposed measure, we have included more specific metrics in the measure specification accompanying the final rule. Three metrics account for pre-processes and fully automated processes related to reconciling and incorporating C–CDAs and two more clearly framed metrics related to C–CDAs for which automated processes were not applied. We made these adjustments to better reflect developers' existing practices related to deduplication and similar pre-processing, including the bundling of C–CDAs described in public comment on the HTI–1 Proposed Rule and accompanying measurement specification. In contrast to the original measure in the HTI–1 Proposed Rule, we have not finalized a requirement that any complex deduplication be performed specifically for the Insights Condition by those developers who do not currently deduplicate or otherwise automatically process C–CDAs, which will result in reduced burden on developers.

In so doing, we believe the updated metrics represent a direct evolution of the focus in the HTI–1 Proposed Rule on deduplication that is responsive to comments and reduces burden on developers. To that end, in the measure specification accompanying this final rule, we sub-divided the proposed metrics to more precisely capture rates of pre-processes and fully automated processes described by commenters.

- In addition to the metric, number of unique C–CDA documents obtained, we have also included two metrics to enable the proper and accurate capture of the use of pre-processing that may facilitate efficient and effective review of information contained within C–CDA documents: (1) number of total C–CDA documents obtained that were pre-processed, and (2) number of total C–CDA documents obtained that were not pre-processed. Following the change to what constitutes a duplicate C–CDA previously discussed, the number of unique C–CDAs will reflect elimination of an important subset of duplicate C–CDAs, but will not reflect more complex deduplication processes. The complementary metrics reflect the extent that developers performed pre-processes, inclusive of those deduplication processes, for obtained C–CDAs. This approach eliminates the need to perform specific, complex deduplication processes for the Insights Condition and the final metrics should decrease developer burden compared to what was proposed. We expect that some developers that do not have the capability to pre-process C–CDAs would report a zero for the first metric.
- We have divided the proposed metric ''number of C–CDA documents of the Continuity of Care Document (CCD), Referral Note, Discharge Summary document types that are obtained and incorporated across all exchange mechanisms supported by certified health IT during the reporting period'' into two metrics to more clearly differentiate between reconciliation activities that were and were not supported by pre-processes: (1) number of total C–CDA documents obtained that were pre-processed where problems, medications, or allergies and intolerances were reconciled and incorporated via any method; and (2) number of total C–CDA documents obtained that were not pre-processed where problems, medications, or allergies and intolerances were reconciled and incorporated via any method. This division was made in response to public comment requesting that we specify how the proposed metrics accounted for pre-processing and requesting that we reduce the complexity of C–CDA processing necessary, specifically for the Insights Condition. We expect that some developers that do not have the capability to pre-process C–CDAs would report a zero for the first measure.

Finally, we have included a specific standalone metric to capture fully automated processes that did not result in new information. In the proposed measure specification, we stated, ''if no update is necessary, the process of reconciliation may consist of simply verifying that fact or reviewing a record received and determining that such information is merely duplicative of existing information in the patient record.'' We believe that this statement was ambiguous about whether automated processes for making this determination would count as reconciliation, and commenters indicated as much by comparison to the CMS PI measure. Given commenters' interest in highlighting various approaches to processing C–CDAs, we have included a metric focused directly on this process as the number of total C–CDA documents obtained that were determined to have no new problems, medications, or allergies and intolerances information by pre-processes or fully automated processes. This metric is intended to disambiguate how to capture pre-processes and fully automated processes for verifying that no new information was available relative to the measure specification accompanying the HTI–1 Proposed Rule.

We believe this approach will facilitate measurement of C–CDAs that are bundled together prior to end-user review. For instance, if the bundle is not reviewed by a clinician end user or their delegate and information is not automatically reconciled and incorporated, the metric related to reconciling information that has been pre-processed described above would not include C–CDAs that contained new information presented in a bundle. Prior to manual review, C–CDAs that contributed no new information to the bundle could either be counted as contributing to both the metric related to reconciling information that has been pre-processed and the metric related to determining that the C–CDA contained no new information, or to neither metric depending on the approach that most closely matched the product's logic. Once manual review of a bundled C–CDAs is completed, each C–CDA that comprised the bundled review would increment the metric related to reconciling information that has been pre-processed above, and those that contributed no new information to the bundle would increment the metric related to determining that the C–CDA contained no new information as well. We have adopted this approach to acknowledge the health IT systems that have functionality that streamlines the reconciliation process, with the interest

of understanding how this functionality reduces burden for end users. We recognize that today many developers may apply no pre-processes or fully automated processes to obtained C–CDAs, and these developers would report a zero for these metrics.

C–CDA documents obtained via all mechanisms (including from national networks, such as the Carequality framework and CommonWell, Direct Trust, and eHealth Exchange; Health IT Developer networks; EHR to EHR exchange; regional, local, and community HIE; and Direct Secure Messaging) should be counted in the measure. However, we clarify that the measure does not require any stratification by exchange mechanism.

Comments. One commenter raised a concern that it would be difficult to deduplicate patients across EHR instances and thus ONC should clarify that deduplication across EHR instances is not expected.

Response. We appreciate the request for clarification. We recognize that this requirement represents a significant level of burden and do not expect deduplication of patients across EHR instances for this measure.

Comments. Many commenters recommended to include any valid C–CDA R2.1 IG document-level template for measurement, as opposed to only the CCD, Discharge Summary, and Referral Note templates described in the measure specifications sheets related to this measure. Some commenters also noted that including a broader set of document types would better capture the full scope of C–CDA document exchange that is active in healthcare today and aligns with CMS PI Program. Additionally, one commenter representing health IT developers noted it would be less burdensome to include all documents, rather than only the subset, as they did not have the capability to identify the subset. Relatedly, numerous commenters also suggested that we modify the definition for obtaining C–CDAs. Many commenters indicated that excluding C–CDA without any data would be problematic as that would involve reviewing the content of the C–CDA which would be burdensome. One commenter noted that a C–CDA without any data (such as a patient header) would be rejected and not counted. Some commenters suggested including any document received inbound that is in a valid file format with a header indicating that it is a C–CDA R2.1 document template.

Response. In an effort to align with the ''automated measure calculation'' (§ 170.315(g)(2)) criterion that health IT developers follow to support reporting the CMS measures, we have revised the measure specification so that the measure includes any valid C–CDA document-level template referred to in the standards adopted for certification to § 170.315(b)(2) for measurement, as opposed to only the CCD, Discharge Summary, and Referral Note templates. This brings the measure into alignment with the CMS PI Program measure (Support Electronic Referral Loops By Receiving and Reconciling Health Information), which states ''Starting in 2019, for the Promoting Interoperability measure an EP may use any document template within the C–CDA standard for the purposes of the measure.'' We note that this scope is substantially broader than the ''clinical information and reconciliation and incorporation'' (§ 170.315(b)(2)) criterion, which only requires that certified Health IT Modules be able to reconcile and incorporate Continuity of Care Document, Referral Note, and (inpatient setting only) Discharge Summary. We will not require developers to exclude documents without data, acknowledging that some developers do not parse or otherwise pre-process C–CDAs and, therefore, cannot readily evaluate whether the C–CDA contains data. We plan to collaborate with the community to determine if more nuanced levels of analysis are warranted for future measure updates to refine the measure.

Comments. Some commenters asked ONC for clarification on the proposed denominator, ''number of unique patients with an associated C–CDA document during the reporting period.'' One commenter indicated they were not sure how it differed from ''documents obtained'' in one of the other denominators and whether it was intended to only capture new associations that occurred during a reporting period or a snapshot of all patients at the end of the reporting period. One commenter also inquired about how to count a document received during one reporting period but matched in another reporting period.

Response. We clarify that the metric, number of unique patients with an associated C–CDA document during the reporting period, refers to the number of unique patients that have been matched to at least one C–CDA within the certified Health IT Module by automated or manual means in the reporting period and, therefore, have at least one associated C–CDA. The metric, number of total C–CDA documents obtained through certified health IT during the reporting period, refers to the total number of C–CDA documents obtained across all patients for the reporting period. For example, if two C–CDAs were received for a single patient during the reporting period, the first metric would count this as a single unique patient, while the second metric would count this as two C–CDAs. These counts would not depend on whether information had previously been received for a patient prior to the reporting period. As noted in the HTI–1 Proposed Rule, we believe these denominators support an understanding of the volume of C–CDA documents exchanged relative to the number of instances when external information could inform health care providers.

With regard to documents that may be obtained in one reporting period and reconciled in another reporting period, the measure's metrics call for counting C–CDAs obtained, reconciled, and incorporated in the same reporting period. We recognize that some C–CDAs obtained prior to the reporting period, but reconciled and incorporated during the reporting period, are not counted in the metrics. However, we expect these instances will not substantially impact the interpretation of the metrics' results. We also recognize that some C–CDAs obtained during the reporting period may be reconciled and incorporated following the reporting period, but similarly believe these instances will be uncommon. We expect that the shift to calendar year reporting will further minimize the exclusion of documents that are received before the start of a reporting period and reconciled during the start of the reporting period.

Comments. One commenter suggested the encounter-based metrics may not adequately measure one of the key areas of interest, which is to assess the extent to which exchange of outside information can potentially inform care. This commenter suggested that to identify the extent to which encounters benefited from information exchange would require a denominator of total number of encounters during the reporting period, and a numerator of encounters in which information from a C–CDA document was incorporated. Such a measure would provide the percentage of encounters in which outside information was potentially beneficial to the encounter was incorporated from received documents.

Response. We agree with the commenter that many variations on the required metrics could provide additional insight into how exchanged information is used and that measures related to the proportion of encounters in which obtained information was incorporated could be particularly insightful. However, we have sought to

balance that consideration against the potential for additional burden associated with the measure. To that end, we decline to revise or extend measures to capture the proportion of encounters in which information was incorporated. We plan to continue to collaborate with the community to investigate the degree of development necessary to link C–CDAs incorporated to their use to inform care during an encounter.

Comments. Several commenters raised questions regarding what actions count as reconciliation. One commenter requested clarification on whether a document would be considered incorporated if any amount of data was incorporated or by specific data element. A couple of commenters requested ONC be more explicit about what types of data are included for reconciliation, asking whether a document should be included only if it had problems, allergies, or medications (PAM) for reconciliation, or if reconcilable laboratory results (*e.g.,* blood tests) or immunizations should also be included. A commenter requested that ONC limited it to reconciliation of PAM, given that it is a certification requirement, and that the numerator be explicitly defined in that manner. Relatedly, a couple of commenters recommended that if a document did not contain any new information to be reconciled that it should still increment the numerator to match the existing CMS PI measure. Another commenter requested that ONC clarify that viewing documents is not equivalent to reconciling documents.

Response. Our intent is to align the measure requirements with the ''clinical information reconciliation and incorporation'' (§ 170.315(b)(2)) certification criterion. As such, we describe in the measure specification accompanying the final rule that metrics related to reconciliation of C–CDAs would increment upon reconciliation of medications, allergies and intolerances, or problems. The two metrics are: (1) number of total C–CDA documents obtained that were pre-processed where problems, medications, or allergies and intolerances were reconciled and incorporated via any method; and (2) number of total C–CDA documents obtained that were not pre-processed where problems, medications, or allergies and intolerances were reconciled and incorporated via any method. We clarify that the increment occurs when reconciliation is completed for any one of the three types of data, that is, when at least one medication, allergy and intolerance, or problem is reconciled and incorporated or when it is determined that no new information should be incorporated. We agree with the recommendation from commenters that documents that do not contain any new information for reconciliation should still increment the metrics when an end-user or automated process verifies the fact that information in the C–CDA is duplicative of existing information in the patient record to match the existing CMS PI measure. The third metric, number of total C–CDA documents obtained that were determined to have no new problems, medications, or allergies and intolerances information by pre-processes or fully automated processes, would also increment when automated processes were used to make this determination. We believe that distinguishing between automated processes that identify no new information and other reconciliation is important for a valid understanding of the use of information and burden on end-users. We clarify that the act of simply viewing a C–CDA, without an affirmative action verifying that information is either absent or duplicative, would not increment these metrics.

Comments. One commenter suggested focusing measurement on transitions between outside organizations/systems, as patients within health systems are often referred, admitted, and discharged to providers within the same system which might make it difficult to interpret the results.

Response. The measure is intended to count C–CDAs that must be exchanged outside of a ''one patient one chart'' system, where multiple specialists within a system can access a single patient record and manage a single list for problems, medications, and medication allergies. We note that this measure applies to intra-system exchange, where specialists within the same provider organization do not have access to a ''one patient one chart'' health IT system, and inter-system exchange, where specialists across different provider organizations also do not have access to a ''one patient one chart'' health IT system. We also note that this measure is not limited to transitions of care. We may consider if the measure should be reported by transitions of care in future rulemaking.

Finalization of Measure

We have finalized the measure as ''consolidated clinical document architecture (C–CDA) problems, medications, and allergies reconciliation and incorporation through certified health IT'' in § 170.407(a)(3)(ii). We have revised the proposed measure based on public comments received related to variation in industry practices, including approaches to deduplication and automation. Specific metrics to support this finalized measure are described in the related measure specification located on ONC's website and in the section above. We also note that if regulatory baselines associated with the metrics change in the future—such as a revision to a criterion through notice and comment rulemaking—the measure specification would also be changed to ensure alignment with the revised criterion:

1. Number of encounters
2. Number of unique patients with an encounter
3. Number of unique patients with an associated C–CDA document
4. Number of total C–CDA documents obtained
5. Number of unique C–CDA documents obtained
6. Number of total C–CDA documents obtained that were pre-processed
7. Number of total C–CDA documents obtained that were not pre-processed
8. Number of total C–CDA documents obtained that were pre-processed where problems, medications, or allergies and intolerances were reconciled and incorporated via any method
9. Number of total C–CDA documents obtained that were not pre-processed where problems, medications, or allergies and intolerances were reconciled and incorporated via any method
10. Number of total C–CDA documents obtained that were determined to have no new problems, medications, or allergies and intolerances information by pre-processes or fully automated processes

The reporting period for the measure and related metrics consists of one calendar year. Data collection for the measures and associated metrics will begin during the second and third phases of reporting (which is described later in the preamble).

Measurement Area: Standards Adoption and Conformance

We proposed (88 FR 23837) to adopt four measures in the ''standards adoption and conformance'' area in § 170.407(a)(4) through (7) to provide insight into the role that standards play in enabling the access, exchange, and use of EHI. We proposed to measure the following aspects within this area: (1) availability of apps to support access to EHI for a variety of purposes; (2) the usage of FHIR-based APIs to support apps; (3) the use of bulk FHIR to support the access to EHI for groups of individuals; and (4) the use of EHI

export functionality (88 FR 23837). We stated that together, these measures will provide a foundation for understanding whether and to what extent ONC's policies to promote standards are supporting users of health IT, including patients, clinicians, researchers, and others to access, exchange, and use EHI via certified health IT for a variety of purposes. These measures would also provide visibility into industry adoption of standards required by the Program and provide data to inform future standards development work.

Comments. Many commenters supported the ''standards adoption and conformance'' measurement area. One commenter expressed support for interoperability measurement as a national priority. One commenter disagreed with ONC's statement that data on the volume of information exchanged would provide the means to assess the extent that patient information is moving between providers to facilitate high value care, stating that pure volume does not accurately reflect quality.

Response. We appreciate the support expressed by many commenters and agree that only collecting data on the volume of information exchanged will not strictly reflect the quality of care provided. However, we plan to use this data in conjunction with other collected data from the ''Insights Condition and Maintenance of Certification'' to create metrics that will assess the extent that patient information is exchanged between providers to facilitate high value care.

Comments. We received numerous comments with suggestions for new or revised measures in the ''standards adoption and conformance'' area. Throughout this measurement area we use the abbreviation ''app'' for the term application. Apps that may connect to ONC-certified health IT via the capabilities enabled by 170.315(g)(10), refer to third-party software or IT system not offered by the certified health IT developer including but not limited to: mobile apps, web portals, locally hosted software, enterprise software solutions, and custom software.

For the ''applications supported through certified health IT'' measure, the majority of comments received suggested metrics focused on the availability (*e.g.,* number of distinct apps) and accessibility (*e.g.,* number of accesses) of patient-facing and non-patient-facing apps. Two commenters suggested metrics focused on requesting additional qualitative context/information about the purpose for which apps were developed or use cases, especially for specialty care apps, and clinical decision support. One commenter requested for app developers to report the turnaround time for app developer authentication and authorization to production environments. One commenter requested for app attestation to be included in the Insights Condition requirements.

For the ''use of FHIR in apps supported by certified API technology'' measure, a majority of the comments suggested metrics focused on IG development, adoption, and conformance beyond the US Core IG. One commenter requested a metric that counts the number of queries made by either a patient or a clinician. One commenter suggested counting the total number of FHIR resources by individual resource.

For the ''use of FHIR bulk data access through certified health IT'' measure, most of the commenters suggested metrics focused on obtaining information related to the FHIR Bulk Data request metadata (*i.e.,* user-type of the FHIR Bulk Data requester, export time per resource (average), and group size for successful exports (average)). One commenter suggested a metric that counts the number of FHIR Bulk Data export requests. Another commenter suggested a metric that focuses on real-world performance of FHIR Bulk Data implementations.

Response. We thank all commenters for their thoughtful input. We appreciate the interest expressed in requiring additional reporting metrics for the ''standards adoption and conformance'' measurement area, and may explore the feasibility of these suggested reporting metrics in the future.

Applications Supported Through Certified Health IT Measure

In the HTI–1 Proposed Rule (88 FR 23837), we proposed to adopt the ''applications supported through certified health IT'' measure in § 170.407(a)(4), which would provide information on how certified health IT supports the health app ecosystem by asking certain health IT developers under the Program to report app names and app developer names, intended app purposes, intended app users, and whether a registered app is in ''active'' use across a developer's client base (as further detailed below). We stated in the HTI–1 Proposed Rule that this measure would result in a listing of apps that could be used to generate a variety of metrics. Only developers of certified health IT with Health IT Modules certified to the ''standardized API for patient and population services'' (§ 170.315(g)(10)) criterion would be required to report data for this measure.

In the HTI–1 Proposed Rule (88 FR 23837 through 23840), we proposed that developers of certified health IT with Health IT Modules certified to § 170.315(g)(10) provide certain information about the apps that are connected to their certified technology. We proposed that the app name and the developer (company/organization or individual) responsible for the app would be reported for each app registered to a developer of certified health IT whose Health IT Module is certified to the § 170.315(g)(10) criterion. We noted that the app registration process required under § 170.315(g)(10)(iii) may provide an opportunity for developers of certified health IT to gather standard information for apps connecting to their certified API technology as part of existing workflows. There may be other mechanisms besides the app registration process by which developers of certified health IT wish to obtain this information.

We proposed that developers of certified health IT with Health IT Modules certified to § 170.315(g)(10) obtain and report the intended purpose(s) for each app connected to their certified API technology using the following categories:

- Administrative Tasks (*e.g.,* scheduling & check-in, billing & payment)
- Clinical Tools (*e.g.,* clinical decision support, risk calculators, remote patient monitoring)
- Individuals' Access to their EHI (*e.g.,* enables patients to access their health information, medications, test results, vaccine records)
- Research (*e.g.,* used to perform clinical research)
- Population Data (*e.g.,* bulk transfer of data, population analytics & reporting)
- Public Health (*e.g.,* electronic case reporting)
- Patient-Provider Communication (*e.g.,* secure messaging, telehealth)
- Educational Resources (*e.g.,* patient and provider educational resources)
- Other Intended Purpose
- Unknown (*e.g.,* missing)

As stated in the HTI–1 Proposed Rule (88 FR 23838), developers of certified health IT to whom the measure applies would report the intended purpose(s) of the app for each app registered to their Health IT Module(s) certified to the § 170.315(g)(10) criterion. The categories we proposed under this measure were informed by app category taxonomies in published literature from Barker &

Johnson (2021),[199] Ritchie and Welch (2020),[200] and Gordon and Rudin (2022).[201] While we recognized this taxonomy may need to evolve over time, we conveyed in the HTI–1 Proposed Rule our belief that the proposed categories represented a large majority of the current market, and that the types of information, if reported on a complete set of apps, would provide insightful information to guide ONC's future efforts to support individuals' access to their EHI via apps, along with other priority uses, such as research and clinical care.

Additionally, we proposed (88 FR 23838) that developers of certified health IT with Health IT Modules certified to § 170.315(g)(10) obtain the following intended user(s) categories for each app connected to their certified API technology:

- Individual/Caregiver
- Clinician
- Healthcare Organization
- Payer
- Researcher
- Other Intended User
- Unknown (*e.g.,* missing)

We also proposed (88 FR 23838) that developers of certified health IT with Health IT Modules certified to § 170.315(g)(10) obtain the status for each app connected to their certified API technology using the following categories:

- Actively Used—An app is defined as ''Actively Used'' if EHI has been transferred to the app using certified API technology for 10 or more unique patients during the reporting period
- Not Actively Used—An app is defined as ''Not Actively Used'' if EHI has been transferred to the app using certified API technology for fewer than 10 unique patients during the reporting period

Comments. Most commenters, including EHR and app developers, as well as commenters representing health care providers, were generally supportive of this measure and provided specific requests for clarification and recommendations to constrain the measure. Several commenters indicated that the data collection burden is high for this measure. One commenter expressed concerns that the reporting of these data could lead the public to believe that health IT developers had a role in recruiting application developers to connect to § 170.315(g)(10). Another commenter recommended that this information be collected directly from application vendors to reduce burden on health IT developers.

Response. We thank commenters for their general support. We believe this measure provides greater transparency regarding apps that are connected to certified health IT. Specifically, this measure would enable ONC and the public to understand to what degree apps are connecting across different certified health IT products, which is important for enabling individuals' access to their EHI. The ONC Cures Act Final Rule (85 FR 25750) emphasized the importance of standardization, transparency, and pro-competitive business practices through the API Condition and Maintenance of Certification requirements that would make it easier for third-party apps to connect to certified health IT, and subsequently facilitate individuals' access to their EHI. This measure also provides insights into the types of apps that integrate with certified health IT. Collecting this information will be beneficial to developers as well, for it will provide them with insights about available technologies and uses for data that are in demand in the marketplace.

We acknowledge that collecting this information may require new or updates to existing data collection as part of the app developer registration processes. Although developers expressed concerns related to the burden associated with collecting this information, most commenters indicated that they have an existing app registration process, and thus we believe that developers of certified health IT are best positioned to collect and report this measure. The app registration process would provide an opportunity to gather standard information for apps connecting to their certified health IT as part of existing workflows. We currently do not have data regarding which apps are connected to their developers' health IT and thus cannot directly collect this information. We also recognize that health IT developers do not recruit application developers to connect to certified health IT, but rather are collecting this information among those application vendors that are connected to their systems and through the app registration processes.

Comments. Numerous commenters recommended that ONC directly acknowledge that mandatory collection of intended purposes and intended users via the health IT developer registration process would not violate the API Condition of Certification. One health IT developer expressed concern that some of the measures will require collection of new types of data, specifically app categories and audiences. Commenters representing app developers indicated they supported this measure and furthermore had suggestions for additional measures to include.

Response. We appreciate the comments, and note that the collection of app information required for this Insights Condition measure will not violate the API Condition and Maintenance of Certification (§ 170.404(b)). Specifically, the requirements in § 170.404(b) enable a Certified API Developer to institute its own process to register applications for production use, so long as it occurs within five days of completing its verification of an API User's authenticity. We do not believe requiring app developers to provide basic information such as the characteristics of their application, including intended users and purpose, to be creating undue burden on app developers. Given the support we received for this measure, including from app developers, we do not believe this will be a widespread concern or issue. However, we remind Certified API Developers that the registration process must still occur in the allotted five business days of completing its verification of an API User's authenticity, pursuant to paragraph § 170.404(b)(1)(i) and consistent with § 170.404(b)(1)(ii).

Comments. Several commenters had questions related to which apps would be subject for inclusion in this measure. Commenters representing EHR developers inquired whether applications relevant for this measure would be exclusively those registered for and using the scope of FHIR resources required under the scope of the relevant program criterion at § 170.315(g)(10). Another commenter indicated that some § 170.315(g)(10) certified health IT does not transfer patient EHI and requested clarification on whether this technology would be subject to reporting for this measure.

Response. We appreciate the feedback and offer the following clarifications. Any app that is registered via the app registration process for the § 170.315(g)(10) criterion is subject for inclusion in this measure. We note that the apps that are used by a variety of interested parties to interact with health

[199] The ecosystem of apps and software integrated with certified health information technology: *https://academic.oup.com/jamia/article/28/11/2379/6364773?login=false.*

[200] Categorization of Third-Party Apps in Electronic Health Record App Marketplaces: Systematic Search and Analysis: *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7293052/.*

[201] Gordon WJ, Rudin RS. Why APIs? Anticipated value, barriers, and opportunities for standards-based application programming interfaces in healthcare: perspectives of US thought leaders. JAMIA Open. 2022 Apr 6;5(2):ooac023. doi: 10.1093/jamiaopen/ooac023. PMID: 35474716; PMCID: PMC9030107.

IT certified to § 170.315(g)(10) are in scope and could include, but are not limited to, provider-, patient-, and payer-oriented apps. This variety is also reflected in the category of intended user types we plan to collect. We did not fully understand the comment regarding a § 170.315(g)(10) certified health IT that does not transfer patient EHI because that is the primary point of such technology. As a result, we are unable to provide further clarity in response to the comment aside to reiterate that all apps registered through the § 170.315(g)(10) app registration process is in scope for this measure.

Comments. Many commenters indicated that it would be difficult to collect additional information from app developers that are already registered with their certified health IT and that new information will not be collected until app developers need to re-register their app. Thus, ONC should expect a disproportionate number of ''unknown'' entries related to intended purpose of app and users during early years of reporting. Another commenter indicated that it would be unable to capture this information for applications that do not register with the developer of certified health IT. One commenter noted that with a dynamic client registration process, where the registration of applications with an authorization server would be done dynamically using a trust framework, might lead to attributes needing to be collected as part of the registration assertion process. They recommended that this may need to be reviewed, perhaps by a FHIR at Scale Taskforce (FAST) workgroup.

Response. We appreciate these comments, and recognize that the measure data may not be as comprehensive initially as it will be in future years since the year 2026 will be the first measure collection phase and some health care providers will still be implementing § 170.315(g)(10) upgrades. Thus, there may be many ''unknown'' entries in early years of reporting, and as apps re-register, this information would be provided. Many developers certified to § 170.315(g)(10) may require app developers to register via a process that allows for the collection of the data required for this measure. To the commenter who indicated app information may be missing for those apps that do not register, we recognize that apps not connected to the certified (§ 170.315(g)(10) API (and therefore not required to register) would not be included. We also note that while the app registration process required under § 170.315(g)(10)(iii) may provide an opportunity to collect this information, developers of certified health IT may wish to use other mechanisms such as surveys, forms, or health IT system-based methods to obtain this information. We are not limiting or specifying the methods by which developers of certified health IT collect this information. Developers should describe the method(s) they used to collect the data in the required documentation they submit to ONC. Further, we believe it will be possible to collect these data through the dynamic client registration process; however, we note that existing dynamic registration implementation guides may need additional specification. We appreciate the recommendation to consult with a FAST workgroup or other groups working on dynamic client registration to ensure that this step is included as part of that process.

Comments. One commenter supported the proposed collection of user type (intended user of app) for apps and encouraged collection of information that would identify the types of users that are the focus of the app (*e.g.,* patient, provider, system) to the dataset of information collected about apps. Another commenter requested clarification between ''clinician'' and ''healthcare organization.'' One commenter suggested that the value sets for metrics, intended purpose of app and intended user of app, be based upon a standardized value set referenced in other interoperability initiatives such as TEFCA and HL7 Role Class, respectively. One commenter also noted that some apps may have multiple intended purposes and intended users and wanted to confirm that reporting of multiples where relevant was acceptable.

Response. We appreciate the input provided by commenters on establishing or selecting an available value set for intended purpose and intended user. We agree that ''clinician'' and ''healthcare organization'' may seem duplicative and to avoid confusion we have revised the value set by removing both of these options and replacing ''clinician'' with ''clinical team'' and ''healthcare organization'' with ''healthcare administrator/executive.'' We appreciate the recommendation to consider standardized value sets and may consider identifying relevant value sets in future rulemaking. With regards to selection of metrics, intended purpose, and intended user, we understand that there may be multiple purposes and users so apps should select all that apply and not be limited to one response. Therefore, these are the following intended user(s) categories for each app connected to their certified health IT:

- Individual/Caregiver
- Clinical Team
- Healthcare Administrator/Executive
- Payer
- Researcher
- Other Intended User
- Unknown (*e.g.,* missing)

Comments. Several commenters requested clarification on whether an application is ''actively used'' or ''not actively used,'' noting applications that are ''not actively used'' are not a reflection of the certified health IT. One commenter recommended that an application should be designated as actively used based upon either a particular threshold of total API call volume, or total authorization events constituting a unique user session for the app. The commenter indicated that this approach would help ensure that apps used in high frequency for retrieving health information on a small number of patients are not erroneously classified as ''not actively used.'' The same commenter expressed concern about a threshold of 10 or more unique patients, indicating that an app that is used daily by fewer patients should still be considered ''actively used,'' especially for developers that may only serve a smaller scope of providers. Another commenter suggested an additional category of ''evaluating'' that represents an app is connected but used by fewer individuals (such as 3 or 5), along with a ''superactive'' designation for larger numbers of individuals, therefore creating four categories, rather than two.

Response. We thank commenters for their input. We realize that usage of apps is not necessarily a reflection on health IT developers. However, this information is critical to collect in order to distinguish between production apps that are registered and are in use (*e.g.,* 10 or more unique patients), production apps that are registered and are not in use (*e.g.,* less than 10 unique patients), and production apps that are registered but not enabled by the health IT developer. Without this information, the value of the overall data would be limited.

The definition of active use is described in our measure specification. The definition is based on whether EHI has been transferred to the app using certified health IT for ten (10) or more unique patients during the reporting period. By setting the threshold at ten or more unique patients, we expect that this threshold will represent active use. While mobile patient portal apps and well-known healthcare apps (*e.g.,* Apple

Health) have large user bases, for lesser-known healthcare apps that filled specific healthcare segments (*e.g.,* rare or terminal diseases, chronic or hereditary diseases, age-related conditions, pediatrics, behavioral and mental health), ONC expects smaller user bases.[202] An ONC internal analysis of the Google Play™ store data found that the number of Android installs for apps that enable patients to access their data, ranged from 4 to over 400,000. There is little public data on number of users specifically, and thus, in setting the criteria of active use, we are relying upon the number of installs for these types of apps, even though it is not equivalent to the number of users. A mix of self-reported data show approximately 3.87 million people use health and fitness apps, and data from app stores list approximately 350,000 mobile health apps (many of which include apps that do not integrate with EHRs and are not applicable to this metric); on average, health apps have approximately 11 users each.[203] However, none of these data sources provide data on actual use for the apps that connect with EHRs. We aim to be broad in determining active use and balance the need to define app use to include apps that have a smaller target audience. Thus, we have set a relatively low threshold of ten or more unique patients for defining active use. We appreciate the alternative suggestions for measuring whether an app is actively used. However, using total API call volume to measure usage would skew results and make it difficult to determine appropriate level of API calls to qualify for ''active use,'' as certain apps may make API calls multiple times per day. A lower threshold of less than ten users that would also take into account the use of apps on a daily or weekly basis may be more complex to implement, as this also involves measuring the frequency of use (as opposed to simply the number of users). Also, the call or requested data (which would be used to assess frequency of use) may be difficult to interpret as apps using APIs regularly request data from providers as part of their process to update the data within the app, and it may not reflect user driven behavior. The other suggested alternative, using authorization events, could be difficult to implement because it would be difficult to determine the number of authorization events that would define whether an app is actively used given the number of authorization events could vary by individual and app. However, we plan to continue collaborating with the community to assess level of usage using authorization events for future iterations of this measure.

With regards to expanding usage from two to four categories, we may consider expanding categories in the future.

Comments. A couple of commenters also had questions about the inclusion of apps as of the last day of the reporting period (*i.e.,* report only existing apps as of the last day of the reporting period) or whether apps should be included based upon whether they had registered at any point during the reporting period (*i.e.,* report all apps that had been registered during the reporting period, even if they are not registered on the last day of the reporting period). A commenter suggested counting the total number of apps active at any point in the reporting period to appropriately account for onboarding and offboarding activity, whereas a couple of commenters noted that reporting of the app status is not a metric that is measured over a reporting period and would be an indication at a point in time at the end of the reporting period.

Response. We clarify that the app status (*e.g.,* usage) should include apps based upon whether they had registered at any point in time during the reporting period. We seek to measure the unique number of individuals who used the app during the reporting period (a calendar year) and do not want to limit the inclusion to apps that are registered as of the last day of the reporting period. For apps that were registered during the reporting period and are not registered at the end of the reporting period, we would want their status to be calculated and included.

Comments. One commenter representing medical professionals recommended that as part of this measure, ONC include a metric requiring health app developers to attest to whether they adhere to (yes/no) any of the following: (1) Industry-recognized development guidance (*e.g.,* Xcertia's Privacy Guidelines/Privacy Is Good Business: a case for privacy by design in app development); (2) Transparency statements and best practices (*e.g.,* Mobile Health App Developers: FTC Best Practices/CARIN Alliance Code of Conduct/AMA Privacy Principles); and/or (3) A model notice to patients (*e.g.,* ONC's Model Privacy Notice). The commenter noted that almost all patients want transparency on how apps access, exchange, or use their medical information, and this would address that need.

Response. We thank the commenter for their recommendations to include a metric on an app developer's adherence to various privacy and security practices and frameworks. We may consider these recommendations in future rulemaking. We also refer readers to other federal regulations such as Section 5 of the FTC Act,[204] Children's Online Privacy Protection Act (COPPA) [205] and the COPPA Rule,[206] and other industry initiatives [207] supporting consumers in app privacy, security, and transparency.

Finalization of Measure

We have finalized the ''applications supported through certified health IT'' measure in § 170.407(a)(3)(iii). We have revised the proposed measure based on public comments received. Specific metrics to support this finalized measure are listed below and described further in the accompanying measure specification located on ONC's website. We also note that if regulatory baselines associated with the metrics change in the future—such as a revision to a criterion through notice and comment rulemaking—the measure specification would also be changed to ensure alignment with the revised criterion.

1. Application Name(s);
2. Application Developer Name(s);
3. Intended Purpose(s) of Application;
4. Intended Application User(s); and
5. Application Status.

The reporting period for the measure and related metrics above consists of one calendar year. Data collection for the measures and associated metrics will begin during the first phase of reporting (which is described later in the preamble).

Use of FHIR in Apps Through Certified Health IT Measure

In the HTI–1 Proposed Rule (88 FR 23839), we proposed the adoption of the ''use of FHIR in apps supported by certified API technology'' measure in § 170.407(a)(5), which would capture the volume of FHIR resources transferred in response to API calls from apps connected to certified API technology by FHIR resource type. We also proposed (88 FR 23839) that the FHIR resources transferred be reported by FHIR version used and by US Core Implementation Guide version

[202] *https://www.healthit.gov/sites/default/files/page/2020-11/Accelerating_APIs_Consumer_Perspective.pdf.*

[203] *https://www.mobius.md/2021/10/25/11-mobile-health-statistics/.*

[204] *https://www.federalreserve.gov/boarddocs/supmanual/cch/200806/ftca.pdf.*

[205] *https://www.govinfo.gov/content/pkg/PLAW-105publ277/pdf/PLAW-105publ277.pdf.*

[206] *https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa.*

[207] *https://www.ftc.gov/business-guidance/resources/mobile-health-apps-interactive-tool.*

deployed. This measure also proposed requiring developers to report FHIR resources transferred in response to calls from two different endpoint types: patient-facing and non-patient-facing, the latter of which would include endpoints that do not facilitate individuals' access (*e.g.,* clinician, payer, or public health endpoints). We explained that this measure proposed to require developers of certified health IT with Health IT Modules certified to the ''standardized API for patient and population services'' (§ 170.315(g)(10)) certification criterion to report on the number of deployments they support across their customer base, and that together, these data points would provide insights into the usage of certified APIs by collecting data on the volume of FHIR resources transferred to apps in response to API calls by FHIR resource type, type of endpoint, and US Core Implementation Guide used.

We proposed (88 FR 23839) the first numerator to be the number of FHIR resources returned/transferred in response to a call to a certified API technology by resource type. We proposed the second numerator to be the number of distinct certified API technology deployments (across clients) associated with at least one FHIR resource returned/transferred in response to a call. We noted that each of the numerators would be stratified (*e.g.,* divide into subsets) by type of endpoint (patient-facing vs. non-patient-facing), by FHIR version, and by US Core Implementation Guide.

We proposed (88 FR 23839) the denominator to be the total number of distinct certified API technology deployments (across clients). In addition, we proposed this denominator to be stratified by type of endpoint (patient-facing vs. non-patient facing), FHIR version, and US Core Implementation Guide. We noted that non-FHIR APIs, such as those represented with proprietary standards, are excluded from this measure, including numerators and denominators. We refer readers to the HTI–1 Proposed Rule for a complete listing of the metrics this measure would enable us to calculate (88 FR 23839). As stated in the HTI–1 Proposed Rule, this measure would require that developers report the volume of FHIR resources transferred in response to calls by FHIR version and by US Core Implementation Guide. While Health IT Modules certified to § 170.315(g)(10) are required to respond to requests according to FHIR version Release 4, we are aware that there will be newer versions of FHIR supported by newer versions of the US Core Implementation Guide. Gaining insights into the frequency in use of US Core Implementation Guides will inform ONC of the variability in the implementation of FHIR across developers.

We requested feedback on whether information on both aspects of the measure, FHIR version and US Core Implementation Guide, are necessary as each provides unique insights, or whether focusing on one of these (either FHIR version or US Core Implementation Guide) would be sufficient to understand where the industry is in the implementation of FHIR. We also requested comment on the feasibility of reporting the use of different HL7 FHIR implementation guides and FHIR versions, versus being stratified by type of endpoint, type of FHIR resources, and by the number of certified API technology deployments (88 FR 23840).

We also proposed (88 FR 23840) to require developers of certified health IT to whom the measure would be applicable to report the number of certified API technology deployments (as a proxy for organizations that have installed certified API technology) where FHIR resources were transferred in response to a call (relative to the total number of certified API technology deployments). We stated that this information can shed light on whether usage is concentrated versus dispersed, indicating the breadth of usage across end users and organizations. However, given that API deployments may vary across developers, we sought feedback on whether this measure would be a good proxy for understanding usage across their client bases.

Comments. The majority of commenters expressed support for the proposed measure. Two commenters, one of which represents ONC's Health IT Advisory Committee, indicated the support for metrics that would help inform the future development of interoperability standards, including versions and variations. Commenters indicated these data would provide use of standards in the field that can shed light on industry-wide readiness for the adoption of standards, such as those adopted through Standards Version Advancement Process (SVAP). One commenter suggested to delay or eliminate the measure. Commenters representing community healthcare associations expressed support for this measure, stating that this measure benefits community health centers by measuring the interoperability and seamless data exchange between healthcare applications and exchange partners, which leads to better care coordination and improved population health outcomes.

Response. We thank commenters for their support and believe that these measures provide real-world usage data to help guide and inform the future development of interoperability standards, and therefore we do not plan to eliminate this measure as suggested by one commenter. While the data for this measure will be collected in the first year of the Insights Condition (CY 2026), the first response submission period has been delayed to July, 2027 to provide more time to implement the measure and reduce burden. More details on the compliance dates associated with all the measures can be found in section III.F.3.

Comments. A couple of commenters provided qualitative ratings of burden associated with the metrics. One commenter indicated that the first metric (number of FHIR resources returned/transferred in response to a call to a certified health IT by resource type) would be medium level of effort; whereas the other commenter indicated that first metric would be high level of effort. Both commenters indicated that the second metric (number of distinct certified health IT deployments (across clients) associated with at least one FHIR resource returned/transferred in response to a call) would be low level of effort. A couple of other commenters requested additional clarity on whether the first metric intends for developers to report the number of total resources returned for each resource, or the number of requests that returned at least one (1) resource for each resource. For example, if a request returns 100 different Observations, would that be considered a count of 1 or 100 total resources. Two commenters recommended defining the first metric to be the total number of resources returned. Another commenter recommended simplifying the metric by measuring only the number of queries or requests made by patients and by clinicians to measure the actual usage of API functionality.

A few commenters requested clarifications on whether any FHIR resources supported by CEHRT need to be counted. Commenters also recommended for ONC to isolate USCDI v1 FHIR resources that are within scope of § 170.315(g)(10) for reporting consistency across health IT developers. Several commenters recommended that this measure should not require tracking of FHIR resources that developers may support beyond USCDI v1, as required by § 170.315(g)(10).

Response. We appreciate the feedback on the burden associated with the

measure. As discussed earlier in the preamble, to address burden, we have phased the implementation of the measures starting with a simpler version in the first year and then added the additional complexity in the subsequent years. Additionally, we have revised the measure to address burden. We agree with commenters that for reporting consistency and certain, clear requirements that the FHIR resources reported should align with the criterion § 170.315(g)(10). FHIR resources supported by and within the scope of the § 170.315(g)(10) criterion include FHIR resources referenced in the US Core IG attributed to and that support USCDI data elements. In this case, as an HTI–1 regulatory baseline, would be version 6.1.0 and v3, respectively, because data collection for this measure will begin after the technical requirements for health IT developers to update their certified health IT to these newer standards would have occurred as of January 1, 2026. We also note that if regulatory baselines associated with the metrics change in the future—such as a revision to a criterion through notice and comment rulemaking—the measure specification would also be changed to ensure alignment with the revised criterion. Additionally, if a health IT developer chooses to use the SVAP to adopt a newer version of standards referenced in § 170.315(g)(10), they will need to report based on the newer versions.

We also appreciate the requests for clarification on the metrics. Our intent is to measure the adoption and use of FHIR by industry users (*e.g.,* third-party app developers, health IT developers, provider organizations). To clarify on whether the metric intends for developers to report the number of total resources returned for each resource, or the number of requests that returned at least one resource for each resource, we have revised the first metric to make it clear that we expect the latter. Additionally, we have removed the phrase, ''in response to a call'' across the metrics associated with the measure. For example, we have revised the metric from, number of FHIR resources returned/transferred in response to a call to certified API technology by FHIR resource type to the following, number of requests made to certified health IT that returned at least 1 FHIR resource by FHIR resource type. Both the proposed and revised metric assess the types of FHIR resources provided by certified health IT in response to a request. A request made to certified health IT can return a variety of different types and number of FHIR resources in response. The proposed metric focused on both the number of resources and types of resources returned; the revised metric focuses largely on the types of resources returned rather than the volume of resources returned. This simplified metric will still provide us with the necessary information on the types of resources provided. As noted by commenters, the total volume of FHIR resources returned is more difficult to interpret. The volume of resources could be related to a small number of apps returning a lot of data or many apps returning a little data. In contrast, the number of requests that returned at least 1 resource by resource type provides us insights into the ''demand'' for each resource and is easier to interpret. Measuring queries alone doesn't provide insight into whether data was shared in response to the query as there may not be data available to return. The goal in this metric is to understand the number of API requests that return various FHIR resources to gain insight on the resources most commonly exchanged.

Comments. A couple commenters requested specific clarification on whether the metric, number of distinct certified health IT deployments (across clients) is intended to be the total number of API deployments active at any time during the reporting period, or the total number active as of the end of the reporting period. The commenters recommended defining it to be the total number of API deployments active at any time during the reporting period. Another commenter noted a limited situation where an EHR user may have more than one production database of a certified solution and requested additional clarification for reporting on the measure, anticipating that they would count all deployments of the certified solution regardless of the number of clients that represents. A couple commenters provided qualitative ratings of burden associated with the metric, indicating that this would be low level of effort.

Response. We thank commenters for their feedback. Originally, we proposed reporting the number of distinct certified API technology deployments (across clients) during the reporting period. We clarify that this refers to counting the total number of certified health IT deployments active at any time during the reporting period, not the total number active as of the end of the reporting period. We had not intended, nor indicated, that we would be measuring this as of the end of the reporting period. We also acknowledge situations where an EHR user may have more than one production database of a certified solution and have revised the measure to count all deployments of the certified solution regardless of the number of clients that represents. The metric now measures the number of distinct certified health IT deployments (across clients) active at any time during the reporting period (overall) and by user type (*i.e.,* patient-facing and non-patient-facing).

Comments. Several commenters expressed support for patient-facing versus provider-facing stratification. One commenter expressed concern about reporting in this manner as endpoints can serve multiple and broad audiences. For example, the same endpoint could be used for both patients and providers. The same commenter recommended to report based on user type instead of endpoint types.

Response. We thank the commenter for their input and agree that FHIR endpoints are not necessarily specific to a user type and can serve multiple audiences. Given that endpoints can serve both patients and providers (for example) and thus would have to be double counted if that was the case, we have modified the metric to instead report the types of users the endpoint serves. We believe this will simplify reporting. Therefore, we have replaced the term endpoint type with user type. The user type categories are patient-facing and non-patient-facing. We believe the revision better represents our intention of understanding the user types that are using FHIR resources and FHIR APIs.

Comments. Commenters were generally split on the proposed stratification of reporting both the FHIR version and the US Core Implementation Guide (IG) version. Those in support of stratifications indicated that the stratifications provide important distinctions for understanding the use and development of FHIR and is appropriately scoped in alignment with how most health IT developers' certified APIs are deployed. One commenter noted that being able to track IG conformance beyond US Core is essential to understanding how the industry is using FHIR and the data being exchanged via FHIR. Additionally, one commenter who supported the stratification noted that given continued updating of the US Core IG, future FHIR versions and US Core IG versions may not be synonymous in describing the capabilities of a technology, making it necessary to stratify by both FHIR version and the US Core IG version. One commenter recommended requiring the reporting of each FHIR resource by IG conformance beyond the US Core IG at

the installation level for all health IT developers, including smaller developers that certify to FHIR API criteria. Several commenters suggested that ONC remove the stratifications for FHIR version and US Core IG version, noting that FHIR R4 is currently the only relevant version of FHIR base specification version and that, in most cases, health IT developers are only conformant to one version of the US Core IG. However, one commenter was supportive of the inclusion of the proposed stratifications for future reporting, as long as ONC provides specific guidance to health IT developers. One commenter noted that stratifying the number of deployments by the proposed stratification attributes does not make sense unless ONC's objective is to measure FHIR APIs or resources transferred and recommended stratifying deployments by the version of the certified health IT product. Another commenter highlighted that the proposed stratifications for FHIR version and US Core IG version would be a high level of effort and recommended limiting the measure stratifications to only patient-facing and non-patient facing endpoints.

Response. We thank commenters for their feedback. We agree that the stratifications provide real-world data regarding the implementation and use of FHIR and US Core IG. This detailed reporting would help inform our goal of guiding future development of standards and insights on the current implementation and use of standards. We also acknowledge some support for restricting the measure specification to FHIR R4 and to one version of the US Core IG. In response to comments, we have made changes to metrics related to this measure so that the metrics are simplified and the stratification by FHIR version no longer needs to be reported. We also have developed a phased approach to implement the measure and related metrics over two years. Similar to the HTI–1 Proposed Rule metric, which called for reporting the number of FHIR resources returned/transferred in response to calls (also called requests) to a certified health IT by FHIR resource type, the first metric listed below also assesses the types of FHIR resources provided by certified health IT in response to a request. The revised metric no longer requires the number of FHIR resources, but instead requires counting the number of requests where at least one FHIR resource was provided. As described earlier, we sought to simplify this metric in response to comments and thus scaled back this metric to the number of requests made that returned at least 1 FHIR resource by resource type. For the second metric listed below, we have simply embedded the original stratification—by user type (which replaced type of endpoint)—within the metric; rather than listing the stratifications separately. The third metric differs from the second metric because it asks about the number of distinct certified health IT deployments (across clients) overall and by user type, and is not limited to those certified health IT deployments which were associated with at least one FHIR resource returned or transferred. We note that for the third metric, the word ''total'' was removed from the HTI–1 Proposed Rule measure as there is no substantive difference between ''total number'' of distinct certified health IT deployments (across clients) by user type (*i.e.,* patient-facing and non-patient-facing) and ''number'' of distinct certified health IT deployments (across clients) by user type (*i.e.,* patient-facing and non-patient-facing) and we seek to create consistency across the metrics.

As noted earlier, to reduce burden, we have dropped the stratification by FHIR version but have kept the US Core IG version stratification. Given that we are aligning the reporting of FHIR resources to those supported by the § 170.315(g)(10) criterion and health IT developers will also report on the US Core IG version which aligns with the specific version of FHIR, we do not also need to separately obtain information on FHIR version. The metrics indicate the number of distinct certified health IT deployments (across clients) associated with at least one FHIR resource returned by US Core IG version(s). Together, the phasing of the reporting requirements and simplifying metrics (including removing the FHIR version stratification) will lower the initial reporting burden for health IT developers, as well as provide health IT developers additional time to develop the infrastructure necessary to report on the more advanced stratification (US Core IG versions) which would have valuable insights.

Finalization of Measure

We have finalized the measure as ''use of FHIR in apps through certified health IT'' in § 170.407(a)(3)(iv). We have revised the proposed measure based on public comments received. Specific metrics to support this finalized measure are listed below and described further in the accompanying measure specification located on ONC's website. As noted earlier, if regulatory baselines associated with the metrics change in the future—such as a revision to a criterion through notice and comment rulemaking—the measure specification would also be changed to ensure alignment with the revised criterion. The reporting period for the measure and related metrics below consists of one calendar year. Data collection for the measures and associated metrics will begin during the first and second phases of reporting (which is further described later in the preamble):

In the first year (where responses will be due July 2027, and annually thereafter), we require developers to report the:

- Number of requests made to distinct certified health IT deployments that returned at least 1 FHIR resource by FHIR resource type.
- Number of distinct certified health IT deployments (across clients) associated with at least one FHIR resource returned, overall and by user type (*e.g.,* patient-facing and non-patient-facing).
- Number of distinct certified health IT deployments (across clients) active at any time during the reporting period, overall and by user type (*i.e.,* patient-facing and non-patient-facing).

In year 2, in addition to what is required in year 1, we require developers to report the metrics below. These metrics will be due July 2028 (and annually thereafter):

- Number of distinct certified health IT deployments (across clients) associated with at least one FHIR resource returned by US Core Implementation Guide version.

Use of FHIR Bulk Data Access Through Certified Health IT Measure

We proposed (88 FR 23840) to adopt the ''use of FHIR bulk data access through certified health IT'' measure in § 170.407(a)(6), which would measure the number of bulk data downloads completed through certified health IT relative to the number of certified health IT deployments or installations. Specifically, we stated that this measure would provide information on how certified health IT is being used to perform ''read'' services for a specified patient population using the HL7 FHIR® Bulk Data Access (Flat FHIR) V1.0.1 standard. A developer of certified health IT with Health IT Modules certified to the ''standardized API for patient and population services'' (§ 170.315(g)(10)) certification criterion would be required to report under this proposed measure.

We proposed (88 FR 23840) the first numerator to be the number of data/download requests completed during the reporting period using certified health IT certified to the ''standardized

API for patient and population services'' (§ 170.315(g)(10)) in response to a bulk data download request to export all data for patients within a specified group. We proposed (88 FR 23840) the second numerator to be the number of distinct certified health IT deployments or installations certified to the ''standardized API for patient and population services'' (§ 170.315(g)(10)) (across clients) that successfully completed at least one bulk data download request during the reporting period.

We proposed the denominator (88 FR 23840) to be the total number of distinct certified health IT deployments or installations (across clients). We requested comment on whether additional stratifications would provide valuable insights, what additional data developers of certified health IT are collecting, and what effort developers of certified health IT are devoting to collecting additional data such as: (1) intended use case (*e.g.,* population analytics, reporting, research); (2) entity calling the API (*e.g.,* healthcare organization, payer, public health agency); and (3) automated queries (refreshing the data at certain intervals) versus ad hoc queries. For future measure development, we requested comment on whether it is possible to collect information on the number of authorized users calling a bulk FHIR API, the level of effort required to collect this information, and whether it would provide valuable insights.

We also noted and clarified that non-standard or proprietary resources (*e.g.,* non-FHIR based) transferred would be excluded from this measure, and that the proposed data for this measure would not include patient-facing applications, as individual patients only have the right to access their own records or records of patients to whom they are a personal representative.

Comments. The majority of commenters were supportive of the proposed measure. Two community healthcare associations supported this measure, expressing that this measure benefits community health centers by monitoring the ability to leverage comprehensive data for population health management and analytics, which will guide public health and population health initiatives. One commenter strongly recommended including at least one metric to track the real-world performance of current HL7/SMART FHIR bulk data implementations. One commenter expressed an opinion that the burdens of data capture for this reporting purpose outweighed the value of additional stratification and suggested starting with a ''core'' measure and layering on additional stratifications using a phased approach. The commenter noted that while reporting is feasible, it may require development to capture a specific countable event for reporting purposes. A couple of commenters also provided qualitative ratings of burden associated with the measure. One commenter indicated that the first numerator would be medium level of effort; whereas the other commenter indicated that the first numerator would be low level of effort. Both commenters indicated that the second numerator would be low level of effort, and that the denominator would be low level of effort.

Response. We appreciate the support expressed by commenters as well as the desire to phase in the measure, providing more time to implement the measure which, overall, has relatively lower burden. We also appreciate the suggestion to include at least one reporting metric to track the real-world performance of current bulk FHIR implementations. However, this will require additional research to determine whether the reporting metric should be included for future rulemaking.

Comments. Several commenters requested additional clarity on whether the specification of ''operationalized as [FHIR ServerBase]/Group/[groupid]/$export'' is used for both numerators in this measure. Additionally, commenters expressed confusion on whether the count for both measures is defined as the number of group export completed or the number of group export completed, accessed, and downloaded. The commenters recommended to count the number of completed requests, regardless of whether they are subsequently accessed and downloaded by the requestor. One commenter noted that their health IT solution cannot determine when a user has downloaded all queried and retrieved data files. One commenter requested additional clarity on the difference between ''requests completed'' in the first numerator and ''successfully completed'' in the second numerator for a bulk data download request. Another commenter suggested defining ''complete'' as when the Bulk Data Status Request reports a status of complete (*i.e.,* the timepoint when the user may begin downloading files). One commenter requested additional clarity on how ''rate'' will be measured under the second numerator. One commenter requested clarification regarding the requirement to include API-enable ''read'' services for multiple patients across all endpoints regardless of whether it is publicly available or not and specifically whether non-patient-facing endpoints are to be counted, since regulations only require patient-facing URL endpoints to be published. One commenter suggested for ONC to collect data on bulk FHIR data queries by cohort type (*e.g.,* research, financial operations, care management, public health, electronic case reporting).

Response. We thank commenters for their feedback. To clarify, the bulk data download request using certified health IT to export all data for patients within a specified group will be operationalized as ''[FHIR ServerBase]/Group/[groupid]/$export'' for the metrics associated with this measure. We agree with commenters that the measure should focus on the number of completed requests, regardless of whether they are subsequently accessed and downloaded by the requestor and have revised the wording of both metrics to reflect this change. Thus, ''completed'' is defined as when the Bulk Data Status Request reports a status of complete (*i.e.,* the timepoint when the user may begin downloading files). We believe there is not a substantive difference between ''successfully completed'' and ''completed,'' and to keep consistency between these metrics, we have removed the proposed term ''successfully'' from both metrics. We have also replaced the term ''data/download'' to ''bulk data access'' for consistency with the title of the measure.

We have removed ''expected metrics'' that we had originally listed in the measure specifications sheets accompanying the HTI–1 Proposed Rule, such as the rate of bulk data download requests. To clarify, it is ONC that will be responsible for calculating derived statistics based upon the metrics and data the developers report. We will also determine how calculated metrics will be aggregated and reported (whether at the national, developer, and/or product level) once we receive the data. How the data is presented will depend in part upon the completeness and quality of the data received.

These metrics apply to API-enabled ''read'' services for multiple patients where the number reported should reflect the ''read'' access queries that used the population services capabilities in § 170.315(g)(10) (*e.g.,* the FHIR Bulk Data Access IG). Given that bulk FHIR is likely primarily for non-patient facing use cases, it should not be limited to patient-facing endpoints; it needs to include ''all'' endpoints and use cases. Furthermore, these metrics are unrelated to the API Condition of Certification requirements for publishing patient-facing endpoints,

which supports patient access to their data using 3rd party apps and not related to Bulk FHIR. To reiterate, the metrics should reflect activity across all endpoints regardless of whether publicly available or not and type of endpoint user. The endpoints included should not be limited to those only used by patients. This is important as we seek insight on bulk data usage volume independent of user type and have developed a measure in a manner that does not differentiate between public and private APIs. In addition, we note that the measure applies to FHIR Bulk Data requests for FHIR resources that within the scope of § 170.315(g)(10) as discussed in more detail in the responses to comments in the previous measure above.

We appreciate the interest expressed in a reporting metrics that measure the adoption and conformance of FHIR Bulk Data APIs by cohort type or use case and may explore the feasibility of this in the future.

Comments. One commenter recommended ONC to align the denominator to the ''use of FHIR in apps supported by certified API technology'' measure. Another commenter requested clarification on whether the denominator is intended to be the total number of API deployments active at any time during the reporting period, or the total number active as of the end of the reporting period and recommended to define the denominator to be the total number of API deployments active at any time during the reporting period. Another commenter noted a limited situation where an EHR user may have more than one production database of a certified solution and recommended to count all deployments of the certified solution regardless of the number of clients that represents.

Response. We thank commenters for their input. In response to comments, we have reviewed the metrics (previously referred to as denominators) for the two measures (''use of FHIR in apps supported by certified API technology'' [finalized as ''use of FHIR in apps through certified health IT''] and ''use of FHIR bulk data access through certified health IT''). We concur that these metrics should be consistent with each other and measure the number of distinct health IT deployments (across clients) active at any time during the reporting period. Therefore, we will use the metric from the ''use of FHIR in apps through certified health IT'' measure for calculating any derived statistics.

We acknowledge situations where an EHR user may have more than one production database of a certified solution and clarify that this measure counts all deployments of the certified solution regardless of the number of clients that represents.

Finalization of Measure

We have finalized the ''use of FHIR bulk data access through certified health IT'' measure in § 170.407(a)(3)(v). We have revised the proposed measure based on public comments received. Specific metrics to support this finalized measure are listed below and described further in the accompanying measure specification located on ONC's website. We also note that if regulatory baselines associated with the metrics change in the future—such as a revision to a criterion through notice and comment rulemaking—the measure specification would also be changed to ensure alignment with the revised criterion:

1. Number of bulk data access requests completed (across clients) to export all data requested for patients within a specified group.

2. Number of distinct deployments of the certified health IT deployments (across clients) that completed at least one bulk data access request.

The reporting period for the measure and related metrics above consists of one calendar year. Data collection for the measures and associated metrics will begin during the second phase of reporting (which is described later in the preamble).

Electronic Health Information Export Through Certified Health IT Measure

We proposed (88 FR 23841) to adopt the ''electronic health information export through certified health IT'' measure in § 170.407(a)(7) which would capture the use of certified health IT to export single patient and patient population EHI. A developer of certified health IT with Health IT Modules certified to the ''electronic health information (EHI) export'' (§ 170.315(b)(10)) certification criterion will be required to report data under this proposed measure.

We proposed (88 FR 23841) a count for this measure (rather than a numerator and denominator) that includes the number of full data EHI exports requests processed during the reporting period and reported by the following subgroups: (1) by a single patient EHI export; and (2) by patient population EHI export. We also proposed (88 FR 23841) reports should include a ''yes'' or ''no'' attestation for enabling direct-to-individual EHI exports. We stated that the proposed measure would report on the number of EHI export requests processed by a health IT developer and provide insights on the implementation of the EHI export capability. We refer readers to the HTI–1 Proposed Rule for detailed background on the measure (88 FR 23841).

As stated in the HTI–1 Proposed Rule (88 FR 23841), we also noted in the ONC Cures Act Final Rule (85 FR 25695) that the EHI Export certification criterion in § 170.315(b)(10) does not require ''direct-to-patient'' functionality in order for a developer to demonstrate conformance to the criterion. However, we did not preclude this functionality, and we sought comment as part of the HTI–1 Proposed Rule on whether any products support direct-to-patient EHI Export functionality to inform future policy decisions. We also sought comment on whether it would be valuable for this measure to be reported by ''use case'' for why the data was exported (*e.g.,* moving to another certified health IT system, use for a population health tool), and how feasible would it be for impacted developers to report in this manner. Lastly, we sought comment on whether it would be valuable, and if so, how valuable, for this measure to include reports regarding the types of recipients (*e.g.,* patients, organizations) of the exported data, and how feasible would it be for impacted developers to report this data in this manner.

Comments. Most commenters expressed support of this measure with numerous commenters indicating that this measure is feasible as written and that the burden to report this measure is low. One commenter recommended delay or removal of this measure though did not provide a rationale. One commenter recommended ONC to consider how patient EHI can be best protected upon export, given concern regarding inappropriate use of information. Another commenter recommended creation of patient-facing and provider-facing educational materials in support of this measure. One commenter asked for clarity regarding the term ''processed'' and whether it intended to indicate started or completed. One commenter disagreed with an attestation reporting requirement for functionality that is not required. One commenter who supported attestation asked for clarification on ''direct-to-individual,'' specifying whether the capability should be performed by the patient without any health care provider involvement. One commenter indicated that capturing and reporting ''use case'' does not provide value and did not support this capability while requesting that the ''use case'' and ''recipient''

types be standardized across all health IT developers. One commenter requested clarification of the definition of a ''full data export'' and whether a subset of data in a timeframe or based upon patient request would constitute ''full data'' in the context of this measure.

Response. We appreciate the support expressed by numerous commenters, as well as the thoughtful feedback and suggestions for this measure. However, in our overall efforts to reduce burden, we have not adopted the ''electronic health information export through certified health IT'' measure. We plan to revisit the EHI export capability in § 170.315(b)(10) as a potential measure when this capability is more widely deployed and may propose measures that provide more valuable insights in future rulemaking.

Measurement Area: Public Health Information Exchange

In the HTI–1 Proposed Rule (88 FR 23841), we discussed how the COVID–19 pandemic exposed many gaps and challenges in the nation's public health infrastructure, including a need for more accurate and timely data, increased electronic exchange of patient health information between health care providers and public health agencies, and greater support for vulnerable individuals and communities disproportionally affected by the pandemic.[208] Therefore, in § 170.407(a)(8) and (9), we proposed two measures within the ''public health information exchange'' area for reporting health care providers' use of certified health IT to exchange data with an immunization information system (IIS) (88 FR 23841). We stated that the insights from these measures could help ONC (and HHS more broadly) assess the public health capabilities of certified health IT, and that we believe that more detailed measurement of health care providers' ability to use certified health IT to successfully exchange health information with public health agencies would provide critical data for pandemic response and other public health emergencies.

Comments. We received broad support for the adoption of two measures within the ''public health information exchange'' area. These commenters also encouraged additional public health information exchange measures in future iterations of the Insights Conditions, such as for cancer reporting, electronic case reporting, syndromic surveillance, and electronic laboratory reporting, along with an estimated timeframe for the development and implementation of these measures. A couple of commenters recommended that ONC align future public health information exchange measures with CMS measures. One commenter expressed support and requested clarity on how the information will be used to evaluate performance, or inform policy or other decision making. Another commenter requested ONC to make aggregate responses available to the public.

Response. We thank commenters for their support and agree that the goal is to help measure progress related to certified health IT's ability to support public health information exchange. This data will provide ''insights'' into health care providers' use of certified health IT for public health information exchange that can guide policy efforts to improve these efforts through initiatives such as the CDC Data Modernization Initiative. In this iteration of the Insights Condition, we have focused on immunization related exchange. However, in future rounds, we plan to consider other areas of public health information exchange to include as part of the Program, working with CMS, CDC, and other federal partners as necessary to ensure alignment of measures. As noted in the HTI–1 Proposed Rule (88 FR 23847), we plan to make the measures and the required data documentation reported by health IT developers available to the public.

Comments. One commenter expressed concern on the level of burden required by health IT developers to obtain the necessary data for each measure and recommended requiring only overall administration submission numbers. Another commenter opined on whether engaging with public health agencies to generate some meaningful data might be less burdensome on vendors and their users and may paint a more complete picture of the situation.

Response. We understand the concerns expressed regarding burden and recognize that these measures may require discrete effort on the part of health IT developers. We appreciate the feedback from commenters and made revisions to reduce the burden associated with creating and reporting these measures which are further detailed below in this section of the preamble. This includes removing our proposal to report by age for the ''immunization history and forecast'' measure, providing additional time for implementation by phasing in the measures over two years, and phasing in complex aspects of the requirements (*e.g.,* reporting by age and/or IIS) over a span of three years.

Data from the measures we have finalized in this final rule will provide insights into the level of exchange between certified health IT systems and IISs, to identify opportunities to address gaps or lags discovered. With regards to public health entities having similar measures, the CDC's Immunization Integration Program (IIP) Testing and Recognition initiative, an ONC approved alternative testing method for the ''transmission to immunization registries'' (§ 170.315(f)(1)) criterion, share some similarities to the measures we had proposed and subsequently finalized. We seek to build upon the IIP by expanding the scope of their measures, which cover a sample of jurisdictions, to include all jurisdictions. This expansion would provide national level insights. In contrast to the IIP, ONC's electronic submission of immunization administrations to IISs shall be reported by age categories, which will help interpret the data as IISs are more likely to have mandates for reporting vaccinations given to children and adolescents compared to adults. We also have a unique measure in comparison to the IIP, which measures the total number of vaccine administrations. Developers that participate in the IIP should gain experience that will help them with reporting for the Insights Condition. Regarding the concern whether public health jurisdictions may serve as an alternative source for this data, while an IIS serves as a valuable source to understand vaccination coverage using unique patient records and vaccination histories, not all jurisdictions have access to or the ability to produce the measures that we proposed. Jurisdictions with high performing IISs and staff to support them are more likely to have these data and use them to improve data quality. However, not all jurisdictions have access to these data. Thus, the measures address an important gap in information that can help improve interoperability between health care providers and jurisdictional IISs.

Immunization Administrations Electronically Submitted to Immunization Information Systems Through Certified Health IT Measure

In the HTI–1 Proposed Rule (88 FR 23842), we proposed to adopt in § 170.407(a)(8) a public health exchange measure that would report on the volume of immunization administrations electronically submitted

[208] Dixon BE, Rahurkar S, Apathy NC. Interoperability and health information exchange for public health. In Public health Informatics and information systems 2020 (pp. 307–324). Springer, Cham. *https://doi-org.ezproxyhhs.nihlibrary.nih.gov/10.1007/978-3-030-41215-9_18.*

to an immunization information system through certified health IT. We stated that this measure would capture the use of certified health IT to send information on vaccination and immunization administrations to an IIS. Specifically, the proposed ''immunization administrations electronically submitted to an immunization information system through certified health IT'' measure would require developers of certified health IT with Health IT Modules certified to the ''transmission to immunization registries'' (§ 170.315(f)(1)) criterion to report on the number of records of immunizations administered that were sent electronically to an IIS during the reporting period. We proposed that developers of certified health IT with Health IT Modules certified to § 170.315(f)(1) that do not have users that administered immunizations during the reporting period would attest that they are unable to report on this measure.

We stated that the intent of the measure is to ensure that ONC has the information necessary to assess whether Health IT Modules certified to § 170.315(f)(1) are being used to support electronically sending vaccination information data to IISs, which has proven to be critical to public health preparedness and response.

For the numerator, we proposed (88 FR 23842) developers of certified health IT with Health IT Modules certified to § 170.315(f)(1) report the number of immunization administrations from which the information was electronically submitted to an IIS successfully during the reporting period by IIS and age group. We proposed (88 FR 23842) that the numerator and denominator counts would be reported overall (across IIS and age subgroups) and by the following subgroups: (1) number of administrations by IIS; and (2) number of administrations by IIS and age group (adults (18 years and over) and children/infants (17 years and under)). We defined a successful submission to an IIS would be the total number of messages submitted minus acknowledgments with errors (2.5.1, severity level of E). We stated that we believe this definition will avoid limitations from IIS jurisdictions that do not send HL7 Acknowledgment messages (ACKs) for this measure. Given that, we proposed that ACKs with an error (severity level of E) [209] would not be counted, and we sought comment on whether ACKs with a warning (severity level W) should still be counted in the numerator. We also sought comment (88 FR 23842) on whether the number of immunizations administered can be linked to immunizations submitted to the IIS, effectively creating a subset of the numerator (immunizations administered). Additionally, we sought comment (88 FR 23842) on whether a successful submission should be counted if a health care provider is able to successfully submit to at least one registry, as opposed to all the registries they submitted to (*e.g.,* health care providers who operate in multiple states sending data for the same administration to multiple IISs). In the Proposed Rule (88 FR 23842), we also considered whether ''replays,'' which involve resubmitting administrations until they are successfully submitted, qualify as a successful submission. In other words, we sought comment on whether successful submissions should be limited to the first attempt to submit.

We proposed (88 FR 23842) the denominator for this measure to be the number of immunizations administered during the reporting period, and that the denominator be stratified by the following subgroups: (1) number of administrations reported to each IIS; and (2) number of administrations reported to each IIS, by age group (adults (18 years and over) and children/infants (17 years and under)). Given the variation in immunization reporting requirements and patient consent by state or jurisdiction, reporting of administrations by IIS is critical to interpreting the data correctly, therefore we proposed this measure to be stratified by IIS. In addition, given that immunization requirements are different for children and adults, we proposed stratifying by age group as well. To further inform public health exchange efforts, we also sought comment (88 FR 23842) on whether adolescents/infants should be further stratified by age, and by what age limits. For providers who operate in multiple states, and thus would be sending data for the same administration to multiple IIS, we sought comment (88 FR 23842) on whether a successful submission should be counted if a provider is able to successfully submit to at least one registry versus all the registries to which the provider submitted. As stated in the HTI–1 Proposed Rule (88 FR 23843), the data collected for this measure would enable ONC to calculate the percent of immunizations administered where the information was electronically submitted to an IIS.

Comments. The majority of commenters supported the proposed ''immunization administrations electronically submitted to an immunization information system through certified health IT'' measure, stating that these reporting metrics will encourage providers to institute proven best practices for obtaining consent and report vaccinations where consent is received. Commenters also stated that organizations using certified health IT would benefit, as it would provide aggregate numbers and user-friendly reports, and help detect connectivity interruptions, as well as help federal agencies, public health agencies, and health IT developers better understand the extent to which health IT is exchanging data with an IIS. A commenter also stated that this would provide real-time and comprehensive data on immunization coverage, facilitating targeted interventions, and contribute to overall population health protection. One commenter recommended that ONC and CMS continue collaborating to consider how their measures can be analyzed and interpreted in tandem to answer questions about data exchange, as well as to collaborate on additional future public health measures.

Response. We thank commenters for their support of the measure and agree with the potential benefits of a measure that assesses how Health IT Modules certified to the ''transmission to immunization registries'' (§ 170.315(f)(1)) criterion are being used to support electronically sending vaccination information data to an IIS. This criterion has proven to be critical to public health preparedness and response. We believe this measure can provide insights beyond current physician surveys limited by small sample size that do not provide information on actual usage of functionality that supports electronically sending vaccination data to an IIS.

Comments. Several commenters expressed concern regarding the burden related to this measure. Commenters representing health IT developers recommended we delay the patient age and IIS stratifications from the measure and proceed with the overall administration submission numbers, due to the high burden level rating for these stratifications. Other commenters expressed support on the age group stratifications as proposed and did not believe any additional age group stratifications were necessary, stating that it may add unnecessary complexity

[209] HL7 Version 2.5.1. Implementation Guide for Immunization Messaging. Release 1.5. October 1, 2014. *https://www.cdc.gov/vaccines/programs/iis/technical-guidance/downloads/hl7guide-1-5-2014-11.pdf.*

to the measure. One commenter suggested eliminating the measure. Another commenter stated that since API access can be measured at either endpoint of the transaction, ONC should request this information from the IIS rather than from providers. One commenter recommended to lessen the burden, ONC could provide standardized value sets for use by all vendors in the counting of mandatory immunization requirements across the nation, however, the commenter conveyed that the necessary work for this effort would outweigh the benefits.

Response. We appreciate the support expressed on the stratifications and have finalized the IIS and age stratifications as proposed. The IIS stratification is critical for assessing both the interoperability and exchange of information between certified health IT and immunization information systems as well as the extent to which health care providers are engaging in immunization reporting. Examining these data by IIS will allow us to monitor the evolving state of immunization data exchange as efforts are made to modernize public health information technology. Additionally, public health jurisdictions will obtain data which they currently don't have access to, and understand the extent to which certified health technology is used for immunization reporting. Therefore, we have kept the proposed IIS stratification. We also believe stratifying by age is important for the purpose of interpreting the results. Public health jurisdictions commonly mandate immunization reporting for children, but do so less for adults. Without the age stratification, it would be difficult to assess whether high or low rates of submission were due to differences in requirements related to adults versus children or another reason (*e.g.,* issues with exchange between certified health IT systems and IIS). Thus, we kept the proposed stratification for age to provide insights on trends related to reporting immunizations for adults and children.

However, we also understand and acknowledge the concerns expressed for the resources required to develop stratifications for this measure. In response to commenters, we have updated the implementation timelines to provide additional time for compliance by phasing in the stratifications (IIS and age) by an additional year and refer readers to the Insights Conditions and Maintenance of Certification section (III.F.3) for a detailed discussion of timelines and the phasing in of measures in this final rule.

We appreciate the comment inquiring about the potential role to leverage public health APIs to support measurement. The measure focuses on data submitted via certified health IT and note that the suggested use of public health APIs for measurement is currently outside the scope of the Program, and not all public health entities may have APIs to support this type of measurement.

We also clarify that the measure does not require logic customized to individual jurisdiction reporting mandates. As noted in the HTI–1 Proposed Rule (88 FR 23842) the number of immunizations transmitted to an IIS will reflect the provider organization's existing practices to transmit this data in accordance with jurisdictional requirements. Therefore, we do not see an immediate need to create a value set that would express those requirements. However, we may explore this suggestion in the future rulemaking to reduce burden.

Comments. One commenter requested clarification on whether the age to be used for counting purposes is the age at the time of immunization administration or at the time the information is transmitted to the IIS. Another commenter recommended that adolescent data extend through age 18, rather than to age 18, to align with the Vaccines for Children program age ranges, as well as requested expectations for jurisdictions that either have limited adult reporting or have an adult ''opt-in'' model, as these jurisdictions will likely have a low level of reporting.

Response. We thank commenters for their feedback. In response to comments, we have modified the age categories for clarity. In alignment with the CDC's Vaccines for Children program, we have modified the age stratifications to the following two categories: (1) immunizations administered for patients 18 years of age and younger (children and adolescents) and (2) immunizations administered for patients 19 years of age and older (adults). We are aware that age-related requirements vary by jurisdiction but for the purposes of standardization and ease of reporting, we have opted to align our requirements with the CDC's Vaccine for Children Program. Patients in the measure's metrics should be counted based on age at time of administration. We acknowledge that a relatively small number of patients may fall into separate counts if the date of immunization is close to the end of the reporting period, but we expect that these instances should not significantly impact the metrics calculated.

Comments. One commenter recommended that timeliness should be added to this measure's numerator and stratify the measure by the definition of ''timely'' to be less than or equal to 24 hours to provide health IT developers, providers, and public health agencies with insights into how rapidly immunization data is being shared with IIS registries and accessed by health agencies.

Response. We appreciate the recommendation to factor timeliness and agree this plays a critical role in data quality and utility. We may consider this aspect for future potential measure enhancements as we seek to appropriately factor variation in provider workflow and jurisdictional reporting requirements.

Comments. One commenter requested clarification on whether a message is a failure or success if the initial message for a vaccination administration is successful, but the administration is updated in the EHR, and the update message fails. One commenter suggested collecting how many submissions needed to be repeated. Several commenters stated that replays should qualify as a successful submission since there are scenarios that could create a submission failure at no fault of the developer, and immunization submitters should be recognized for successful error remediation. One commenter recommended that ''replays'' are considered successful submissions, but each replay of a single immunization administration should not be counted as a separate submission, as overcounting may result in inflating the numerator of the measure.

Response. We thank commenters for their feedback. The intent of the measure is to understand the process of submitting immunization to an IIS and efforts by health care providers to successfully submit immunization administrations to an IIS. While the process and effort can involve resolving message failures, the measure counts the number of immunizations administered that are submitted to the IIS, rather than the number of attempts to successfully transmit the immunization. With this in mind, we clarify that, in the instance where the initial message for an immunization administration is successful and a subsequent update in the EHR has an update message that fails, the metrics for the number of immunizations administered that were electronically submitted successfully to IISs overall, by age category and IIS should reflect the final status of the immunization submission to the IIS. There should not be two counts in these metrics for the successful initial

message and the subsequent failure update message. We expect that the shift to calendar year reporting will minimize instances where the final status of successful vaccine submissions would not be available to count in the measure. Therefore, the measure will count the status of the final submission at the time the reporting period ends in these metrics, rather than counting each attempt separately. This applies to replays, which should not count as separate submission attempts in these metrics. Although this measure will not separately document the number of replays, we agree with commenters who supported counting replays and multiple messages as separate attempts to successfully submit an immunization and may consider future measures that would document the level of effort taken for successful error remediation. We encourage those reporting on this measure to include counts of replays in the supplemental documentation as this could shape future iterations of this measure.

Comments. Several commenters expressed support that those acknowledgements with a severity level of ''E'' be considered a failure for purposes of the measure's numerator. The commenters added that acknowledgements with the severity level ''W'' should not be considered a failure, given that they were likely successfully processed by the IIS and their data accepted by the immunization program. However, another commenter noted the possibility that including acknowledgements with the severity level ''W'' could inflate the measure and make interpretation challenging. One commenter requested confirmation that only ''E'' responses should be subtracted from the success acknowledgements and noted it would be helpful for ONC to define the concepts of error and warning responses in the context of this measure. One commenter stated that there is variation on how the error status of level ''E'' is used in practices, noting that this would likely make the aggregated data ONC proposes to report less than accurate, and requested clarification on whether the purpose of the use of error and warning messages in this context is to assess whether immunization registries are functioning effectively. One commenter recommended that the successful submission definition be revised to reflect that no negative acknowledgement is a successful submission, until an alternative mechanism is used to route acknowledgements from the registry back to the EHR.

Response. We thank commenters for their feedback. We appreciate the comment that acknowledgements from IIS with a severity level of ''W'' could potentially inflate the measure and acknowledges the variation on how ''E'' is used in practices. We intend to collaborate with the community to monitor how these instances may impact the interpretation of the measure and determine if it should be revised in the future. We also appreciate commenters requesting confirmation that the measure should consider acknowledgements with a severity level of ''E'' as a failed message. We confirm that this is the only severity level for messages that should be excluded from the measure's metrics for the number of immunizations administered that were electronically submitted successfully to IISs overall, by age category and IIS. We thank commenters for their consideration of the implications for error status level ''E.'' We confirm that successful submissions are defined as the total number of messages submitted to an IIS, minus acknowledgements with errors (2.5.1, severity level ''E''). For these metrics, we clarify that not all immunizations that are administered and submitted during the period may receive a status of the submission acknowledgement message from an IIS during the reporting period. In this situation (where an acknowledgement from an IIS is not received), the immunization submission should be counted as successful. We request that health IT developers report the number of submissions that did not receive acknowledgement in the supplemental documentation so these metrics can be refined in the future if needed.

Comments. A few commenters stated that a successful submission should be counted if a health care provider is able to successfully submit to all of the registries to which the provider submitted, including submissions to more than one IIS, stating that the inflation of the count would be minimal.

Response. In response to comments, the metrics for the number of immunizations administered that were electronically submitted successfully to IISs overall, by age category and IIS, indicate that each successful submission to an IIS to which a provider submits immunizations should be included and counted as a successful submission. Thus, an immunization that is successfully submitted to more than one IIS would be counted the number of times it was successfully submitted to each IIS. When the stratified metric is reported by IIS, the count inflation should not be an issue as the multiple submissions would be separated by IIS.

Comments. Several commenters requested clarification on the denominator counts. One commenter requested clarification on whether a patient who opts out of having certain administered immunizations submitted to the IIS should be included in the denominator, as well as if an immunization is ordered but refused by the patient. The same commenter also requested clarification on whether the denominator includes administered vaccines from provider organizations that do not yet have connectivity in place to an IIS for reporting administered vaccines. One commenter recommended that the denominator exclude the number of patients who have opted out of vaccination reporting to capture more accurately the proportion of immunization administrations electronically submitted.

Response. We thank commenters for their request for clarification. We clarify that the measure focuses on counting immunizations administered and submitted. Patients who have been administered an immunization and opt out of submitting their data to an IIS should count in the metrics for the number of immunizations administered overall, by age category and IIS, but not the metrics for the number of immunizations administered that were electronically submitted successfully to IISs overall, by age category and IIS. To ease burden and given the assumption that the number of opt-outs are relatively low, we believe it is sufficient to include them. However, there may be value in counting the number of opt-outs in the future to determine whether it is worth removing them (or separately report on these). Patients who decline an immunization will not appear in the metrics for the number of immunizations administered overall, by age category and IIS, and there will be no immunization submission to count in the metrics for the number of immunizations administered that were electronically submitted successfully to IISs overall, by age category and IIS. We also clarify that immunizations administered at health care provider organizations that have certified health IT eligible for reporting but do not have an existing, active connection to electronically submit immunizations to an IIS will count in the metrics for the number of immunizations administered overall, by age category and IIS, while there will be no count in the metrics for the number of immunizations administered that were electronically submitted successfully to IISs overall, by age category and IIS. This approach

will contribute to insights on the number of immunizations that could be electronically submitted to reduce provider burden associated with manual submission.

Comments. One commenter stated that stratifying the denominator (number of immunizations administered within the reporting period) by IIS does not make sense since an IIS is not identified with an immunization administration. One commenter expressed concern stating that an EHR is unlikely to know of administrations reported to an IIS through a web portal or alternate mechanism and recommended that the measure should instead be out of the total number of doses administered how many doses were submitted electronically, and of those electronically submitted, how many were successful. A couple of commenters recommended that the number of administrations reported to each IIS should be revised to number of administrations valid for reporting to each IIS to ensure that the count of doses sent electronically only include those doses tagged as newly administered. Another commenter requested guidance on how doses should be counted in the metrics if two EHR systems merge, and another requested clarification on how data submitted from a non-traditional location should be counted.

Response. The metrics for the number of immunizations administered overall, age category and IIS, is stratified or reported by IIS because we seek to assess the extent to which an IIS is receiving data on immunizations administered. While the location of the patient typically determines the IIS to which vaccine administration information is sent, given that it is unclear as to which data sources may be easily accessible to make this determination, we provide two options regarding how best to select the IIS for those vaccines that are administered but not submitted: (1) based upon the primary IIS used by the client site; or (2) based upon the jurisdiction associated with the client site's location. Whatever approach is used should be documented in the required documentation for this measure. We note that the stratification by age in the total vaccines administered within the reporting period enables comparisons with the vaccines submitted electronically metric.

We clarify that the measure pertains to immunizations electronically submitted to IISs through certified health IT. Immunizations submitted via web portals or alternate mechanisms, such as manual submission of spreadsheets, would not be reported in the immunizations submitted electronically metrics, but, given that these were administered but not electronically submitted via certified health IT, they would be included in the metrics for the number of immunizations administered overall, age category and IIS. We do not believe it is feasible to remove these from the total vaccines administered metrics; however, if available, the volume of immunizations could be noted in the health IT developer's supplemental reporting to provide additional insight and context.

We also appreciate the requests for clarification on whether doses tagged as newly administered are included. We acknowledge that the ''transmission to immunization registries'' (§ 170.315(f)(1)) criterion includes historical vaccines and newly administered vaccines, giving health IT developers that certify to this criterion the capability to report both. We note this treatment of historical vaccines administered applies to data migrated from one EHR to another, and vaccines that were previously administered by another provider site. Because the proposed measure referred to administered immunizations (and not historical specifically), we clarify that the finalized measure will only count immunizations newly administered during the reporting period and will not count historical vaccines previously administered that were recorded during the reporting period. The inclusion of historical vaccines in addition to newly administered vaccines within one measure would be difficult to interpret; in the future we may consider the inclusion of historical vaccines based upon industry experience and the input we have received. The measure is not constrained to the type of health care provider who administered the vaccine or the location the vaccine was administered, provided the certified health IT is eligible for reporting.

Comments. One commenter requested clarification whether the immunization administration would have to be within the reporting period or the IIS submission in the reporting period (or both).

Response. For the metric, immunizations administered that were electronically submitted successfully to IISs, immunizations should be both administered and submitted during the reporting period. An immunization administered outside the reporting period but submitted during the reporting period would not count for these metrics. We note that if no acknowledgment is received for immunizations administered, and submitted during the reporting period, then the immunization would count as successfully submitted.

Comments. One commenter requested clarification on whether health IT vendors will be required to calculate a percentage and if so, requested ONC provide explicit guidance on the calculation components.

Response. We clarify that ONC will be responsible for calculating percentages based on the counts that health IT developers submit.

Finalization of Measure

We have finalized the measure as ''immunization administrations electronically submitted to immunization information systems through certified health IT'' in § 170.407(a)(3)(vi). We have revised the proposed measure based on public comments received. Specific metrics to support this finalized measure are listed below and described in the accompanying measure specification located on ONC's website. We also note that if regulatory baselines associated with the metrics change in the future—such as a revision to a criterion through notice and comment rulemaking—the measure specification would also be changed to ensure alignment with the revised criterion. The reporting period for the measure and related metrics below consists of one calendar year. Data collection for the measures and associated metrics will begin during the first and second phases of reporting (which is described later in the preamble):

1. Number of immunizations administered overall (year 1),
2. Number of immunizations administered overall by IIS and age category (year 2).
3. Number of immunizations administered that were electronically submitted successfully to IISs overall (year 1),
4. Number of immunizations administered that were electronically submitted successfully to IISs overall, by IIS and age category (year 2).

Immunization History and Forecasts Through Certified Health IT Measure

In the HTI–1 Proposed Rule, in § 170.407(a)(9), we proposed to adopt a public health information exchange measure to require reporting on the number and percentage of IIS queries made per individual with an encounter (88 FR 23843). The ''immunization history and forecasts'' measure would capture the use of certified health IT to query information from an IIS under the ''transmission to immunization

registries'' (§ 170.315(f)(1)) criterion. Therefore, we proposed (88 FR 23843) that developers of certified health IT with Health IT Modules certified to § 170.315(f)(1) would be required to report for this measure. We emphasized that understanding whether health care providers are engaging in electronically querying immunization information from IIS is critical to public health preparedness.

For the numerator, we proposed (88 FR 23843) developers of certified health IT with Health IT Modules certified to § 170.315(f)(1) report the number of query responses received successfully from an IIS overall and by subgroup, by IIS and age group (adults (18 years and over) and children/infants (17 years and younger)) during the reporting period. The definition of a successful response from an IIS should be the total number of messages submitted minus acknowledgments with errors (2.5.1, severity level of E). However, since HL7 Z42 messages contain both immunization history and forecast, whereas Z32 messages exclusively contain history, we sought comment (88 FR 23843) on whether both message types should be included in the measure numerator.

As stated in the HTI–1 Proposed Rule (88 FR 23843), the first denominator we proposed for this measure would be the total number of immunization queries overall and by subgroup, by IIS and age group (adults (18 years and over) and children/infants (17 years and younger)) during the reporting period. We proposed to add this denominator to the measure proposed by the Urban Institute to provide data on the total number of query responses that are and are not successfully received from an IIS, as this will give further insights into any potential technical challenges that may be occurring during query exchange. The second denominator we proposed for this measure would be the total number of encounters overall and by subgroup during the reporting period. However, since it is unlikely that queries happen for every patient encounter, we sought comment (88 FR 23843) on whether the second denominator should capture to total number of applicable patient encounters during the reporting period regardless of whether a query was sent to an IIS. We proposed (88 FR 23843) that the numerator and denominator counts would be reported overall (across IIS and age subgroups) during the reporting period and by the number of IIS queries made by IIS and age group (adults (18 years and over) and children/infants (17 years and younger) during the reporting period. In the HTI–1 Proposed Rule (88 FR 23843), we conveyed our belief that reporting by these subgroups would be necessary to interpret the data and create public awareness that could inform IISs and other public health participants about the progress being made in immunization data exchange. We sought comment (88 FR 23843) on whether children/infants should be further divided and by what age limits.

We also proposed (88 FR 23843) developers of certified health IT with Health IT Modules certified to § 170.315(f)(1) would attest that they are unable to report on this measure if they have no users that administered immunizations during the reporting period. There may also be providers who do not administer immunizations but would want to query an IIS to determine whether their patient has received a vaccination. We sought comments (88 FR 23843) on whether we should include this exclusion or suggestions on how we could better refine it.

Comments. A few commenters expressed support for the proposed measure, stating that comprehensive immunization history and forecasts through certified health IT enables health care providers to proactively manage immunization programs and promote preventative care. Also, by utilizing certified health IT to track history and generate forecasts, health care providers can identify immunization gaps, schedule timely vaccinations, and implement outreach initiatives to increase vaccination rates.

Response. We thank commenters for their support of the proposed measure and appreciate the examples of how the measure would support improvements in preventive care for patients. We agree that this measure, which provides insights on how certified health IT is used to support health care providers to electronically query immunization information from IIS, is critical to public health preparedness.

Comments. One commenter expressed concern with the second denominator, stating that the total number of visits will not accurately reflect the number of immunization query messages expected to be generated, as not all encounters can reasonably be expected to result in a query message, and suggested an alternate measure to include a numerator defined as the total number of unique individuals queried for during the reporting period and a denominator defined as the total number of unique individuals with encounters during the reporting period. Another commenter recommended that ONC develop a simpler definition of encounters that developers can apply to their own systems and encounter classification structures or establish a clear set of encounter type categories with fully defined mapping such as OMB/CDC Race categories/details. The same commenter suggested ONC coordinate with CMS to ensure that the value set references include all SNOMED and CPT codes in the proposal or identified alternatives. One commenter recommended modifying the second denominator to include encounters with immunizing provider sites rather than all encounters.

Response. We concur that not all encounters can be expected to generate a query to an IIS. Therefore, as one commenter noted, the number of visits may not reflect the number of immunization queries expected. We may collaborate with the community to consider the measure of unique patients for whom queries were made to the IIS for future rulemaking. The measure does not include encounter-based metric from the immunization measure domain to address the concern raised by commenters that not all encounters can be expected to result in a query message. We will still receive counts of the number of unique patients with an encounter during the reporting period, as proposed (and finalized) in the ''consolidated clinical document architecture (C–CDA) problems, medications, and allergies reconciliation and incorporation through certified health IT'' measure. We refer readers to the definition of terms section immediately following this section for a more detailed discussion on defining encounters.

Comments. A few commenters expressed concern with the intent and interpretation of the proposed measure. One commenter stated that if the intent is to assess the overall functioning of bidirectional query, ONC should clarify this intent such that a low ratio does not reflect poorly on the developer of certified health IT or the querying organizations. One commenter commented that it was their experience that some IISs are not ready to return the data for response to the query and noted that this would impact the countable events for this measure and should be publicly disclosed if/when the data is published. One commenter recommended that these measures be considered exploratory and should not be used to penalize any certified health IT product or developer.

Response. We acknowledge that some IIS are not able to return data for a query response and as such, agree that the finalized measure should be seen as informative and reflects the role that the health IT developers, health care

providers, and IIS systems play with the exchange of this information. We acknowledge that an IIS may have issues in returning the data for response to the query, thus impacting the value of this measure. We recognize this contextual information will be important to note with the publication of these data. Where health IT developers encounter instances where a complete bidirectional loop is not possible, we encourage health IT developers to document this information in the supplemental reporting to allow for more complete understanding of the metrics.

In this finalized measure, counts of queries sent to an IIS and responses received successfully are intended to provide insight on the functioning of bidirectional query to obtain immunization data. The metrics reported by health IT developers will provide new insights for ONC and the public health community that are currently unavailable at a national level. By understanding trends related to queries made and responses received over time, we will also gain feedback on the performance of queries and responses, which are part of the ''transmission to immunization registries'' (§ 170.315(f)(1)) criterion. As noted above, we will receive counts of the number of unique patients with an encounter during the reporting period, as proposed (and finalized) in the ''consolidated clinical document architecture (C–CDA) problems, medications, and allergies reconciliation and incorporation through certified health IT'' measure, and expect to use this data to provide encounter context to the ''public health information exchange'' measures. Together, these metrics can inform efforts to increase the availability of IIS data for health care providers to have a more complete immunization background for individuals and groups of patients. We plan to collaborate with the community to consider the measure of unique patients for whom queries were made to the IIS for future rulemaking.

Comments. Several commenters requested clarification on the proposed numerator. One commenter noted that the proposed numerator reflects the interoperability of the IIS, not the certified health IT, and requested clarification on ''received,'' stating that the successful response definition is not clear in cases where the error can be detected by the certified health IT in the IIS response such as ''received technically'' versus ''received into the chart.'' A few commenters requested clarification on how ''refines'' are counted for measurement, when a query attempt must be refined before a successful attempt, and suggested the numerator should reflect total queries performed.

Response. We appreciate the concern expressed that the metric does not reflect the interoperability of certified health IT. Through our measures we seek to assess bidirectional exchange activity between IIS and certified health IT, which can help identify potential issues related to interoperability and track trends over time. We appreciate the comments and the opportunity to provider greater clarity. In this final rule, we clarify that the metrics for the number of query responses received successfully from IISs overall, and by IIS, should count an IIS response as ''received technically,'' in the form of a message or transaction. This clarification addresses that health care providers may not ingest all responses into the record. We agree that the initial query and each refined query should individually increment the total number of immunization queries sent to an IIS in order to acknowledge the effort to ensure a successful query.

Comments. A couple commenters expressed support that acknowledgement with a severity level of ''E'' be considered a failure for purposes of the measure. One commenter noted that an error with a severity level of ''E'' could be included in either an acknowledgment or a response (RSP) message. A couple commenters noted that a significant portion of messaging failures are communication failures where there will be no response received which should be excluded from the denominator or included in a separate metric. The commenter suggested that messages of ''no patient found'' or ''too many patients'' found, as well as messages with no response from the IIS (in the case of downtime, for example), would be considered successful. One commenter requested clarification on whether a query response message responding that a patient match was not possible should be counted in the numerator. The commenter also suggested that the submission of descriptive context should be required, stating that it may help with future evolution and fine tuning of the measures.

Response. We appreciate the comments received regarding that the measure should consider acknowledgements with a severity level of ''E'' as a failed message. We confirm that only severity level of ''E'' for messages are excluded from the metrics, the number of query responses received successfully from IISs overall and by IIS. We also appreciate the additional description of communication failure scenarios due to IIS downtime or other accessibility issues. We will collaborate with the community to monitor how these instances impact the measure's interpretation and determine if it should be revised in the future. At this time, we will not require health IT developers to provide separate counts for communication failures and counts of the descriptive context levels. We encourage health IT developers to capture information about communication failures as their functionality permits and include this explanation in the supplemental documentation.

Comments. In our request for public comment regarding whether both Z42 and Z32 messages should be included in the metrics, several commenters suggested that both Z42 and Z32 messages be included, stating that both are objectively relevant to patient care, contain significantly similar content, and have both been implemented in the real world.

Response. Given the support expressed in response to our specific question, the metrics, the number of query responses received successfully from IISs overall and by IIS will include Z42 and Z32 messages.

Comments. Commenters representing health IT developers expressed concern related to the proposed measure's stratification by IIS and age. These commenters suggested that the initial implementation of the measure should only require administration submission counts and that the development burden was high relative to the value of the stratifications. Other commenters supported the stratifications as defined, given that not all jurisdictions require comprehensive adult reporting. One commenter noted that additional age stratification was unnecessary and might add complexity. One commenter suggested delaying or eliminating the ''immunization history and forecasts'' measure.

Response. We appreciate the comments that indicated support for the measure's proposed stratifications, but that development burden would be high especially associated with the age stratification. We acknowledge that the age stratification is not as critical early on for this measure (compared to the submission of immunization data) as there are no state and jurisdiction level mandates for querying history and forecasts which vary by age. Therefore, we have delayed the implementation of this measure from ''year 1'' to ''year 2'' to provide health IT developers more time to produce the measure.

Furthermore, the reporting by IIS will be delayed to ''year 3.'' We have not removed this measure as suggested by one commenter as there was a high level of support for this measure and we are providing additional time to implement the metric and related stratification.

Comments. One commenter requested clarification on how a query sent to multiple IIS should be counted. One commenter requested clarification on whether the first denominator should include only query response messages that support both the history and forecast. One commenter requested clarification on whether developers would be required to calculate a percentage and if so, ONC must provide explicit guidance on the calculation components.

Response. We clarify that the metrics related to the total number of immunization queries sent (overall and by IIS), should be incremented for each query sent to an IIS and the metrics related to number of query responses received successfully from an IIS (overall and by IIS), should increment for each successful message received. The measure should count queries and response messages so that the increment occurs for history, forecast, or history and forecast. This approach is supported by the ''transmission to immunization registries'' (§ 170.315(f)(1)) criterion that treats forecast and history separately. At this time, health IT developers are not required to report separate metrics for forecast and history. We clarify that ONC will calculate percentages based on the counts that the health IT developer submits.

Comments. One commenter stated that they did not agree with excluding queries performed by health care providers who do not administer immunizations, while another commenter recommended excluding these health care providers for simplicity.

Response. We acknowledge that the suggestion to constrain the measure to only include health care providers who immunize simplifies the interpretation of results. However, the National Vaccine Advisory Committee (NVAC) recommends that all healthcare professionals, regardless of whether they administer vaccines, routinely assess patients for vaccines due.[210] Furthermore, there was no consensus across the comments to make this change. In this phase of reporting, it may add burden for health IT developers to segment the measure by whether the health care providers are immunizing providers. Therefore, the measure does not make distinctions for health care providers who do and do not administer immunizations and will collaborate with the community to understand the potential to incorporate this aspect in future rulemaking.

Finalization of Measure

We have finalized the measure as ''immunization history and forecasts through certified health IT'' in § 170.407(a)(3)(vii). We have revised the proposed measure based on public comments received. Specific metrics to support this finalized measure are listed below and described in the accompanying measure specification located on ONC's website. We also note that if regulatory baselines associated with the metrics change in the future—such as a revision to a criterion through notice and comment rulemaking—the measure specification would also be changed to ensure alignment with the revised criterion:

1. Number of immunization queries sent to IISs overall (year 2).
2. Number of immunization queries sent to IISs overall by IIS (year 3).
3. Number of query responses received successfully from IISs overall (year 2).
4. Number of query responses received successfully from IISs overall by IIS (year 3).

The reporting period for the measure and related metrics above consists of one calendar year. Data collection for these measures and associated metrics will begin during the second and third phase of reporting (which is described later in the preamble).

Encounters

For measures where patient encounters are relevant, we proposed the definition of an encounter should be based on the National Committee for Quality Assurance (NCQA) outpatient value set and SNOMED CT inpatient encounter codes. For outpatient codes, developers should use NCQA's Outpatient Value Set.[211] [212] For inpatient codes, developers should use SNOMED CT codes 4525004, 183452005, 32485007, 8715000, and 448951000124107.[213] Listed below is a description of each SNOMED CT code:

- Emergency department patient visit (procedure)—4525004
- Emergency hospital admission (procedure)—183452005
- Hospital admission (procedure)—32485007
- Hospital admission, elective (procedure)—8715000
- Admission to observation unit (procedure)—448951000124107

Comments. Several commenters requested guidance for implementation of encounter value sets. Commenters representing health IT developers suggested adopting a broad definition of encounters for developers to apply and map to their own classification structures, while others suggested constraining the codes to a more limited and defined set. One commenter suggested limiting inpatient encounter codes to discharges only.

Several commenters supported the proposed approach (FR 23832) to align Insights Condition value sets for encounters with CMS programs. Commenters representing quality measure developers supported the proposed value sets that are used in electronic clinical quality measures (eCQMs). While calling for alignment with CMS programs, several commenters representing health IT developers recommended that the encounter value sets should follow industry standards, such as the FHIR Encounter.type field in the US Core Implementation Guide.[214]

Response. We agree with commenters on the importance of aligning encounter value sets with industry approaches as well as re-using existing value sets that support CMS programs to reduce the burden of developing and reporting Insights Condition measures. In the HTI–1 Proposed Rule (88 FR 23832), we proposed to define encounters leveraging a code set defined by the National Committee for Quality Assurance and recommended by the HITAC, while requesting comment on alternative approaches. We proposed this approach in large part to align with existing measurement approaches used within CMS programs. As commenters described, not all codes included in the proposed approach are reflected in the US Core IG version 6.1.0, which is the version we believe commenters referenced. Based on public comment, we have revised the definition of encounters to maintain alignment with

[210] NVAC Standards for Adult Immunization Practice: *https://www.cdc.gov/vaccines/hcp/adults/for-practice/standards/index.html.*

[211] See: 2022 Quality Rating System Measure Technical Specifications. Published October 2021. *https://www.cms.gov/files/document/2022-qrs-measure-technical-specifications.pdf.*

[212] NCQA's Outpatient Value Set is available with a user ID and login at *https://store.ncqa.org/my-2021-quality-rating-system-qrs-hedis-value-set-directory.html;* or *https://vsac.nlm.nih.gov/valueset/expansions?pr=all* OID: 2.16.840.1.113883.3.464.1003.101.12.1087.

[213] Available for search at *https://www.findacode.com/index.html.*

[214] *https://build.fhir.org/ig/HL7/US-Core/index.html.*

definitions of encounters within existing quality measurement approaches used by CMS while responding to industry concerns about burden and potential misalignment. Specifically, several CMS programs, including the Promoting Interoperability Program and the Quality Payment Program, require the counting of encounters using specific codes, and CMS maintains an CQM library that specifies specific encounter codes related to quality measurement.[215] Developers of certified health IT have years of experience with those reporting efforts. Specifically, health IT certified to any criterion in § 170.315(c)(1) through (4) supports recording, importing, reporting or filtering CQMs, and health IT certified to § 170.315(g)(1) or (2), supports numerator recording and measure calculation for each Promoting Interoperability Program percentage-based measure. For the purpose of the Insights Condition, we define applicable encounters as all encounters that the developer includes in its calculation of encounters within the existing certification criteria in § 170.315(g)(1) or (2) and the CQMs that they have presented for certification as part of certification to § 170.315(c). For those developers that do not attest to any of the certification criteria at § 170.315(c), (g)(1) or (2), we specify that they include all encounters regardless of encounter code. Based upon analysis of the Certified Health IT Product List (CHPL), we note that of the 306 products currently certified to § 170.315(b)(2), 281 are certified to at least one of the included criteria, with 232 certified to criterion in § 170.315(c) and 260 certified to § 170.315(g)(1) or (g)(2).

In finalizing this approach, we have eliminated the prescriptive approach to defining value sets that delineate encounters taken in the HTI–1 Proposed Rule, which was based on a specific set of quality measures and their associated Value Sets. The finalized approach instead relies on existing developer competencies and experience as demonstrated by their existing certification to any criterion in § 170.315(c)(1) through (4), (g)(1) or (g)(2) while retaining a close link to existing quality measurement. Our goal in finalizing this approach is to build upon existing CMS program requirements, certification criteria, and developer of certified health IT's experience with these requirements. Rather than specify specific value sets, our intent is to allow the definition of an encounter to evolve as use of CQMs and approaches within this Program and the Quality Payment Program change. In finalizing this approach, we have also emphasized alignment with measurement within CMS programs (*i.e.,* eCQM and Promoting Interoperability percentage-based measures) rather than following industry standards, such as the FHIR Encounter.type field in the US Core Implementation Guide. As approaches within CMS' programs come into alignment with industry standards, the measure of encounters within the Insights Condition will also come into alignment. For developers that do not currently support the identification of specific types of encounters, our intent is to avoid creating a new requirement to implement specific terminologies or code sets.

Counts of Unique Patients

Comments. One commenter opposed the use of unique patient counts in the proposed measures under the Insights Condition. Further, the commenter stated unique patient counts when aggregating across many certified health IT instances would require significant burden and cost to deduplicate across customer databases. The commenter requested that ONC either change to transaction-based counts or clarify that unique patient counts will be unique only within each instance of the certified health IT and can be duplicated across instances.

Response. We thank the commenter for this input, and as noted in the individuals' access to EHI measurement area section in this preamble, we have revised our definition of unique patient counts so that counts would only be unique within each instance of the certified health IT. We recognize the potential difficulty of de-duplicating unique patients across more than one instance of a certified health IT and clarify that the patient counts should be unique within the instance and can be duplicative across instances.

3. Insights Condition and Maintenance of Certification—Requirements

As stated in the HTI–1 Proposed Rule (88 FR 23843), the Cures Act specifies that a health IT developer be required, as a Condition and Maintenance of Certification requirement under the Program, to submit responses to reporting criteria in accordance with the ''Electronic Health Record Reporting Program'' established under section 3009A of the PHSA, as added by the Cures Act, with respect to all certified technology offered by such developer. We proposed to implement the Cures Act ''Electronic Health Reporting Program'' Condition and Maintenance of Certification requirements as the ''Insights Condition and Maintenance of Certification'' (Insights Condition) requirements in § 170.407. As a Condition of Certification, we proposed that developers of certified health IT would submit responses to comply with the Insights Condition's requirements, described in this section of the preamble in relation to the Insights Condition's measures and associated certification criteria.

Comments. A number of health IT developers expressed concern about the burden that collecting and reporting measures for the Insights Condition will impose on health IT developers. A commenter stated that developing Insights Condition measures overlaps and competes with health IT developers' other priorities, including CMS' digital quality initiative and user requested analytics. One commenter expressed concern that the requirements would introduce barriers to market entry and reduce competition. However, one health IT developer commented that they do not believe that the Insights Condition presents a significant regulatory burden, as the measure data can be collected and reported using currently widespread technologies.

Relatedly, many commenters, including health IT developers, developer associations, and health systems, opposed the overall number and type of measures proposed in § 170.407 for the Insights Condition. Commenters suggested reducing the number and complexity of measures to reduce burden and improve feasibility for developers of certified health IT and their customers. Commenters stated the number of measures is higher than described due to the multiple numerators and denominators. Commenters recommended ONC remove the list of expected metrics or ratios and focus only on the individual data elements to be collected and reported. Some commenters suggested 10 or fewer counts as a starting point. One commenter indicated that there were duplicate measures in the set that should be combined or harmonized. One commenter recommended that ONC select measures that are well-defined and targeted, and designed not to heavily burden health IT system resources when collecting data. Commenters also suggested gradually increasing the number of measures over several years.

[215] Medicare Promoting Interoperability Program Specification Sheets *https://www.cms.gov/medicare/regulations-guidance/promoting-interoperability-programs/resource-library.*

eCQM Library *https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/eCQM_Library.*

Response. We appreciate the concerns expressed for the potential burden imposed on health IT developers to report the Insight Condition measures. We emphasize the Insights Condition fulfills the Cures Act specified requirements in section 4002(c) to establish an Electronic Health Record (EHR) Reporting Program to provide transparent reporting on certified health IT.

We believe this final rule will address information gaps in the health IT marketplace and provide useful insights on certified health IT use while minimizing implementation burden on health IT developers. Our final rule includes multiple revisions to our proposals, described in greater detail throughout this section of the preamble under their respective sections, that are intended to minimize the burden on health IT developers in implementing the Insights Condition. In sum, for this final rule, we have:

- Delayed the submission of the first phase of measures and related metrics to July 2027 to allow health IT developers adequate time to develop and implement the measures.
- Established a more incremental approach for implementing the measures over a longer timeframe (three years), including phasing in more complex aspects of the measures. Extending the time frame will allow developers to work on other priorities, such as CMS' digital quality initiative and user requested analytics, and not have to exclusively focus on developing Insights Condition measures.
- Not finalized two proposed measures (''electronic health information export through certified health IT'' and ''C–CDA documents obtained using certified health IT by exchange mechanism'').
- Addressed potentially duplicate metrics to make it easier to understand the total number of unique metrics that are required. For example, the same encounter-related metrics were previously listed in the patient access, immunization, and clinical exchange measure specification. Those metrics are now only listed in the clinical exchange section and measure specification.
- Reduced the frequency of measure reporting from semiannual to annual, and changed the submission date for more convenience to health IT developers.
- Provided an alternative reporting approach for health IT developers who are not able to report on their entire customer base due to contractual reasons. This should limit the need to renegotiate contracts for the sole reason of complying with the Insights Condition requirements addressing a major source of burden. This approach is described below in section III.F.4 of this final rule.
- Supported health IT developers who choose to use their Insights Condition measurements and data as part of their Real World Testing plans and results, thus reducing the need to generate separate data for both Conditions of Certification.
- Replaced the terms numerators and denominators, which caused confusion from commenters, with lists of metrics within each measure that health IT developers will be required to report, and limited stratification of measures.
- Consolidated the required Insights Condition measures and related metrics into the table that is located later in this section of the preamble.

We do not believe that the Insights Condition introduces a barrier to market entry. The minimum reporting qualifications we proposed and have subsequently finalized further below in this preamble are designed to ensure that small and startup developers are not unduly disadvantaged by the Insights Condition requirements. Further, the availability of information on what capabilities are widely available or lacking in the marketplace may encourage new entrants to provide needed technologies.

Comments. Several commenters raised concerns that customers of health IT developers will perceive burden and lack incentives that would impact their willingness to allow access to data for health IT developers to report in order to comply with the Insights Condition requirements. A few commenters encouraged ONC to coordinate with CMS on ways to provide insights on EHI access, exchange, and use while reducing physician burden related to requirements for the Insights Condition and the CMS Promoting Interoperability Programs.

Several commenters suggested ONC collaborate with CMS to adopt regulatory requirements to promote customers of health IT developers to agree to allow data from their systems to be used for the Insights Condition. One medical professional society commenter suggested that ONC coordinate with CMS and use the Insights Condition data and metrics to augment CMS physician reporting requirements. Further, the commenter stated the goals of reducing physician reporting burden and providing CMS and ONC insight into EHI access, exchange, or use can be jointly achieved by allowing physicians to attest to meeting CMS reporting requirements, rather than reporting a numerator-denominator, supplemented by health IT developers reported data under the Insights Condition. One commenter stated that attestations exist for agreeing to cooperate with ONC–ACB surveillance activities as a precedent for such an attestation requirement.

Response. We appreciate the suggestion for ONC to collaborate with CMS. We recognize that health care providers in certain CMS programs were expected to attest to cooperate in ''good faith'' with both ONC–ACB surveillance activities and ONC Direct Reviews.[216] [217] We will explore potential opportunities with CMS to encourage support for the Insights Condition among hospitals, physicians and other healthcare professionals that participate in CMS programs. We will also explore potential opportunities with CMS on ways to reduce burden on physicians and other health care providers related to reporting requirements. We will continue to coordinate and work with CMS on points of intersection for potential future rulemaking.

Comments. Several commenters expressed concern that the Insights Condition reporting requirements will lead to increased burden or frustration for health care providers and health care provider organizations and encouraged ONC to consider the impacts of Insights Condition reporting by health IT developers on their customers. Commenters also expressed concerns that health IT developers will 'pass on' the burden of reporting to end users (*i.e.,* health care providers), who will end up being required to assist their developers of certified health IT in collecting data or creating reports for the Insights Condition. Some commenters indicated that health care providers and health care provider organizations are already overburdened with reporting requirements. One commenter expressed concern about creating any additional direct or indirect reporting burden for rural and underserved health care providers. A few commenters suggested to reduce health care provider burden by making healthcare organization participation and data contribution optional and avoid selecting measures that will require mapping of data by the healthcare organization staff. One advocacy organization and a health system expressed support for ONC efforts to

[216] 42 CFR 495.40(a)(2)(i)(H). Demonstration of meaningful use criteria. *https://www.ecfr.gov/current/title-42/chapter-IV/subchapter-G/part-495#p-495.40(a)(2)(i)(H).*

[217] 42 CFR 414.1375(b)(3). Promoting Interoperability (PI) performance category. *https://www.ecfr.gov/current/title-42/chapter-IV/subchapter-B/part-414/subpart-O/section-414.1375.*

establish the Insights Condition and encouraged ONC to minimize its administrative burdens.

Response. We appreciate the concerns expressed by commenters and aims to minimize burden on customers of developers of certified health IT related to the Insights Condition. We emphasize that developers of certified health IT are responsible for reporting the Insights Condition measures, and that health care providers, including health care providers who provide care to rural and underserved populations, are not responsible for reporting under the Insights Condition.

We have sought to design the measures so they would not require providers to separately collect data outside of their normal activities as part of delivering care or create reports to assist developers of certified health IT for the Insights Condition measures. The measures are designed to come from system-generated data and not involve additional effort by health care providers. We believe that, using widely available database technology, health IT developers should be able to collect data required for reporting under the Insights Condition without significant end-user burden. As noted in the clinical care information exchange measurement area of the preamble, we did not adopt the ''C–CDA documents obtained using certified health IT by exchange mechanism'' measure, partly because it was identified as potentially requiring mapping of data at the healthcare organization level.

We describe earlier in this section of the preamble the multiple changes to our proposals that are intended to minimize the burden on health IT developers in implementing the Insights Condition. These changes to our proposals are also intended to minimize the burden on customers of health IT developers. We believe this final rule includes several changes to our proposals that significantly reduce potential indirect burden on users (*i.e.,* health care providers) of certified health IT. As noted earlier, we provide health IT developers with an alternative reporting option if they are unable to report on all their customers due to contractual reasons.

Comments. One health system expressed support for the Insights Condition and requested clarification on how health IT developers will have access to the information in locally installed systems to complete the reporting while maintaining appropriate confidentiality.

Response. We appreciate this comment. We expect that confidentiality would already be addressed in existing contracts or business agreements between the health IT developer and their customers. Health IT developers will not submit protected health information or personally identifiable information to ONC under the Insights Condition. The data that we are requiring health IT developer to report is aggregated at the product level and is not at the health care provider or patient level.

Comments. Several commenters were supportive of the measures in general, but recommended restructuring the measures as a single set, in table format identifying the associated certification criteria, with numerator/denominator pair as its own row. Some commenters provided a sample format for our consideration.

Response. We thank commenters for their feedback. We have taken a more streamlined approach to categorizing, describing, and displaying the measures under the Insights Condition. We also refer readers to the HTI–1 Proposed Rule (88 FR 23831) for detailed background and history of the proposed measures as each measure description includes statements on the intent of the measure. For example, in the HTI–1 Proposed Rule (88 FR 23834), we specified under the ''individuals' access to electronic health information supported by certified API technology'' (now finalized as the ''individuals' access to electronic health information through certified health IT'') measure that we believe this measure would provide a national view into how individuals access their EHI and would inform ONC and health IT community efforts to empower individuals with access to their EHI.

We provide the table below to define the updated metrics that health IT developers are required to provide to ONC at the product level. The table identifies the metrics a health IT developer is required to report based on the certification criterion to which the health IT developer certifies. We reiterate that the health IT developer is responsible for providing and aggregating the data for each applicable ''metric'' at the product level. The table reflects the metrics that have been modified in some cases based on public comment and described in more detail below. We clarify that ''year 1'' refers to the first implementation year of the Insights Condition. Data collection during ''year 1'' starts in calendar year 2026 (January 1st, 2026–December 31st, 2026), with responses due in July 2027. Reporting is on an annual basis thereafter. The measures designated with ''year 2'' will begin data collection calendar year 2027, with responses due in July 2028 (and annually thereafter). The ''year 3'' measures start data collection in calendar year 2028, with responses due July 2029 (and annually thereafter). The reporting period for each of the measures below consists of one calendar year. Please refer to the measure specifications for details on the metrics, including definitions.

TABLE 2—LIST OF INSIGHTS CONDITION MEASURE METRICS

Measure title	Associated certification criteria	Metrics	Program year
Individuals' Access to Electronic Health Information Through Certified Health IT.	§ 170.315(g)(10)	1. Number of unique individuals who accessed their EHI using technology certified to ''standardized API for patient population services'' certification criterion under § 170.315(g)(10).	Year 1.
	§ 170.315(e)(1)	2. Number of unique individuals who accessed their EHI using technology certified to the ''view, download, and transmit to 3rd party'' certification criterion under § 170.315(e)(1).	Year 1.
	§ 170.315(g)(10) or § 170.315(e)(1)	3. Number of unique individuals who accessed their EHI using any method..	Year 1.
Consolidated Clinical Document Architecture (C–CDA) Problems, Medications, and Allergies Reconciliation and Incorporation Through Certified Health IT.	§ 170.315(b)(2)	4. Number of encounters	Year 2.
		5. Number of unique patients with an encounter	Year 2.
		6. Number of unique patients with an associated C–CDA document.	Year 2.

TABLE 2—LIST OF INSIGHTS CONDITION MEASURE METRICS—Continued

Measure title	Associated certification criteria	Metrics	Program year
		7. Number of total C–CDA documents obtained	Year 2.
		8. Number of unique C–CDA documents obtained	Year 2.
		9. Number of total C–CDA documents obtained that were pre-processed.	Year 2.
		10. Number of total C–CDA documents obtained that were not pre-processed.	Year 2.
		11. Number of total C–CDA documents obtained that were pre-processed where problems, medications, or allergies and intolerances were reconciled and incorporated via any method.	Year 3.
		12. Number of total C–CDA documents obtained that were not pre-processed where problems, medications, or allergies and intolerances were reconciled and incorporated via any method.	Year 3.
		13. Number of total C–CDA documents obtained that were determined to have no new problems, medications, or allergies and intolerances information by pre-processes or fully automated processes.	Year 3.
Applications Supported Through Certified Health IT.	§ 170.315(g)(10)	14. Application name(s)	Year 1.
		15. Application developer name(s)	Year 1.
		16. Intended purpose(s) of application	Year 1.
		17. Intended application user(s)	Year 1.
		18. Application status	Year 1.
Use of FHIR in Apps Through Certified Health IT.	§ 170.315(g)(10)	19. Number of distinct certified health IT deployments (across clients) active at any time during the reporting period, overall and by user type.	Year 1.
		20. Number of requests made to distinct certified health IT deployments that returned at least one FHIR resource by FHIR resource type.	Year 1.
		21. Number of distinct certified health IT deployments (across clients) associated with at least one FHIR resource returned overall and by user type.	Year 1.
		22. Number of distinct certified health IT deployments (across clients) associated with at least one FHIR resource returned by US Core Implementation Guide version.	Year 2.
Use of FHIR Bulk Data Access Through Certified Health IT.	§ 170.315(g)(10)	23. Number of distinct certified health IT deployments (across clients) that completed at least one bulk data access request.	Year 2.
	§ 170.315(g)(10)	24. Number of bulk data access requests completed (across clients) to export all data requested for patients within a specified group.	Year 2.
Immunization Administrations Electronically Submitted to Immunization Information Systems Through Certified Health IT.	§ 170.315(f)(1)	25. Number of immunizations administered overall	Year 1 (overall).
	§ 170.315(f)(1)	26. Number of immunizations administered overall, by IIS and by age category.	Year 2 (by IIS and age category).
	§ 170.315(f)(1)	27. Number of immunizations administered electronically submitted successfully to IISs overall.	Year 1 (overall).
	§ 170.315(f)(1)	28. Number of immunizations administered electronically submitted successfully to IISs overall, by IIS and by age category.	Year 2 (by IIS and age category).
Immunization History and Forecasts Through Certified Health IT.	§ 170.315(f)(1)	29. Number of immunization queries sent to IISs overall	Year 2 (overall).
	§ 170.315(f)(1)	30. Number of immunization queries sent to IISs overall by IIS	Year 3 (by IIS).
	§ 170.315(f)(1)	31. Number of query responses received successfully from IISs overall.	Year 2 (overall).
	§ 170.315(f)(1)	32. Number of query responses received successfully from IISs overall by IIS.	Year 3 (by IIS).

Comments. One commenter noted that ONC only proposed Insights Condition measures for the interoperability category. The commenter further noted that the Cures Act included other categories, including usability and user-centered design, security, conformance to certification testing, and other categories, as appropriate to measure the performance of EHR technology. The commenter encouraged ONC to focus on these

additional areas for future measure development for the Insights Condition.

Response. We thank the commenter for their encouragement to consider other areas for future measure development. As described in our HTI–1 Proposed Rule (88 FR 23832), we intend for this first set of measures to provide insights on the interoperability category specified in the Cures Act. We intend to explore the other Cures Act categories (security, usability and user-centered design, conformance to certification testing, and other categories to measure the performance of EHR technology) in future rulemaking.

Comments. One commenter stated that Conditions and Maintenance of Certification requirements including the Insights Condition should actively seek to identify bias and prevent use of algorithms that may cause discrimination against patients.

Response. We appreciate this suggestion and will consider ways that the Conditions and Maintenance of Certification requirements can help reduce bias and prevent harmful use of algorithms in patient care. We note that this final rule includes requirements that aim to introduce information transparency about Predictive DSIs supplied by health IT developers as part of their certified Health IT Modules, so that potential users have sufficient information about how a Predictive DSI was designed, developed, trained, and evaluated to determine whether it is trustworthy, including evaluation of fairness or bias. We refer readers to section III.C.5 (Decision Support Interventions and Predictive Models) of this final rule.

Comments. One commenter questioned whether ONC could get the information about some Insights Condition measures from existing sources.

Response. We appreciate this comment. As described in our HTI–1 Proposed Rule (88 FR 23831), our approach for identifying measures for the Insights Condition included several considerations, including measures reflecting information that ONC cannot obtain without regulation and efforts that are not duplicative of other data collection. We will continue to consider ways to reuse other data and reduce reporting burden while addressing information gaps in the health IT marketplace through the Insights Condition. Thus, the measures we finalized address an important gap in information that can help assess interoperability.

Cross-Cutting Requirements

In the HTI–1 Proposed Rule (88 FR 23832), we also proposed to apply certain requirements across multiple measures, including, but not limited to: (1) data submitted by health IT developers would be provided and aggregated at the product level (across versions); (2) health IT developers would provide documentation related to the data sources and methodology used to generate these measures; and (3) health IT developers may also submit descriptive or qualitative information to provide context as applicable.

We explained in the HTI–1 Proposed Rule (88 FR 23832) that overall, the documentation should help ensure the responses/data are interpreted correctly. Thus, the documentation related to the data sources and methodology would include the types of data sources used, how the measure was operationalized (*e.g.,* any specific definitions), any assumptions about the data collected, information on the providers or products that are included/excluded from the reported data, and a description about how the data was collected. As described earlier in the preamble, we would then use the measure data submitted by health IT developers to calculate the metrics (*e.g.,* percentages and other related statistics). Developers of certified health IT would submit this information to an independent entity, per statutory requirements in section 3009A(c) of the PHSA, as part of the implementation of the Insights Condition, which we discuss later in this section of the preamble.

Comments. Several commenters supported our proposal under the Insights Condition to require developers of certified health IT to report documentation used to generate each measure. Three commenters also supported the proposal for reporting optional documentation. One commenter favored requiring health IT developers to explicitly outline how they collect, aggregate, and analyze the data for the Insights Condition, including documentation on the assumptions made about the data and decisions made about the inclusion or exclusion of specific data and/or installations. Some commenters suggested that ONC establish consistent topics and categories for the required documentation submissions and requested having the option to keep the additional information submissions confidential. One commenter recommended that ONC prohibit developers from using trade secrets to prevent validation of reporting data. One commenter requested ONC define a clear and accessible pathway for public access to the Insights Condition data, as well as how identified issues will be mitigated by developers certified health IT. Further, the commenter noted that methodological transparency is essential to inform customers, regulators, and policymakers about what the Insights Condition was testing, how testing was performed, and what the reporting informs about achievement of interoperability objectives.

Response. We appreciate the feedback from commenters. We have finalized that developers of certified health IT are required under the Insights Condition to provide documentation related to the data sources and methodology used to generate these measures, and health IT developers may also submit descriptive or qualitative information to provide context as applicable. Later in this preamble, we also note that in accordance with the Cures Act, we intend to make responses (the metrics and required documentation) to the Insights Condition publicly available on our website. The metrics and required documentation will provide methodological transparency and enable assessing progress related to interoperability as requested by commenters.

We require that health IT developers, as part of their responses, will provide documentation used to generate the measures for more accurate and complete data calculation. As we stated in the HTI–1 Proposed Rule (88 FR 23832), the documentation should help ensure the data are interpreted correctly. Therefore, the documentation related to the data sources and methodology should include the types of data sources used, how the measure was operationalized (*e.g.,* any specific definitions), any assumptions about the data collected, information on the health care providers or products that are included/excluded from the metrics, and a description about how the data was collected. We intend to make the required documentation provided by health IT developers publicly available for the purposes of transparency and to allow interested parties to understand and interpret the data.

We do not anticipate that health IT developers will need to share any information they consider proprietary, trade secret, or confidential information for the required documentation related to the Insights Condition. The documentation identified above does not specifically require the disclosure of proprietary, trade secret, or confidential information. Health IT developers should be able to report without the

sharing of any such information. If health IT developers wish to provide additional information as part of the optional documentation, we strongly encourage them to not include any proprietary, trade secret, or confidential information in their submission. Further, we intend to provide a method for health IT developers to first indicate whether they plan to share proprietary, trade secret, and/or confidential information for purposes of either required or optional documentation. If a health IT developer provides an affirmative indication, ONC will engage the developer in dialogue about potential alternative means of meeting either required documentation requirements or providing optional documentation (*e.g.,* in other generalized or descriptive ways that may achieve the same goal). As we noted in the Enhanced Oversight and Accountability (EOA) Final Rule (81 FR 72429), we will implement appropriate safeguards to ensure, to the extent permissible under federal law, that any proprietary business information or trade secrets that are disclosed by the health IT developer in its documentation would be kept confidential by ONC.[218]

We also refer readers to section III.F.4 of this final rule where we describe how we intend for health IT developers to submit the metrics and related documentation electronically using a web-based form, which will provide templates that enable submitting the data to ONC in a structured, electronic format such as comma-separated values (CSV) or JavaScript Object Notation (JSON) for this purpose. For questions and comments that may arise in reviewing the results and supporting documentation, we encourage the public to follow the Certified Health IT Complaint Process described at: *https://www.healthit.gov/topic/certified-health-it-complaint-process.*

Comments. The majority of commenters opposed our proposal that developers of certified health IT report measures aggregated at the product level, across product versions. Several commenters recommended that ONC adopt a flexible approach where health IT developers can report either at the product or developer level with an attestation to indicate which level the health IT developer reported. Commenters noted that this level of flexibility is consistent with the Real World Testing Condition.

Some commenters stated that health IT developers with integrated products or platforms are not able to differentiate certain Insights Condition measures per product as proposed, making product level reporting impossible. In this circumstance, one action would be counted under multiple products. One commenter recommended reporting be permitted at the integrated database level instead of the product level to make reporting feasible. One commenter recommended reporting at the developer level to avoid duplicate counting. One commenter stated health IT developers with both cloud and non-cloud-based products would have problems aggregating data for reporting. Several commenters opposed any reporting at a level lower than a certified Health IT Module.

Three commenters requested reporting that is more granular, at the product version level. Commenters stated product version level reporting would better support health care provider and healthcare organization evaluation and comparison of health IT capabilities.

Response. We thank commenters for their feedback and acknowledge the variety of perspectives on this requirement. We have maintained and finalized in § 170.407(a)(1)(i)(A) that data submitted by health IT developers would need to be provided and aggregated at the product level (across versions). However, we recognize that integrated products, which serve multiple settings or support multiple CHPL ID products, will not be able to differentiate between the settings or CHPL IDs when reporting on the measures. This could result in either double-counting or only reporting for one product. To address this issue, we have revised our requirement, related to integrated products, so that integrated products will only have to report one response for two or more products that are integrated. The web-based form and templates will allow for health IT developers to identify as submitting on behalf of an integrated product and to provide the associated CHPL IDs with the response.

We believe that product level data would provide insights on how performance on the measures vary by market (*e.g.,* inpatient, outpatients, specialty) and by capabilities of products, whereas this type of insight would not be available at the developer level. A product level focus is also aligned with other Program reporting requirements that allow for product level reporting, such as the Real World Testing Condition and Maintenance of Certification (85 FR 25765).

In considering alternatives, such as proposing to require health IT developers to report measures at the health IT developer level or at the most granular level of product version/CHPL ID, we concluded that proposing to require data to be reported at the health IT developer level is unlikely to reduce burden given that data would still need to be obtained from each applicable product and then aggregated. We also concluded that proposing to require reporting at the product version/CHPL ID level could significantly increase burden because developers of certified health IT would need separate reports for each version of their products. A flexible approach with a mix of data at the developer and product levels does not allow for a consistent analysis and reporting across health IT developers.

Minimum Reporting Qualifications

As required by section 3009A(a)(3)(C) of the PHSA, ONC worked with an independent entity, the Urban Institute, to develop measure concepts for the Insights Condition that would not unduly disadvantage small and startup developers. For detailed background, we refer readers to the HTI–1 Proposed Rule (88 FR 23843). Additionally, we proposed (88 FR 23844) to implement the Insights Condition requirements in a way that does not unduly disadvantage small and startup developers of certified health IT. We proposed (88 FR 23844) to establish minimum reporting qualifications that a developer of certified health IT must meet to report on the measure. Developers of certified health IT who do not meet the minimum reporting qualifications (as specified under each measure), would submit a response to specify that they do not meet the minimum reporting qualifications under the Insights Condition measure. In this way, all developers of certified health IT would report on all measures, even if some report that they do not meet the minimum reporting qualifications.

In the HTI–1 Proposed Rule (88 FR 23844), we proposed that the minimum reporting qualifications include whether a health IT developer has any applicable Health IT Modules certified to criteria associated with the measure, and whether the developer has at least 50 hospital users or 500 clinician users across its certified health IT products, which serves as a proxy for its size or maturation status (*e.g.,* whether it is a startup) and refer readers to the HTI–1 Proposed Rule for details on how we determined the proposed thresholds for health IT developers (88 FR 23845).

We proposed (88 FR 23844) that if a developer of certified health IT does not

[218] The Freedom of Information Act, 18 U.S.C. 1905, and the Uniform Trade Secrets Act, 18 U.S.C. Chapter 90, generally govern the disclosure and descriptions of these types of information.

meet these minimum reporting qualifications, it would be required to submit a response that it does not meet the minimum reporting qualifications on specific measures for a given Health IT Module(s) subject to the Insights Condition requirements. In addition, we proposed (88 FR 23844) that if a health IT developer does not have at least one product that meets the applicable certification criteria specified in the measure requirements, or a developer of certified health IT that is certified to the criterion or criteria specified in the applicable measure during the reporting period but does not have any users using the functionality, the developer would still be required to submit a response that it does not meet the applicable certification criteria or the number of users required to report on the measure.

Comments. Several commenters supported our proposal to establish minimum reporting qualifications that a developer of certified health IT must meet to report on each measure. However, commenters stated that minimum reporting qualification would be more appropriate at the product level instead of at the developer level. Commenters recommended ONC maintain the proposed minimum reporting qualifications and apply those qualifications to individual products. One commenter recommended applying the thresholds at the product version level.

Response. We appreciate the interest expressed in applying the minimum reporting qualifications at the product or product version levels. However, we believe applying minimum reporting qualifications at the developer level adequately addresses the Cures Act requirement for the Insights Condition to not unduly disadvantage small and startup health IT developers. Applying minimum reporting qualifications at the product or product version levels could result in missing valuable data related to the use of certain certified health IT products.

Comments. Commenters made a few requests for clarification on the minimum reporting qualifications. One commenter indicated that our minimum reporting qualifications are ambiguous and asked ONC to clarify if the minimum reporting qualification is ''50 users in a hospital'' or ''50 hospital sites that have users.''

Response. We thank commenters for their input. We have finalized the minimum reporting qualification in § 170.407(a)(2) to be at least 50 hospital sites or 500 individual clinician users across the developer's certified health IT. We note that the 50 hospital sites threshold is applicable to health IT modules used in inpatient or emergency department settings, while the 500 individual clinician users threshold is applicable to health IT modules used in outpatient/ambulatory settings (non-inpatient).

Comments. One commenter expressed that requiring health IT developers attest to not having technology certified to a given criterion for purposes of not reporting data for a specific Insights Condition measure was redundant since ONC maintains the list of certified health IT products.

Response. The Cures Act requires that all developers of certified health IT report on all Insights Condition measures. We believe this attestation process provides for compliance with that requirement in the simplest way.

Comments. One commenter requested that the definition of ''developer'' be more specific to include the actual architects and engineers of the software itself. The commenter questioned if the current definition of ''developer'' could also be interpreted to include organizations that provide certified health IT access for practices/clinicians under MSSP agreements. Further, the commenter noted these healthcare organizations would not have resources to comply with the Insights Condition.

Response. The Conditions and Maintenance of Certification requirements in subpart D of 45 CFR part 170 apply to developers participating in the Program (see 45 CFR 170.400). Therefore, the finalized ''Insights Condition and Maintenance of Certification'' requirements (codified in § 170.407) apply to developers participating in the Program that meet minimum reporting qualifications. Although we discuss the finalized ''offer health IT'' and updated ''health IT developer of certified health IT'' definitions for purposes of the information blocking regulations (45 CFR part 171), as discussed in sections IV.B.1 and IV.B.2 of this preamble, this commenter's request is out of scope for this final rule since we did not propose a definition in the HTI–1 Proposed Rule, and there is no codified definition of ''developer'' specific to the Program regulations in 45 CFR part 170 at this time.

4. Insights Condition and Maintenance of Certification—Process for Reporting

We proposed (88 FR 23846) in § 170.407(b)(1) that, as a Maintenance of Certification requirement for the Insights Condition, developers of certified health IT would need to submit responses every six months (*i.e.,* two times per year) for any applicable certified Health IT Module(s) that have or have had an active certification at any time under the Program during the prior six months. We also proposed to provide developers of certified health IT with ample time to collect, assemble, and submit their data. We proposed (88 FR 23846) that developers of certified health IT would be able to provide their submissions within a designated 30-day window, twice a year. Developers of certified health IT would begin collecting their data twelve months prior to the first 30-day submission window. The first six months of this period would be the period that developers of certified health IT would report on for the first 30-day submission window. Developers of certified health IT would then have the next six months to assemble this data for reporting. During the second six months of this period, developers of certified health IT would begin collecting data for the next 30-day submission window and so on. We refer readers to the example we provided in the HTI–1 Proposed Rule (88 FR 23846).

We proposed (88 FR 23847) in § 170.407(b)(1)(i) that a developer of certified health IT must provide responses beginning April 2025 for the following measures: (1) individuals' access to electronic health information; (2) applications supported through certified health IT; (3) immunization administrations electronically submitted to an immunization information system through certified health IT; and (4) immunization history and forecasts. We proposed (88 FR 23847) in § 170.407(b)(1)(ii) that a developer of certified health IT must provide responses beginning April 2026 for the remaining measures: (1) C–CDA documents obtained using certified health IT by exchange mechanism; (2) C–CDA medications, allergies, and problems reconciliation and incorporation using certified health IT; (3) use of FHIR in apps supported by certified API technology; (4) use of FHIR bulk data access through certified health IT; and (5) electronic health information export through certified health IT. For further discussion regarding our rationale for these proposals, we refer readers to the HTI–1 Proposed Rule (88 FR 23847).

We welcomed comments on our proposed approach, as well as the proposed frequency of reporting, other frequencies of reporting such as more or less frequent, and any additional burdens that should be considered for developers of certified health IT to meet the proposed ''Insights Condition and Maintenance of Certification'' requirements.

We also noted in the HTI–1 Proposed Rule (88 FR 23847) that there may be other factors that could impact a developer of certified health IT's ability to easily collect data to comply with the Insights Condition's requirements. For example, a developer of certified health IT may have contracts or business agreements that inhibit the health IT developer's ability to collect data from its customers. We noted that in such scenarios, developers of certified health IT would need to renegotiate their contracts if we finalized our proposals. We explained that we expected developers of certified health IT would work to mitigate any issues and provisions affecting their ability to comply with this Condition and Maintenance of Certification requirement. Therefore, a developer of certified health IT that is required to meet the Insights Condition's requirements must submit responses or may be subject to ONC direct review of the Conditions and Maintenance of Certification requirements, corrective action, and enforcement procedures under the Program. We welcomed comments on our approach, as well as any specific hardships certified health IT may encounter with the Insights Condition of Certification.

We proposed (88 FR 23847) that responses to the Insights Condition would occur via web-based form and method, consistent with the requirements in § 3009A(c) of the PHSA. We noted that under the statute, developers of certified health IT must report to an ''independent entit[y]'' to ''collect the information required to be reported in accordance with the criteria established.'' We intend to award a grant, contract, or other agreement to an independent entity as part of the implementation of the Insights Condition and will provide additional details through subsequent information. We stated that we intend to make responses publicly available via an ONC website, and we intend to provide developers of certified health IT the opportunity to submit qualitative notes that would enable them to explain findings and provide additional context and feedback regarding their submissions.

Further, we proposed (88 FR 23847) a new Principle of Proper Conduct for ONC-Authorized Certification Bodies (ONC–ACBs) in § 170.523(u) that would require ONC–ACBs to confirm that applicable developers of certified health IT have submitted their responses for the Insights Condition of Certification requirements in accordance with our proposals. We stated an expectation that the ONC–ACBs would confirm whether or not the applicable health IT developers submitted responses for the Insights Condition of Certification requirements within the compliance schedule. The intent of this responsibility is not to duplicate the work of the independent entity in collecting and reviewing the response submissions. Rather, it is meant to support the ONC–ACBs' other responsibility in § 170.550(l) to ensure that developers of certified health IT are meeting their responsibilities under the Conditions and Maintenance of Certification requirements before issuing a certification.

Comments. Many commenters, including developers of certified health IT, opposed our expectation related to § 170.407(b)(1) in the HTI–1 Proposed Rule (88 FR 23847) that health IT developers would need to renegotiate their contracts or business agreements that inhibit their ability to collect data from their customers in order to comply with this requirement. Commenters stated that this expectation to renegotiate contracts or business agreements was unreasonable, not feasible, or overly burdensome.

Two commenters questioned the authority of ONC to require developers of certified health IT to renegotiate contracts or business agreements in order to gain access to customer data for the Insights Condition. Two developers of certified health IT commented that they experienced challenges in soliciting participation from customers in data collection for the Real World Testing Condition despite their efforts. One commenter noted that it is not feasible to require a renegotiation of client contracts specific to only one term without reopening renegotiation of all contract terms. One commenter stated the amount of time that finding, assessing, negotiating, and re-finalizing a contract is unreasonable in the proposed timeframe.

Several developers of certified health IT commented that ONC should require a good faith effort by developers to engage their customers to participate. Also, commenters suggested ONC include language in the Insights Condition that allows for exclusions or other flexibilities from reporting where health IT developers have been unable to obtain data for measures despite good faith efforts.

Several developers of certified health IT further commented that establishing a minimum threshold of customers is not a viable way to address their concerns. One developer of certified health IT commented that ONC should set the expectation that health IT developers request participation in data collection under the Insights Condition from all of their U.S.-based customers of certified health IT and report all of the data from participants who agree, as well as what percentage of their total customers this represents. One commenter sought clarification from ONC on whether there is an expectation that developers of certified health IT obtain numerator and denominator data from every U.S. customer using a product or only those customers agreeing to participate.

One commenter noted that time and cost estimates were not included in the Regulatory Impact Analysis for effort necessary from developers of certified health IT, or health systems, for contract renegotiation expectations related to § 170.407(b)(1). The commenter further noted that effort from both health IT developers and health systems would be necessary for each renegotiated contract.

Response. We appreciate the commenters' concerns regarding the feasibility of requiring developers of certified health IT to renegotiate contracts, when needed, with their customers to comply with the Insights Condition requirements. In response to public comment, we have removed this proposed requirement. In a scenario where a developer of certified health IT has contracts or business agreements with a customer that inhibit the health IT developer's ability to comply with the Insights Condition requirements, the health IT developer may exclude that customer's data for reporting under the Insights Condition.

In § 170.407(b)(1) in the HTI–1 Proposed Rule (88 FR 23847) we proposed that health IT developers provide us metrics based upon data from all their customers. In response to health IT developers expressing concerns regarding the difficulty in obtaining data from clients whose contracts would require updating to access the needed data, we have scaled back our requirement for health IT developers to provide complete data on all clients. In addition to the data on available clients that they report, health IT developers will provide ONC with information on the degree to which the data they are submitting is complete. We emphasize that the Insights Condition fulfills the Cures Act specified requirements in section 4002(c) to establish an Electronic Health Record (EHR) Reporting Program to provide transparent reporting on certified health IT with respect to all certified technology offered by a health IT developer, and therefore, health IT developers should be as inclusive as possible.

Based upon the suggestion we received via comments, we have finalized in § 170.407(a)(1)(i)(C) that health IT developers will report the percentage of their total customers, as represented by hospitals for inpatient products and clinician users for their outpatient products, that are included in their reported data for each metric for which they submit a response. The percentage of health care providers that are represented in the data provides transparency on the degree to which the data are complete. Specifically, we seek to determine whether the aggregated data that we receive from all health IT developers will produce nationally representative measures will be critical to generate and report the derived statistics and explain the results. For example, if the percentage of total customers represented is low across many health IT developers, then we would know that the data are incomplete. This in turn, would enable ONC to consider whether it would be valid to generate statistics at the national level. Overall, this information shall help ONC interpret the results and allow us to assess the degree to which the data are complete.

Comments. Many commenters opposed our proposal in § 170.407(b)(1)(i) for the first Insights Condition reporting period to begin in April 2024. Some commenters stated the timeline was unrealistic, not feasible, or impossible given timeframes to develop, deploy, test, and build the capability to compile the data. Commenters offered various alternative timelines for the first Insights Condition reporting period to begin. Several commenters requested delaying the first reporting period to begin in calendar year 2025, such as in January, April, or October of 2025. Several commenters requested delaying the first reporting period to begin in calendar year 2026. Some commenters requested delaying the first reporting period to begin 18 months after the final rule publication. One commenter requested ONC reconsider implementation over a four- or five-year timeframe. One commenter suggested longer timelines to ensure measures are validated before phasing in new measures.

Response. We thank commenters for the feedback and have revised the Insights Condition timelines. We have finalized in § 170.407(b)(1)(i) to delay the first reporting period to allow developers of certified health IT adequate time to develop and implement the Insights Condition measures and related metrics. We have finalized that the first data collection period will be January to December 2026, followed by the submission of the first phase of measures and related metrics due in July of 2027. This represents ''year one'' of the Insights Condition requirements. Reporting is on an annual basis thereafter. We have further extended our phased approach to measure requirements, including layering complexity associated with certain measures over the course of three years, so that certain measures (and related metrics) start in year one, while other measures or stratifications to existing measures begin in subsequent years. We have finalized ''year 2'' measures and related metrics start data collection in calendar year 2027, with responses due in July 2028, and annually thereafter. Finally, we have finalized ''year 3'' measures and related metrics start data collection in calendar year 2028, with responses due in July 2029 and annually thereafter. The phasing of the measures and related metrics are illustrated in the table in this section of the preamble.

We also appreciate the commenter's concern for needing additional time to assess measure validity. Our revised approach of phasing in more complex aspects of each of the measures enables reviewing baseline measures before adding complexity. Furthermore, our revised approach provides additional time for measure development and implementation and will allow us to apply lessons learned from the smaller set of measures to inform the implementation of next set.

Comments. Most commenters opposed our proposal in § 170.407(b)(1) to require the frequency of semiannual (*i.e.,* every six months) data collection and reporting under the Insights Condition. Most commenters suggested an annual frequency of data collection and reporting to reduce burden. Many of these commenters suggested using a calendar-year reporting period with reporting to occur mid-year to better align with the CMS Promoting Interoperability Programs and the Real World Testing Condition, and to avoid other April/October requirements for Attestations submissions. One health system commenter suggested an annual reporting period that does not overlap with clinical quality measure reporting schedules. One commenter stated that semiannual reporting would require two product upgrades within a one-year timeframe and that their customers would not be willing to comply. Three commenters supported our proposal to require semiannual (*i.e.,* every six months) data collection and reporting in April and October. One health IT developer commented the proposed six-month intervals are feasible with current technology and not overly burdensome to health IT developers. Commenters supported our proposal in § 170.407(b)(1) for six months to assemble and assess data collected prior to reporting under the Insights Condition.

Response. We appreciate the feedback on reporting frequency and the concerns expressed related to burden. To address these concerns, we have finalized to reduce the reporting frequency to annually (once per year) in § 170.407(b), on a calendar year cycle, with data collection to be completed from January to December. We have maintained the six-month data assembly period, such that reports for a given calendar year will be due to be submitted in July of the following calendar year.

Comments. Many commenters requested clarification on whether developers of certified health IT have the flexibility to reuse the Insights Condition reporting measurements and outputs for their Real World Testing plans and results.

Response. We appreciate the commenters request for clarity. We appreciate that the data collected related to the Insights Condition and Real World Testing could overlap. Therefore, developers of certified health IT can choose to repurpose the Insights Condition reporting measurements and/or data as part of their Real World Testing plans and results.

Comments. One health IT developer suggested that ONC apply its experience with Real World Testing to reduce measure ambiguity and provide Real World Testing reports as examples for health IT developers to use in planning for the Insights Condition.

Response. We agree with the commenter that the Real World Testing Condition provides relevant experience for health IT developers. We considered Real World Testing Condition reports in developing our proposals for the Insights Condition and intend to provide examples. We plan to leverage a system linked to the CHPL for reporting to make the process similar to other certification related processes. We will use web-based forms within that system for submission and plan to provide templates for health IT developers to use in their data submission for the Insights Condition. The templates will enable health IT developers to submit the data (as noted in the 88 FR 23847) in a machine-readable format, such as JavaScript Object Notation (JSON). We also intend to provide educational sessions and resources for health IT developers to support electronic reporting of the metrics and related documentation.

Comments. Some commenters recommended that ONC expand its governance structure to include patients and other clinicians in reviewing Insights Condition and Real World Testing results to identify new opportunities for action.

Response. We thank the commenters for the input. As described in our HTI–1 Proposed Rule, ONC, and our contractor, conducted various engagement efforts with a variety of groups having potential interests in the Insights Condition. This engagement process [219] included a request for information by ONC, public forums, listening sessions, and discussions with experts and key groups, including health IT end users (*e.g.,* clinicians) and health IT developers. In addition to this engagement and public comments, the Health IT Advisory Committee (HITAC), which includes patient advocates and clinicians, provided recommendations [220] to ONC that informed the Insights Condition. We will continue to look for opportunities to obtain input from a variety of perspectives, including patients and clinicians, on the Insights Condition.

Comments. One health care provider organization recommended that ONC make the Insights Condition metrics easily accessible to users of certified health IT and to the public. One health IT developer sought clarification from ONC if we intend to calculate and display percentages using the reported numerators and denominators across the universe of certified health IT that reported for a given measure, or if we intend to calculate and display metrics at the developer or product level. Another commenter encouraged ONC and developers of certified health IT under the Insights Condition to evaluate measure reliability and validity of the reported data before publicly reporting.

Response. We thank the commenter for the opportunity to clarify how ONC will calculate and display the Insights Condition metrics. In accordance with the Cures Act, we intend to make responses (the metrics and required documentation) to the Insights Condition publicly available on an ONC website. Prior to publicly releasing the data or publishing metrics, we will review and analyze the data to assess completeness and generalizability, which relate to the reliability and validity of the data. After this analysis, we will determine what level(s) the calculated metrics would be displayed, such as at the product, developer and/or national level. The aggregated data that is reported needs to have an adequate number of data points at any given level to make sure the metrics displayed are valid and reliable.

Comments. One commenter recommended that ONC create a public list of the certification status of health IT developers.

Response. We thank the commenter for this input, and note that ONC maintains the Certified Health IT Products List (CHPL) at *https://chpl.healthit.gov/,* which is a comprehensive and authoritative listing of all certified health information technology that have been successfully tested and certified by the Program and includes current certification statuses.

Comments. One commenter suggested requiring health IT developers to report on whether the certified health IT is hosted by the health IT developer or installed locally under the direct control of the user. Further, the commenter noted that this information may provide insight into usage patterns and adoption of cloud services and other technology that can inform HHS regulations.

Response. We thank the commenter for this suggestion, and we agree that this data element could be useful and informative in assessing the state of the certified health IT marketplace. We may consider this for future rulemaking.

Comments. A commenter stated that ONC–ACBs will need more detailed information on the degree of surveillance and validation that ONC–ACBs will need to provide in support of the Insights Condition reporting process in order to plan appropriately.

Response. Similar to other Conditions and Maintenance of Certification requirements, we will provide additional guidance to ONC–ACBs regarding their role and requirements related to oversight of the Insights Condition as the workflow and reporting systems for the Insights Condition are developed and finalized.

G. Requests for Information

1. Laboratory Data Interoperability Request for Information

We sought public feedback in the HTI–1 Proposed Rule (88 FR 23848) that may be used to inform a study and report required by Division FF, Title II, Subtitle B, Ch. 2, Section 2213(b) of the Consolidated Appropriations Act, 2023 (Pub. L. 117–328, Dec. 29, 2022), or future rulemaking regarding the adoption of standards and certification criteria to advance laboratory data interoperability and exchange.

We sought public comment generally on any topics identified in the Consolidated Appropriations Act, 2023, Section 2213(b) study on the use of standards for electronic ordering and reporting of laboratory test results, such as the use of health IT standards by clinical laboratories, use of such standards by laboratories and their effect on the interoperability of laboratory data with public health systems, including any challenges of the types identified above. We also sought comment on whether ONC should adopt additional standards and laboratory-related certification criteria as part of the Program. We received many valuable comments on this RFI. We appreciate the input provided by commenters and may consider their input to inform a future rulemaking.

2. Request for Information on Pharmacy Interoperability Functionality Within the ONC Health IT Certification Program Including Real-Time Prescription Benefit Capabilities

Section 119 of Title I, Division CC of the Consolidated Appropriations Act, 2021, (Pub. L. 116–260) (CAA), requires PDP sponsors of prescription drug plans to implement one or more real-time benefit tools (RTBTs) after the Secretary has adopted a standard for RTBTs and at a time determined appropriate by the Secretary. The law specified that a qualifying RTBT must meet technical standards named by the Secretary, in consultation with ONC. Section 119(b)(3) also amended the definition of a ''qualified electronic health record'' in section 3000(13) of the PHSA to specify that a qualified electronic health record must include or be capable of including an RTBT. In the 2014 Edition Final Rule, ONC established the term ''Base EHR,'' based on the ''Qualified EHR'' definition, for use within the Program (77 FR 54262).

As stated in the HTI–1 Proposed Rule (88 FR 23848), we intend to propose in future rulemaking the establishment of a real-time prescription benefit health IT certification criterion within the Program and include this criterion in the Base EHR definition in § 170.102. We intend to propose a criterion that would certify health IT to enable a provider to view within the electronic prescribing workflow at the point of care patient-specific benefit, estimated cost information, and viable alternatives. We are also considering a proposal to adopt and reference the National Council for Prescription Drug Programs (NCPDP) Real-Time Prescription Benefit (RTPB) standard version 12 as part of the potential

[219] *https://www.urban.org/research/publication/what-comparative-information-needed-ehr-reporting-program.*

[220] *https://www.healthit.gov/sites/default/files/page/2022-07/2021-09-09_EHRRP_TF_2021__HITAC%20Recommendations_Report_signed_508_Edit.pdf.*

certification criterion.[221] This standard would enable the exchange of patient eligibility, product coverage, and benefit financials for a chosen product and pharmacy, and identify coverage restrictions and alternatives when they exist.

While we believe that implementing RTBT functionality required for inclusion in the Program under the CAA would be an important step towards improving prescribing experiences for providers and patients, we recognize that it is only one of a series of capabilities that are part of a comprehensive workflow for evaluating and prescribing medications (88 FR 23849).

Today, the Program addresses these additional capabilities in a limited manner. For instance, in the ONC Cures Act Final Rule, ONC adopted NCPDP SCRIPT standard version 2017071 and updated the ''electronic prescribing'' certification criterion in § 170.315(b)(3)(ii) to reflect this standard, including specifying electronic prior authorization transactions supported by the standard as optional transactions, which health IT developers can elect to have explicitly tested, or not, as part of certification of a product to § 170.315(b)(3) (85 FR 25680).

A ''drug-formulary and preferred drug list checks'' certification criterion had been established for the 2015 Edition in § 170.315(a)(10) but was later removed from the Program by the ONC Cures Act Final Rule (85 FR 25660). ONC removed the criterion due to the lack of associated interoperability standards and to reduce certification burden on developers as this functionality had been widely adopted across industry.

We requested comment in the HTI–1 Proposed Rule (88 FR 23849) from the public about specific issues related to establishing a certification criterion using NCPDP RTPB standard version 12 and other potential actions that could support complementary and interoperable workflows. Given the statutory definition in PHSA § 3000(13) of ''qualified electronic health record'' as an electronic record of health-related information on an individual that includes, or is capable of including, RTBT functionality, we sought to understand whether ONC should offer or require certification of other capabilities to optimize the value of real-time prescription benefit capabilities to clinicians and patients.

[221] For further information about implementing the NCPDP RTPB standard version 12, see resources at *https://standards.ncpdp.org/Access-to-Standards.aspx.*

We requested input on how developers of certified health IT may be able to support drug price transparency, patient choice, and meet other market demands while ensuring reliable and trusted performance. We received many insightful comments on this RFI. We appreciate the input provided by commenters and may consider their input to inform a future rulemaking.

3. FHIR Standard

This request for information included in the HTI–1 Proposed Rule (88 FR 23855) focused on the FHIR standard for APIs (including FHIR Subscriptions, CDS Hooks, FHIR standards for scheduling, and SMART Health Links) and aligned with our aims of advancing interoperability through the use of APIs for treatment, payment and operations use cases. We welcomed technical and policy comments as we consider the potential applicability of these standards and specifications. We received many insightful comments on this RFI. We appreciate the input provided by commenters and may consider their input to inform a future rulemaking.

IV. Information Blocking Enhancements

In the HTI–1 Proposed Rule (88 FR 23746), we proposed enhancements to support information sharing under the information blocking regulations and to promote innovation and competition, as well as address market consolidation (*see* Executive Summary discussion at 88 FR 23749 and 88 FR 23754 through 23755; *see also* preamble discussion in section IV of the HTI–1 Proposed Rule at 88 FR 23857 through 23873). We proposed new and revised definitions of terms for purposes of the information blocking regulations in 45 CFR part 171. The revisions to definitions included, as discussed in section IV.B.3, the removal of references to a period of time now passed in the information blocking definition (§ 171.103). We proposed (as discussed in IV.B.3 of this preamble) to remove reference to the period of time, now passed, from the exception in 45 CFR 171.301. We proposed, consequently, to rename the ''Content and Manner Exception'' to simply the ''Manner Exception.'' Each of these proposals is discussed, and public comments received on each proposal summarized, in section IV.B of this preamble.

We proposed enhancements to certain information blocking exceptions that had been established by the ONC Cures Act Final Rule (85 FR 25642). We proposed to clarify the *uncontrollable events* condition of the Infeasibility Exception (§ 171.204) to make it clear that an uncontrollable event must in fact have affected the actor's ability to fulfill requests for access, exchange, or use of EHI (for a more detailed summary, please see section IV.C.1.a of this preamble). We also proposed to create new conditions for (options through which to satisfy) the Infeasibility Exception when an actor has exhausted the § 171.301 Manner Exception and, separately, when a third party requests to modify EHI held by the actor. These conditions are discussed in sections IV.C.1.b and IV.C.1.c of this preamble. As discussed in section IV.C.2 of this preamble, we proposed to add a *TEFCA manner* condition to the proposed revised and renamed Manner Exception codified in 45 CFR 171.301 (*see* 88 FR 23872 through 23873).

The HTI–1 Proposed Rule included (at 88 FR 23873 through 88 FR 23876) three information blocking requests for information (RFIs). The first of these RFIs sought information on potential additional exclusions from the definition of ''offer health IT.'' The second sought information on possible additional TEFCA reasonable and necessary activities. The third sought information on health IT capabilities for data segmentation and user or patient access. We discuss these requests for information below, in section IV.D.1 through IV.D.3 of this preamble.

A. General Comments

Comments. In general, commenters expressed support for the proposed enhancements and for updating the regulations over time to improve clarity or reduce burdens for actors while continuing to encourage interoperable access, exchange, and use of EHI to the full extent permitted by applicable law and consistent with individual patients' privacy preferences. Some commenters made suggestions, recommendations, or requests for additional guidance, information and educational resources, or for other tools to help actors appropriately share information and avoid conduct that would be considered ''information blocking'' (as defined in 45 CFR 171.103).

Response. We appreciate the support expressed by many commenters. We include below additional explanation of provisions of this final rule. Requests, recommendations, or suggestions that we provide additional guidance, resources, or tools relevant to information blocking are appreciated. As part of our ongoing outreach and education efforts, all feedback and information we receive helps to inform our consideration and development of resources such as webinar

presentations, fact sheets, and frequently asked questions (FAQs).

Comments. Several comments advocated for specific changes to the information blocking regulations, to other HHS regulations, or to state law. For example, a commenter advocated ''aligning HIPAA rules, 42 CFR part 2 requirements, and other state and federal laws with information blocking regulations.'' Another commenter stated that ''ONC needs to clarify the national requirements for production of complete medical records, especially absolute transparency on corrections, deletions, delayed entries, and original content, upon ordinary request.'' A commenter indicated health IT users may mis-apply the designated record set (DRS) definition to electronic records and stated that ONC ''needs to consider discouraging inappropriate DRS definition-based information blocking of complete medical records through significant, powerful disincentives.'' One commenter advocated for ONC to narrow the *health information network* definition ''and clearly state in the regulatory text payers are not included in this definition and thus are not subject to the information blocking provision.'' Another commenter expressed a view that specifying in the information blocking definition's regulatory text the persons whose records access can be affected by a practice would make the rule stronger.

Response. Comments related to the following are outside of the scope of the information blocking provisions of this rulemaking: establishment of health care provider disincentives for information blocking conduct; changes to HHS regulations outside 45 CFR part 171; adoption of requirements for creation or retention of specific metadata by all health care providers nationwide; and any change to any state or tribal law. However, comments recommending policy changes outside the scope of this rule are part of the rulemaking record, and we may refer to them as an information source when assessing potential future rulemaking or outreach and education activities.

Comments. A substantial number of comments expressed concerns about a perceived conflict between the goals of maximizing information sharing and appropriately protecting patients' privacy interests. These comments generally associated these concerns with specific policy recommendations, including the creation of new information blocking exception(s). Some commenters suggested that some § 171.102 actors may believe they have no option under information blocking regulations but to enable the access, exchange, or use of all EHI in all situations—including those where only some of the EHI can be used or disclosed consistent with privacy laws or the patient's individual privacy preferences. A few of these commenters specifically noted sensitive information or information associated with sensitive types of care, such as reproductive or behavioral health care.

Response. Some of the policy recommendations that commenters offered to address these concerns, such as to establish new exceptions or implement revisions beyond anything described in the HTI–1 Proposed Rule, were outside the scope of this rulemaking. Some provisions advocated by commenters appear to duplicate provisions already in place, such as provisions of the Privacy Exception (§ 171.202) and the Infeasibility Exception (§ 171.204). The expressed concerns and advocacy of duplicative policy provisions suggest it may be helpful to highlight here certain aspects of how the information blocking regulations currently operate.

Where applicable law prohibits a specific access, exchange, or use of information, the information blocking regulations consider the practice of complying with such laws to be ''required by law.'' Practices that are ''required by law'' are not considered ''information blocking'' (*see* the statutory information blocking definition in section 3022(a)(1) of the PHSA and the discussion in the ONC Cures Act Final Rule at 85 FR 25794). For example, when the HIPAA Privacy Rule prohibits a covered entity or business associate from disclosing PHI, an actor who is also a covered entity or business associate *can* comply fully with the HIPAA Privacy Rule without implicating the information blocking regulations. For another example, a § 171.102 actor subject to a state or tribal law that expressly prohibits a certain access, exchange, or use of EHI *can* comply fully with that state or tribal law without implicating the information blocking regulations.

We recognize that even where federal, state, or tribal law does not expressly prohibit the actor from fulfilling a request to access, exchange, or use EHI, or require an actor to engage in particular privacy-protective practices, an actor may nevertheless wish to engage in practices likely to interfere with access, exchange, or use in order to honor their patients' privacy preferences. Actors covered by the information blocking regulations—health IT developers of certified health IT, health information networks or health information exchanges (HIN/HIEs), and health care providers—may seek certainty that the privacy-protective practices that are not required of them by law, but in which they choose to engage, will not meet the definition of information blocking.

In the ONC Cures Act Final Rule, we established the Privacy Exception (45 CFR 171.202) to ensure that actors can engage in reasonable and necessary practices that advance the privacy interests of individuals (*see* 85 FR 25845 through 25859) without committing ''information blocking'' as defined in section 3022(a)(1) of the PHSA and 45 CFR 171.103.

For example, the information blocking regulations in 45 CFR part 171 accommodate the fact that, in various circumstances, other applicable law (federal, state, or tribal) does not permit EHI to be used or disclosed unless certain preconditions are met. The Precondition Not Satisfied (45 CFR 171.202(b)) sub-exception of the Privacy Exception outlines a framework for actors to follow to be assured their practices of not fulfilling requests to access, exchange, or use EHI will not constitute information blocking when a precondition of applicable state, tribal, or federal law has not been satisfied.

In addition, for purposes of the Precondition Not Satisfied sub-exception, an actor operating under multiple state laws, or state and tribal laws, with inconsistent preconditions for EHI disclosures may choose to adopt uniform policies and procedures to address the more restrictive preconditions (45 CFR 171.202(b)(3)).

Examples that highlight the alignment between the HIPAA Privacy Rule and the information blocking regulations are included in the ''HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care'' guidance issued by the Office for Civil Rights. As outlined in this guidance, there are certain preconditions that must be met before disclosures about reproductive health care can be made by health care provider workforce members, including to law enforcement officials. For instance, if a law enforcement official requests records of abortions from a reproductive health care clinic: ''If the request is not accompanied by a court order or other mandate enforceable in a court of law, the Privacy Rule would not permit the clinic to disclose PHI in response to the request. Therefore, such a disclosure would be impermissible and constitute a breach of unsecured PHI requiring notification to HHS and the individual affected.'' In this example, federal law does not permit the disclosure of EHI unless certain requirements are met, and therefore, the

actor's practice not to disclose EHI would not be information blocking. We note that this is just one example of how the HIPAA Privacy Rule gives individuals confidence that their protected health information, including information relating to abortion and other sexual and reproductive health care, will be kept private. Please see the guidance from the Office for Civil Rights for additional information and examples.[222]

We also note that information blocking regulations in 45 CFR part 171 accommodate an actor, if they so choose, agreeing to an individual's request for restrictions on sharing of the individual's EHI beyond the restrictions imposed by applicable law(s). Specifically, where the requirements specified in 45 CFR 171.202(e) are met, the Respecting an Individual's Request Not to Share Information (§ 171.202(e)) sub-exception of the Privacy Exception applies to an actor's practice of honoring an individual's request not to provide access, exchange, or use of the individual's EHI. This aligns with the individual's right to request a restriction on certain uses and disclosures of their PHI under the HIPAA Privacy Rule (45 CFR 164.522(a)(1)), to which an actor that is a covered entity *may choose* to agree but is *not required* by the HIPAA Privacy Rule to agree.

In scenarios where a § 171.102 actor that is also subject to the HIPAA Privacy Rule must agree to the request of an individual to restrict disclosure of PHI as provided in 45 CFR 164.522(a)(1)(vi), the actor's practice of agreeing to the request and complying with all requirements of 45 CFR 164.522 applicable to such requests and restrictions is, in our view, a practice that is ''required by law.'' We reiterate that practices that are required by law are excluded from the statutory (PHSA section 3022(a)(1)) as well as the regulatory (45 CFR 171.103) definition of information blocking without needing to also satisfy any of the 45 CFR part 171 exceptions. Therefore, when a § 171.102 actor that is also a HIPAA covered entity engages in a practice of complying with all requirements of 45 CFR 164.522 that are applicable to requests to which a covered entity must agree (as provided in 45 CFR 164.522(a)(1)(vi)) then that actor would not need to also satisfy the Respecting an Individual's Request Not to Share Information (45 CFR 171.202(e)) sub-exception of the Privacy Exception in order for that practice to not be considered information blocking. The practice would be excluded from the definition of information blocking because it would be ''required by law'' and, therefore, an information blocking exception for the practice would not be needed.

We refer commenters and other readers interested in learning more about the interaction of the information blocking regulations with the HIPAA Rules and other laws protecting individuals' privacy interests to the discussion of the Privacy Exception in the ONC Cures Act Final Rule (85 FR 25642, 85 FR 25845 through 25859). We also highlight the availability of additional resources through our website (start at: *https://www.healthit.gov/topic/information-blocking*). Resources focused on how the information blocking rules work in harmony with privacy laws include, for example, an ONC Health IT buzz blog post titled ''*Information Blocking Regulations Work in Concert with HIPAA Rules and Other Privacy Laws to Support Health Information Privacy*'' [223] and the following three frequently asked questions (FAQs) highlighting how information blocking regulations work in tandem with the HIPAA Privacy Rule and other privacy protective laws:

- Would it be information blocking if an actor does not fulfill a request to access, exchange, or use EHI in order to comply with federal privacy laws that require certain conditions to have been met prior to disclosure? [224]
- If an actor, such as a health care provider, operates in more than one state, is it consistent with the information blocking regulations for the health care provider to implement practices to uniformly follow the state law that is the most privacy protective (more restrictive) across all the other states in which it operates? [225]
- If an individual requests that their EHI not be disclosed, is it information blocking if an actor does not disclose the EHI based on the individual's request? [226]

The Infeasibility Exception may also be applicable to matters of patient privacy preferences. Established by the ONC Cures Act Final Rule, the Infeasibility Exception (45 CFR 171.204) applies when an actor's practice meets one of the conditions set forth in § 171.204(a) and also meets the condition in § 171.204(b) (*see* 85 FR 25958, *see also* preamble discussion at 85 FR 25866 through 25870). The *segmentation* condition of the Infeasibility Exception (§ 171.204(a)(2)) can be met in conjunction with other exceptions to provide actors assurance that their practice does not constitute information blocking. The *segmentation* condition is applicable when the actor cannot fulfill the request for access, exchange, or use of EHI because the actor cannot unambiguously segment the requested EHI from EHI that:

- cannot be made available due to the individual's preference (such as where the individual has requested that the EHI not be shared with a specific person(s), for a specific purpose(s), or both); [227]
- cannot be made available by law, for example, the HIPAA Privacy Rule, other federal law, or applicable state or tribal law does not permit the EHI to be made available to the person seeking it, for the purpose it is sought, or both; or
- may be withheld in accordance with the Preventing Harm Exception (45 CFR 171.201).

Applicable law may restrict providing certain types of EHI to a person or class of persons, for a specific purpose, or a combination of types of persons and specific purposes. For example, federal, state, or tribal law may require that certain information not be accessed, used, or exchanged by the person seeking it, for the purpose it is sought, or both. As we discuss above, an actor can, without engaging in ''information blocking,'' withhold information as required by law or withhold information by meeting the Pre-condition Not Satisfied sub-exception. Similarly, an individual (*see* definition of ''*individual*'' in § 171.202(a)) may express a preference that some or all of the EHI for a particular patient not be shared with a specific person(s), for a specific purpose(s), or a specific combination of person(s) and purpose(s). Such a preference could be expressed, for example, by the individual making a request that a HIPAA covered entity restrict uses and disclosures of their PHI that § 164.522

[222] *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html.*

[223] *https://www.healthit.gov/buzz-blog/information-blocking/information-blocking-regulations-work-in-concert-with-hipaa-rules-and-other-privacy-laws-to-support-health-information-privacy.* (Retrieved 7/12/2023.)

[224] Information blocking FAQ identifier: IB.FAQ48.1.2023APR. URL: *https://www.healthit.gov/faq/would-it-be-information-blocking-if-actor-does-not-fulfill-request-access-exchange-or-use-ehi.* (Retrieved 7/12/2023.)

[225] Information blocking FAQ identifier: IB.FAQ49.1.2023APR. URL: *https://www.healthit.gov/faq/if-actor-such-health-care-provider-operates-more-one-state-it-consistent-information-blocking.* (Retrieved 7/12/2023.)

[226] Information blocking FAQ identifier: IB.FAQ47.1.2023APR. URL: *https://www.healthit.gov/faq/if-individual-requests-their-ehi-not-be-disclosed-it-information-blocking-if-actor-does-not.* (Retrieved 7/12/2023.)

[227] We use ''individual'' here, and for purposes of § 171.204 in general, as it is defined in § 171.202(a).

requires covered entities to permit an individual to make. As we discuss above, and in accordance with the § 171.202(e) Respecting an Individual's Request Not to Share Information sub-exception, an actor may withhold information that a patient has requested the actor not share.

The example above illustrates a specific alignment between the information blocking regulations and HIPAA Privacy Rule. However, the § 171.202(e) sub-exception's alignment with the individual's right under the HIPAA Privacy Rule to request restrictions does not limit the sub-exception's availability to actors who are also subject to the HIPAA Privacy Rule's requirements. Nothing in the § 171.202(e) sub-exception limits its availability based on whether the actor is a HIPAA covered entity or business associate that must comply with the HIPAA Privacy Rule. Likewise, § 171.202(e) does not focus on whether the individual requested restrictions under any specific provision of the HIPAA Privacy Rule. Therefore, for purposes of the information blocking regulations, the § 171.202(e) Respecting an Individual's Request Not to Share Information sub-exception can be satisfied by *any* actor who chooses to meet the requirements of the sub-exception.

We recognize many actors may currently be unable to unambiguously segment reproductive health and behavioral health information indicated by some commenters on the information blocking provisions as sensitive information, as well as gender-affirming care information, from other EHI. These are also examples of types of information for which individuals may be likely to request restrictions on uses or disclosure. These are, however, not the only types of information to which the Infeasibility Exception's *segmentation* condition might apply. As we noted in the HTI–1 Proposed Rule, a health care provider might choose to honor a patient's request for restrictions on sharing of their EHI even if the provider did not *know* the patient's specific reasons for the request. The Respecting An Individual's Request Not To Share Information sub-exception (§ 171.202(e)) does not specify that the individual requesting restrictions should have particular reasons for requesting restrictions, or be required to share their reasoning with the health care provider or other actor of whom they make the request (88 FR 23874).

Where an actor engaging in a practice that is not (or practices that are not) fully covered by a single exception seeks certainty that such practices do not constitute information blocking, the actor could choose to satisfy several applicable exceptions that, in complement, do fully cover their practices. Applicable exceptions, and combinations of exceptions, will vary based on the actor's specific practice and particular facts and circumstances in which they engage and the practices for which the actor seeks the certainty offered by information blocking exceptions.[228]

In various circumstances, an actor may wish to engage in one or more practice(s) that are covered in part, but not fully covered, by the Privacy Exception (§ 171.202) or the Preventing Harm Exception (§ 171.201). In some of these situations, such an actor may want to consider the potential certainty that could be available by satisfying a combination of the Infeasibility Exception (§ 171.204) with the Privacy Exception (§ 171.202) or with the Preventing Harm Exception (§ 171.201), or any combination of multiple exceptions applicable to the specific practice in which the actor engages. We provide the following example to illustrate how the use of a combination of exceptions might occur. We note that we have intentionally omitted from this example any consideration of why the individual may request, or why the actor may have chosen to agree to the individual's request. This is because the § 171.202(e) sub-exception's application is not limited based on what particular reasons an individual may have for requesting restrictions of any or all of their EHI, and does not specify that an actor must have specific reasons for choosing to grant rather than deny an individual's request for restrictions. However, as noted above, these exceptions could be exercised, separately or together, when an individual requests certain information (*e.g.,* reproductive health, behavioral health, or gender-affirming care information) not be shared or when such information cannot be unambiguously segmented from other EHI from the reasons noted above.

An individual makes a request of an actor not to share certain EHI. The actor agrees to the request, documents the request, implements the request, and does not otherwise terminate the request. After the actor agrees to the individual's request not to share information, the actor receives a request for the individual's EHI that encompasses information the individual requested that the actor not share. The actor determines that responding to the request is not prohibited by applicable law. The actor then determines that the actor has the technical ability to segment out some, but not all, of the requested EHI from the EHI subject to the individual's request not to share. The actor notifies the requestor in writing in 10 business days from the receipt of the request that the actor cannot unambiguously segment the EHI from the EHI that the actor cannot share for reasons consistent with the § 171.204(a)(2) *segmentation* condition. The actor provides the requestor with EHI the actor can unambiguously segment from the EHI that is subject to the individual's request, and the actor does not provide the requester with certain EHI that the actor cannot unambiguously segment from the EHI subject to the individual's request.

- For purposes of this example, the actor has two exceptions available. First, the actor has received an individual's request not to share information, elected to grant the individual's requested restriction on access, exchange, or use of EHI, and met the requirements of the § 171.202(e) Respecting an Individual's Request Not to Share Information sub-exception of the Privacy Exception. (Note: for purposes of the § 171.202(e) Respecting an Individual's Request Not to Share Information sub-exception, an actor (such as a health IT developer of certified health IT) who maintains or manages EHI on behalf of another entity (such as a health care provider) [229] can rely on the other entity's practice that meets the sub-exception's requirements; the individual need not make a duplicative request for EHI sharing restrictions directly to the actor who is maintaining or managing EHI on behalf of the other entity.) Because the actor met the requirements of that sub-exception, the actor's practice of not providing the requested EHI that cannot be made available due to the individual's request would not constitute information blocking.
- Second, the actor cannot unambiguously segment certain EHI from the EHI that would not be made available due to the individual's request

[228] It is important to remember that the information blocking exceptions defined in 45 CFR part 171 subparts B and C are voluntary, offering actors certainty that any practice meeting the conditions of one or more exceptions would not be considered information blocking. An actor's practice that does not meet the conditions of an exception would not automatically constitute information blocking. *See, e.g.,* IB.FAQ29.1.2020NOV, URL: *https://www.healthit.gov/faq/if-actor-does-not-fulfill-request-access-exchange-and-use-ehi-any-manner-requested-they-have.* (Retrieved 7/12/2023.)

[229] ''Entity'' as used in this paragraph could be an individual (such as a licensed health care professional) or an organization (such as a health care facility).

that the actor has agreed to honor. The Infeasibility Exception is satisfied by a practice that meets a condition in paragraph (a) of § 171.204, such as the *segmentation* condition (171.204(a)(2)) and the *responding to requests* condition in § 171.204(b). Meeting the § 171.204(b) condition does not require that an actor fulfill any EHI in response to any request but does require that the actor provide the requestor within 10 business days of receipt of the request, in writing, the reason(s) the request is infeasible. Thus, the actor in this example would satisfy the Infeasibility Exception for that portion of EHI that cannot be unambiguously segmented from EHI that cannot be made available due to the individual's request that the actor has agreed to honor. In this example, no other exceptions apply to the EHI that the actor can unambiguously segment from the EHI that cannot be shared because the actor has agreed to the individual's request not to share certain EHI. The actor, therefore, provides the EHI that can be unambiguously segmented and is not subject to the individual's request not to share information in response to the request. If the actor did not provide the EHI that can be unambiguously segmented, then the actor might be engaged in information blocking with respect to the EHI that can be unambiguously segmented.

We note that this is only one example to illustrate how the ''stacking'' of exceptions may occur. We have chosen to detail here an example scenario where an individual has requested restrictions to reinforce actors' and individuals' awareness of the § 171.202(e) sub-exception and to emphasize that the information blocking regulations accommodate actors' choosing to respect an individual's request for restrictions on EHI about the individual. We emphasize, however, that there may be a wide variety of scenarios where ''stacking'' other combinations of various exceptions with one another, or with restrictions on use or disclosure of EHI under applicable law, may occur.

Again, we refer actors and other persons interested in learning more about how the information blocking regulations, and particularly the exceptions, work in concert with the HIPAA Rules and other privacy laws to support health information privacy, to the blog post [230] as well as the frequently asked questions referenced and linked above.

We will issue additional guidance as needed and intend to propose additional exceptions in future rulemaking to further support health information privacy, including for information that patients may view as particularly sensitive such as reproductive health-related information.

Comments. A commenter expressed concern about the applicability of information blocking regulations where there are data interoperability problems resulting from different implementations of standards by different EHR vendors.

Response. We thank the commenter for their input. However, we did not propose information blocking provisions specific to this topic in the HTI–1 Proposed Rule.

B. Defined Terms

1. Offer Health Information Technology or Offer Health IT

''Health IT developer of certified health IT'' is defined for purposes of the information blocking regulations in 45 CFR 171.102. As we discussed in the ONC Cures Act Final Rule (85 FR 25798 through 25799), the definition finalized in that rule includes offerors of certified health IT who do not themselves develop certified health IT or take responsibility for the health IT's certification status under the Program. Specifically, we explained that ''an individual or entity that offers certified health IT'' would include ''any individual or entity that under any arrangement makes certified health IT available for purchase or license'' (85 FR 25798, quoted and cited in the HTI–1 Proposed Rule at 88 FR 23857). Both individuals or entities that otherwise fall into at least one category of actor as defined in 45 CFR 171.102—such as health care providers—and individuals or entities that otherwise would not fit the definition of any category of actor could offer certified health IT that they did not themselves develop or present for certification. As offerors of certified health IT, these individuals or entities could engage in conduct that constitutes information blocking as defined in § 171.103, such as through contractual terms or practices undertaken in operating and maintaining health IT deployed by or for another individual or entity.

As discussed in the HTI–1 Proposed Rule (88 FR 23858), we proposed to codify in § 171.102 a definition of what it means to *offer* certified health IT. As proposed, the definition would provide clarity about the implications under information blocking regulations of making available funding subsidies and certain features or uses of certified health IT as well as engaging in certain other conduct (as discussed in more detail below). Specifically, we proposed to define the term ''offer health information technology'' or ''offer health IT.'' For ease of reference, in this preamble, we will generally use the shorter version of the term, ''offer health IT'' when discussing or referencing the definition. In light of our proposal to establish the ''offer health IT'' definition, we also proposed (*see* 88 FR 23915 and 88 FR 23864) to update the wording of the ''health IT developer of certified health IT'' definition specific to the exclusion of certain self-developer health care providers. The proposal specific to the ''health IT developer of certified health IT'' definition is summarized and discussed in section IV.B.2 below.

As explained at 88 FR 23858 through 23859, the definition we proposed for offer health IT generally includes providing, supplying, or holding out for potential provision or supply, certified health IT under any arrangement or terms, but explicitly excludes arrangements and activities specified in paragraphs (1) and (2) of the *offer health IT* definition (which are discussed in detail in section IV.B.1.a and b, below). We proposed exclusions of certain arrangements and activities from the offer health IT definition to serve two primary purposes:

(1) to encourage certain beneficial arrangements under which providers in need can receive subsidies for the cost of obtaining, maintaining, or upgrading certified health IT; and

(2) to give health care providers (and others) who use certified health IT concrete certainty that implementing certain health IT features and functionalities, as well as engaging in certain practices that are common and beneficial in an EHR-enabled healthcare environment, will *not* be considered an offering of certified health IT (regardless of who developed that health IT).

We also proposed (in paragraph (3) of the offer health IT definition in § 171.102) to exclude from the offer health IT definition the furnishing of certain legal, health IT expert consulting, or management consulting services to health care providers or others who obtain and use health IT. The paragraph (3) consulting and legal services exclusion is discussed in detail in section IV.B.1.c, below.

The HTI–1 Proposed Rule included examples illustrating when certain arrangements or activities would or would not fall within a proposed

[230] *https://www.healthit.gov/buzz-blog/information-blocking/information-blocking-regulations-work-in-concert-with-hipaa-rules-and-other-privacy-laws-to-support-health-information-privacy* (Retrieved 12/07/2023.).

exclusion (paragraphs (1), (2), and (3)), and clarified that if any individual or entity that engages in some conduct consistent with an exclusion from the offer health IT definition but also engages in other conduct that meets the definition of offer health IT, that individual or entity would be considered a health IT developer of certified health IT. We noted that once an entity meets the definition of health IT developer of certified health IT based on any of its conduct, that definition will apply to all practices of the entity.[231] (*see* 88 FR 23860 through 23864).

Comments. More than thirty commenters' submissions included comments on the offer health IT definition, health IT developer of certified health IT definition, or both definitions. Of these, over a dozen expressed general support and none expressed general opposition to the proposals.

Response. We appreciate all commenters' feedback. We have finalized the proposed offer health IT definition with one revision to the wording to replace ''for use by'' with ''for deployment by or for'' other individual(s) and entity(ies). Our response to the comments summarized immediately below explains why we believe this finalized wording change improves clarity of the definition for actors and other interested parties.

Comments. With a reference to the exclusion proposed in paragraph (2) of the offer health IT definition in § 171.102, the Health Information Technology Advisory Committee (HITAC) recommended that we clarify that providing access to registries and similar data services provided by public health authorities is not considered providing health IT, regardless of the route used to request/access/receive data (*e.g.,* through direct logon to a public health information system, via an app or third-party tool, or via HIN/HIE). The recommendation's rationale was stated as: ''This change is necessary to provide users the flexibility to connect to the data resource in the manner of the user's choosing.'' Other comments requested that we explicitly exclude, or clarify whether the offer health IT definition excludes, an actor making EHI available through an API or enabling interaction with an API. Commenters also requested clarification on whether such an API-related exclusion would apply to specific types of individuals or entities, or to specific purposes.

Response. Although focused on the detail of the exclusion proposed in paragraph (2) of the offer health IT definition in § 171.102, HITAC's comment informed our review of the interaction between the wording of the proposed offer health IT definition and the distinction between the roles of API User and API Information Source, as we had already defined these roles in § 170.404(c) and (by cross-reference) § 171.102. Specifically, we believe that wording the offer health IT definition in § 171.102 to focus (as proposed, *see* 88 FR 23915) on holding out or providing or supplying under any arrangement certified health IT ''for use by'' others may be a source of uncertainty for health care providers, and for others who deploy Certified API Technology in the role of an API Information Source. This uncertainty, we believe, relates to the implications for purposes of the offer health IT definition of a health care provider or other individual or entity in the role of an API Information Source making Certified API Technology available to individuals and entities (other than their own employees and contractors) in the role of API User.

At this point, a brief review of the distinction between our definitions of the API User and API Information Source roles, with reference to their establishment in the ONC Cures Act Final Rule (85 FR 25748 through 25749), may help to explain why we now believe clarity is improved by aligning the wording of the offer health IT definition with those two definitions. In the ONC Cures Act Final Rule, we finalized in § 170.404(c) definitions of API User and API Information Source for purposes of the ONC Health IT Certification Program, and by cross-reference to § 170.404(c) adopted those same definitions for purposes of the information blocking regulations in 45 CFR part 171. As discussed in the ONC Cures Act Final Rule at 85 FR 25748 through 25749, we received in response to the ONC Cures Act Proposed Rule (*see* 84 FR 7477 for preamble discussion, 84 FR 7588 for proposed definitions) comments requesting a definition of a ''First-Order User'' (to include patients, health care providers, and payers that use apps/services) and a definition of a ''Third-Party Users'' (to include third-party software developers, and developers of software applications used by ''API Data Providers''). We decided, as explained in the ONC Cures Act Final Rule (85 FR 25748 through 25749), that such a distinction was unnecessary from a regulatory perspective, and we finalized the API User definition in § 170.404(c) (85 FR 25948) as ''a person or entity that creates or uses software applications that interact with the 'certified API technology' developed by a 'Certified API Developer' and deployed by an 'API Information Source.' '' We also defined an API Information Source as an organization that deploys certified API technology created by a Certified API Developer. We noted in the ONC Cures Act Final Rule that the definitions finalized in § 170.404(c) were created to describe relationships and to help describe the Condition and Maintenance of Certification requirements to which developers participating in the ONC Health IT Certification Program are subject (85 FR 25749).[232]

A vast array of interoperable health IT items and services are designed and implemented specifically to achieve increasingly efficient access, exchange, and use of EHI for a wide range of permissible purposes. Thus, in an interoperable health IT ecosystem, one may see third-party apps adopted and used by patients, health care providers, health plans, public health authorities, researchers, and others to achieve access, exchange, or use of EHI by connecting to, interacting with, or otherwise making use of Health IT Module(s) deployed within, for example, a health care provider's EHR system or a public health authority's case reporting infrastructure. Our definition of API User in 45 CFR 170.404(c) illustrates this expectation: it includes both those who create and those who use software applications that interact with API technology deployed by anyone functioning in the role of an API Information Source.

We have revised the wording of the finalized offer health IT definition in order to improve certainty for individuals and entities who function in the role of an API Information Source (as defined in § 171.102 by cross-reference to § 170.404(c)) or function in an equivalent role where any APIs involved are not certified but may be part of health IT product(s) that also include one or more Health IT Modules certified under the Program. Specifically, we have replaced in the finalized offer health IT definition the phrase ''for use'' with the phrase ''for

[231] Because we are aware that health care provider organizations may be, have, or include one or more physician or other clinicians' professional practices, we note for readers' clarity that unless otherwise specified (such as by being preceded by ''clinician'' or ''office''), we use the word ''practice'' throughout the section IV of this preamble with the meaning it has in 45 CFR 171.102 (*i.e.,* ''an act or omission by an actor'').

[232] As we clarified in the ONC Cures Act Final Rule (85 FR 25749), health care providers are not subject to the Condition and Maintenance of Certification requirements in § 170.404(c) ''unless they are serving the role of a 'Certified API Developer.' ''

deployment by or for.'' We believe this wording is more consistent with the distinction between the act of connecting to, interacting with, or otherwise making use of a health IT item or service (for example, as an API User) and the act of allowing for such connections or interactions with the health IT that an individual or entity (for example, a health care provider) relies on in conducting its own business operations.

In addition, we believe this updated wording encompasses the full array of models through which individuals and entities obtain health IT for implementation or other deployment in their operations. We include ''or for'' in this finalized wording to ensure it is clear that the offer health IT definition is met regardless of whether the customer to whom the health IT is provided or supplied deploys the health IT by themselves or deploys the health IT by having the offeror or any third party(ies) do some or all such implementation and maintenance for them.

Providing or supplying health IT that includes one or more Health IT Modules certified under the Program meets the offer health IT definition finalized in § 171.102 regardless of whose employees, contractors, or consultants actually install, configure, manage, or maintain such health IT or other health IT with which such health IT may be integrated, interfaced, or otherwise interact. Likewise, holding out such health IT meets the offer health IT definition regardless of whose employees, contractors, or consultants would be needed, expected, or likely to set it up, manage, or maintain it in the event the holding out of the health IT resulted in the health IT being provided or supplied to one or more other individual(s) or entity(ies). To reinforce this clarity, we note that ''deployment by or for'' includes, without limitation, all of the following examples in which an individual's or entity's conduct would meet the offer health IT definition (and thus meet the health IT developer of certified health IT definition) in § 171.102:

- An individual or entity holds out, or provides or supplies, health IT for deployment by or for potential customer(s) under a software-as-a-service (SaaS) model, infrastructure-as-a-service (IaaS) model, or any combination of these and other model(s) under which the offeror would implement and maintain on behalf of the customer any instance of the health IT. For purposes of this example, it would not matter whether a single-tenant instance would be implemented for each customer or whether one or more customer(s) would share multiple-tenant instance(s) of the health IT with the offeror or other customer(s).
- An individual or entity holds out, or provides or supplies, health IT for the customer(s) to implement themselves, using any combination of their own employees and contractors, any single- or multiple-tenant instance(s) of the health IT.
- An individual or entity holds out or provides or supplies health IT that is implemented by a third party to customers. For purposes of this example, it would not matter whether a single-tenant instance would be implemented for each customer or whether one or more customer(s) would share multiple-tenant instance(s) of the health IT with the third party or other customer(s).

Comments. One commenter requested that we provide guidance or examples of how we define ''beneficial'' and ''necessary'' in the context of the exclusions from the *offer health IT* definition. A commenter requested guidance on our use of the verb ''hold out'' in the *offer health IT* definition. (Comments specific to particular exclusions are addressed in subsections IV.B.1.a through c, below.)

Response. In the HTI–1 Proposed Rule, we discussed our purposes for proposing the exclusions, including ''to encourage beneficial arrangements under which providers in need can receive subsidies for the cost of obtaining, maintaining, or upgrading certified health IT.'' Thus, ''encourage[ing] beneficial arrangements'' explains our intent and rationale for the exclusions (88 FR 23858) and the term ''beneficial'' does not appear in the text of any of the exclusions. The text of each exclusion defines and describes the arrangements that it excludes from the offer health IT definition.

The word ''necessary'' appeared in the proposed text describing excluded legal services furnished by outside counsel (subparagraph (3)(i) of the § 171.102, offer health IT definition). We did not propose to establish a purpose-specific meaning for the word ''necessary'' in this context. We intended it to have its widely understood and commonly used meaning of absolutely needed, required, or of an inevitable nature.[233] Upon review of the comments, we have concluded that we can improve the clarity of subparagraph (3)(i) by deleting the word ''necessary.'' The updated language uses the phrase ''as appropriate to legal discovery'' to encompass the activity of facilitating the access or use of the client's health IT when it is necessary as well as when it may be only one of the practicable options through which the counsel's clients can fulfill their legal discovery obligations.[234]

We use the term ''hold out'' in the text of the offer health IT definition as a transitive verb. As such, we believe ''hold out'' is generally understood in common usage to mean presenting an item or service as something realizable, attainable, or for acceptance.[235] With his common usage in mind, we use ''hold out'' to ensure it is clear that an individual or entity's activities can meet the definition of offer health IT without anyone accepting the proffer of a sale (or resale) or of a license (or relicense), and without anyone otherwise obtaining or using any Health IT Module(s) from that individual or entity. This operates as a safeguard against, for example, the holding out for sale or license one or more ONC-certified Health IT Module(s) (or products containing such Module(s)) and ultimately only agreeing to provide non-certified health IT in an attempt to avoid meeting the *offer health IT* definition and to avoid being subject to information blocking regulations. For purposes of the information blocking regulations, if any individual or entity is holding out health IT that includes one or more ONC-certified Health IT Modules, that individual or entity will be considered to be offering health IT and thus would meet the definition of health IT developer of certified health IT.

We further note that whether such a scenario might implicate other federal or state laws does not affect whether an individual or entity's conduct meets the offer health IT definition.

Comments. A commenter requested we ensure adequate protection of the

---

[233] *See* definitions of the adjective ''necessary'' by

- *Merriam-Webster Dictionary:* ''1: Absolutely needed: required; 2 a of an inevitable nature'' (*https://www.merriam-webster.com/dictionary/necessary#:~:text=%3A%20absolutely%20needed%20%3A%20required,of%20an%20inevitable%20nature%20%3A%20inescapable,* retrieved Nov 7, 2023);
- *Dictionary.com:* ''1. Essential, indispensable, or requisite. 2. Happening or existing by necessity.'' (*https://www.dictionary.com/browse/necessary,* retrieved Nov 7, 2023).

[234] The offer health IT definition exclusion in subparagraph (3)(i) encompasses the activities by counsel it describes for both EHI and other electronically stored information (ESI). For purposes of legal discovery, ESI includes writings, drawings, graphs, charts, photographs, sound recordings, images, or other data or data compilations. (*See, e.g.,* Fed. R. Civ. P. 34(a)(1)(A).).

[235] *See e.g., https://www.merriam-webster.com/dictionary/hold%20out* (Retrieved Jul 6, 2023): ''to present something as realizable: proffer.''

provision of open-source tools developed by open-source communities, irrespective of the terms on which they are made available, whether the tool is necessary for use of the product or the provision of care or whether the tool is integrated into a certified health IT product as part of the product. This comment appears to convey uncertainty on the commenter's part about whether a health care provider's (for example, a health system) integration of open-source modules with the certified health IT products it deploys (or has deployed by a third party on its behalf) to support its provision of patient care and other operational activities meets the offer health IT definition. The commenter also encouraged ONC to ensure that the provision of clinical decision support modules by a health system through an open-source community is protected. This comment also appears to convey uncertainty on the commenter's part as to if or when a participant in an open-source community might be considered to offer health IT and, therefore, would meet the health IT developer of certified health IT definition in § 171.102.

Response. We will discuss here how the finalized definition addresses these concerns, in the order in which they are summarized above.

First, specific to a health care provider deploying open-source health IT to support its provision of patient care and other operational activities, we do not believe that the fact that the health care provider is deploying open-source health IT impacts the analysis. As we discussed above, the offer health IT definition as finalized aligns with the API User and API Information Source role definitions previously established in § 171.102 and we believe the finalized definition of offer health IT provides clarity that deploying [236] health IT that incorporates one or more Health IT Modules certified under the Program is not an activity that meets the offer health IT definition, regardless of whether, or how much of, the health IT in question was developed by an open-source community or any other source or developer of health IT. For purposes of the finalized offer health IT definition, we do not treat deploying a health IT product developed by an open-source community different from deploying a health IT product developed by a commercial developer.

Also of note, the finalized offer health IT definition focuses on the holding out or provision or supply of certified health IT products for deployment by or for other individual(s) or entity(ies). As cited in the HTI–1 Proposed Rule in connection to the proposed implementation and use activities exclusion (paragraph (2) of the offer health IT definition (88 FR 23860)), we noted in the ONC Cures Act Final Rule that ''some use of a self-developer's health IT may be made accessible to individuals or entities *other than* the self-developer and *its employees* without that availability being interpreted as offering or supplying the health IT *to other entities* in a manner inconsistent with the concept of 'self-developer' '' (85 FR 25799, emphasis added). We add emphasis here to ''other than . . . its employees'' and ''to other entities'' to highlight that the offer health IT definition is not met by an individual or entity deploying health IT for use or implementation in their own operations by their employees and contractors in the course of employment or scope of the contract. We further note that the offer health IT definition is not met when the action is deployment that makes the health IT available to individuals in certain non-employee roles other than the deploying entity's contractors. For these reasons, a health care provider deploying health IT in the health care provider's own operations would not meet the offer health IT definition—whether the health IT is open-source or not.

Turning to the question of participation in an open-source development effort, we believe the question of which participants in such communities fall within the definition of offer health IT is, necessarily, dependent on the specific facts and circumstances of any given case. For example, relevant facts would include which participants in an open-source community have undertaken what role(s) and responsibility(ies) in relation to the certification status of the Health IT Module(s) involved.

The question of whether or when a participant in an open-source community engages in conduct that constitutes holding out, or providing or supplying, health IT that includes at least one certified Health IT Module is similarly, and also necessarily, dependent on the specific facts and circumstances of the conduct. In any case, it is also important to recall that the offer health IT definition that we proposed, and have finalized, cannot be met unless the technology held out, or provided or supplied, for deployment by or for others includes one or more Health IT Module(s) certified under the Program. To the extent an open-source community produces only non-certified health IT items or services, the development or offering of that non-certified health IT would not, of itself, result in the community or its participants being considered health IT developers of certified health IT—regardless of whether the product is intended, designed, or fit for use only in conjunction with certified health IT in general or specific certified health IT product(s). The community's exclusively non-certified health IT items or services may be styled, branded, named by the community, or commonly referenced in the marketplace as products, apps, modules, or something else without affecting whether the community's conduct falls within the § 171.102 offer health IT definition. Neither the holding out nor the providing or supplying of entirely and exclusively non-certified health IT can meet the offer health IT definition.

We recognize that once integrated with any deployment of a compatible certified product (such as ONC-certified EHR software), a non-certified health IT item such as a macro or template might be difficult or impossible for the end user (such as a doctor using a health system's EHR system to document a diagnosis) to distinguish from the certified health IT product. For individuals or entities who deploy certified health IT product(s), we recognize that sharing such items with others may raise questions similar to the one posed by the comment specific to open-source health IT: does sharing with other individuals or entities a non-certified item that, as experienced by end users, may seem like part of a certified health IT product meet the offer health IT definition? [237]

We note that whether an actor's conduct meets the offer health IT definition is *not* determined by the end user's perception of what is or is not part of a single certified health IT product. Likewise, whether an individual's or entity's conduct meets the offer health IT definition is not determined by whether a particular health IT item or service that is not *certified* health IT can or cannot be used independently of certified health IT. The individual's or entity's conduct can meet the offer health IT definition only when the health IT that the individual

[236] As discussed above, the individual or entity ''deploying'' the health IT need not, for purposes of the offer health IT definition, do any or all of the implementation or maintenance of the health IT. The deploying individual or entity could have any or all implementation and maintenance work for the health IT done for them by the offeror or one or more third party(ies).

[237] For ease of reference, we may sometimes refer to suites, bundles, or other combinations of health IT items, services, or functions that include one or more Health IT Modules certified under the Program as ''certified health IT products.''

or entity holds out, or provides or supplies, includes at least one Health IT Module certified under the ONC Health IT Certification Program.

Even if a non-certified health IT item or service (for example, a macro or template) can only be used in conjunction with a specific certified health IT product, the offer health IT definition is not met by holding out, or by providing or supplying, for deployment by or for others *only* the non-certified health IT item or service. For example, a health care provider might choose to make available to other members of a developer's user group a macro that works only with one of the developer's Health IT Modules that is certified to § 171.315(b)(3). The hypothetical macro in this example is not a Health IT Module that is certified under the Program, and does not include any Health IT Module(s) certified under the Program when the health care provider makes it available to other members of the user group. In this example scenario, the act of supplying the non-certified macro to other individual(s) or entity(ies) does not meet the definition of offer health IT.

For a similar example, an open-source community or its participants could make available a ''clinical decision support'' (CDS) algorithm. In this example, the CDS algorithm is not a Health IT Module that is certified under the Program. The act of holding out the algorithm for deployment by or for others does not meet the offer health IT definition because the algorithm is not certified health IT. Likewise, the act of providing or supplying the algorithm for deployment by others does not meet the offer health IT definition. If, however, the algorithm was included as a part of a certified health IT product, and an individual or entity holds out, or provides or supplies, the certified health IT with the algorithm in it for deployment by other individual(s) or entity(ies), that conduct would meet the offer health IT definition.

Comments. Two comments on the offer health IT definition referenced reporting requirements in connection to the offer health IT definition. These comments did not identify specific reporting requirements they perceived entities would become subject to by engaging in conduct meeting the offer health IT definition.

Response. As established by the ONC Cures Act Final Rule and updated by the provisions finalized in this rule, the information blocking regulations (45 CFR part 171) do not include any requirements for any actor to proactively report to ONC.

Comments. Several commenters suggested that hosting, the provision of hosting services, or ''extending their EHR'' by health care providers for other health care providers should be excluded from the definition of offer health IT. One such commenter stated a view that such organizations should not be considered to offer health IT and should not be subject to ''more stringent'' information blocking requirements.

Response. In the HTI–1 Proposed Rule, we did not propose defining what conduct would meet or not meet the offer health IT definition based on whether it was done by an individual or entity that otherwise meets the definition of any type of actor (as the term actor is defined in § 171.102). These commenters' rationale for excluding hosting, the provision of hosting services, or ''extending their EHR'' by health care providers for other health care providers centered on preventing health care providers engaged in such conduct from also meeting the definition of health IT developer of certified health IT. Therefore, we discuss in context of our proposal to update the health IT developer of certified health IT definition (*see* section IV.B.2 of this preamble, below) why we decline to establish at this time any regulatory provision with the effect these comments advocate.

Summary of finalized policy—offer health IT: we have finalized the proposed offer health information technology or offer health IT definition with a revision to its wording in response to comments received. The wording revision is from ''for use by other individual(s) or entity(ies)'' to ''for deployment by or for other individual(s) or entity(ies).''

To increase clarity, we have further revised the definition by replacing the phrase ''under any arrangement other than the following'' with ''under any arrangement except an arrangement consistent with subparagraph (3)(iii), below.'' As discussed above, activities described in other paragraphs and subparagraphs we do not interpret as holding out or as providing or supplying health IT for deployment by or for other individuals or entities. Thus, only subparagraph (3)(iii) functions to exclude from the offer health IT definition arrangements under which someone obtains from an individual or entity any certified Health IT Module(s).

To improve readability, we also revised the opening phrases of the definition. This revision was from ''. . . means to hold out for sale, resale, license, or relicense; or to sell, resell, license, relicense, or otherwise provide or supply health information technology (as that term is defined in 42 U.S.C. 300jj(5)) that includes one or more Health IT Modules certified under the ONC Health IT Certification Program, . . .'' to ''. . . means: to hold out for sale, resale, license, or relicense; or to sell, resell, license, relicense, or otherwise provide or supply health information technology (as that term is defined in 42 U.S.C. 300jj(5) and where such health information technology includes one or more Health IT Modules certified under the ONC Health IT Certification Program) . . .'' as finalized.

For readability, we added a second sentence to the offer health IT definition that also enhances clarity as to the function of the definition's subparagraphs on the whole. That added sentence reads: ''Activities and arrangements described in subparagraphs (1) through (3) are considered to be excluded from what it means to offer health IT.''

The finalized definition is shown in its entirety in the CFR amendatory instructions for § 171.102 (see ''Regulation Text'' section of this rule, below).

a. Exclusion of Certain Funding Subsidy Arrangements From Offer Health IT Definition

In the HTI–1 Proposed Rule, we included a provision to address concerns regarding the potential of some health care providers and other donors to stop making available funding subsidies that would go toward the cost of certified health IT in situations where the receiving health care provider is not able to afford the cost of the certified health IT. The proposal, in paragraph (1) of the offer health IT definition in § 171.102, explicitly excluded certain arrangements that focused on providing funding subsidies for providers to obtain, maintain, and/or upgrade certified health IT. We explained how this exclusion would operate in the HTI–1 Proposed Rule (88 FR 23859). We refer readers to the HTI–1 Proposed Rule for the full discussion of the donation and subsidized supply arrangements exclusion (paragraph (1)).

Comments. Of the comment submissions addressing this proposed exclusion, six supported exclusion of funding subsidy arrangements from the offer health IT definition. One comment submission did not express general opposition to the exclusion but expressed opposition to the definition of offer health IT excluding subsidies tied to a specific product, or excluding subsidies that would promote or

prioritize imaging referrals of patients to the subsidizing entity or its partners. This comment, from two large clinical societies, recommended that if we finalize this exclusion, we state in preamble that promotion or prioritization of the subsidizing entity's services over those of unaffiliated, competing providers would not be exempted from the offer health IT definition.

Response. We appreciate commenters' feedback. We have finalized the exclusion of funding subsidy arrangements (paragraph (1) of the offer health IT in § 171.102) as proposed (88 FR 23915). The donation and subsidized supply arrangements exclusion as proposed and as finalized is conditional, as indicated by this language in paragraph (1) of the offer health IT definition: ''provided such individual or entity offers and makes such subsidy without condition(s) limiting the interoperability or use of the technology to access, exchange, or use electronic health information for any lawful purpose.'' Thus, the donation and subsidized supply arrangements exclusion (paragraph (1)) does *not* apply if the subsidy is conditioned on limiting the interoperability or use of the technology to access, exchange, or use EHI for any lawful purpose. Any agreement terms, statements (written or oral), patterns of conduct, or singular actions whereby the source of donation or funding subsidy conditions the donation on the recipient's limiting its use of health IT or its access, use, or exchange of EHI in ways specified or signaled by the funding source would be considered a condition limiting interoperability or use of the technology. Therefore, we do not believe that the purpose of this exclusion would be better served by limiting it at this time to arrangements under which recipients can choose to apply a funding subsidy to a minimum array of products or to any product on the market. However, we plan to remain alert for signals that funding subsidy sources may be misusing this exclusion.[238] We note that we may consider amending this definition in future rulemaking in response to changing market conditions.

We appreciate commenters' concerns about donation or subsidy arrangements tied to specific technology where the donation or arrangement is for the purpose of promoting referrals to the source of the funding or its affiliates. We believe the proviso in the donation and subsidized supply arrangements exclusion (paragraph (1)), as proposed, is sufficient to ensure it does not apply to arrangements conditioned by the source(s), donor(s), or giver(s) on limiting interoperability or use of the technology. As stated in the HTI–1 Proposed Rule, we do not believe it is necessary to assess, for purposes of determining whether a funding subsidy should be considered an offer of certified health IT, whether the source(s) of the subsidy conditions the subsidy on the recipient referring patients to or away from the source. As we noted, there may be other laws implicated by solicitation or receipt of any remuneration in return for referral steering and similar conduct (88 FR 23859). For example, the Federal Anti-Kickback Statute (42 U.S.C. 1320a–7b(b), section 1128B(b) of the Social Security Act) could be implicated where remuneration is directly or indirectly offered, paid, solicited, or received for the referral of or arrangement of a referral of any item, service, or good for which payment may be made in whole or part under a ''Federal health care program'' (as defined in 42 U.S.C. 1320a–7b(f)). Nothing in this final rule should be construed as creating an exception to any fraud and abuse laws.

In light of the commenters' concern, we believe it may be useful to clarify how the donation and subsidized supply arrangements exclusion from the offer health IT definition operates for purposes of 45 CFR part 171 in the context of a donor or funding source that is using a subsidy to steer referrals or to distort the market for healthcare items or services through a condition(s) that limit the use of donation-supported or subsidized technology or the lawful access, exchange, or use of EHI. As noted in the HTI–1 Proposed Rule (at 88 FR 23859), we interpret ''conditions limiting the interoperability or use of the technology to access, exchange, or use electronic health information'' broadly. Specifically, we noted we would consider conditions to include not only the explicit terms of any written agreement but also oral statements and patterns of conduct on the part of the subsidy's source(s) toward, in the presence of, or made known by the source(s) to the subsidy's recipient. We further noted that we would consider a condition(s) to include a subsidy source limiting the use of the subsidy to particular technology that includes, or otherwise arranges for subsidy-supported technology to include, features, functions, coding, or other means that would limit recipients' options to lawfully use that technology to access, exchange, or use EHI. A recipient health care provider's access, exchange, and use of EHI for such purposes is not limited to but necessarily includes access, exchange, and use by care team members in the course of making diagnosis and treatment decisions within their scopes of practice and making referrals in accord with their professional judgement and understanding of their patient's preferences.

The limitation on the application of the offer health IT definition's donation and subsidized supply arrangements exclusion in paragraph (1) of the definition is, as noted in the HTI–1 Proposed Rule, a safeguard against inappropriate use of the exclusion by entities seeking to distort the health IT market. This would include efforts to limit recipients' options to use additional technology or to otherwise impede innovations and advancements in health information access, exchange, and use (88 FR 23859). The donation and subsidized supply arrangements exclusion (paragraph (1)) applies only where the individual or entity donates, gives, or otherwise makes available funding *without* condition(s) limiting the interoperability or use of the technology to access, exchange, or use EHI for any lawful purpose. We did not propose that the exclusion could apply to any arrangement conditioned in any way on limiting the interoperability or use of the subsidy-supported technology or the recipient's use of the technology to access, exchange, or use EHI for any lawful purpose. We have finalized the exclusion as proposed.

We further clarify in view of comments received that the limitation on application of the donation and subsidized supply arrangements exclusion in paragraph (1) of the definition does not consider what underlying intent or motive the funding source may have for any condition that limit the interoperability or use of the

[238] Patterns described to us in claims or suggestions of possible information blocking submitted through the Report Information Blocking Portal represent just one example of the ways such signals may come to our attention. (The Report Information Blocking Portal's URL is: *https://inquiry.healthit.gov/support/plugins/servlet/desk/portal/6*). Information on the claims process that is publicly available on Health IT.gov (*https://www.healthit.gov/topic/information-blocking*) includes a fact sheet on the Report Information Blocking portal process (*https://www.healthit.gov/sites/default/files/page2/2021-11/Information-Blocking-Portal-Process.pdf*) and a resource titled ''Information Blocking Claims: By the Numbers'' (*https://www.healthit.gov/data/quickstats/information-blocking-claims-numbers*). As of October 2023, ''Information Blocking Claims: By the Numbers'' provides the total number of portal submissions received since April 5, 2021, the number of these submissions that represent claims of possible information blocking, and the number of these claims by type of potential actor and type of claimant. (URLs confirmed Oct 18, 2023.)

technology to access, exchange, or use electronic health information for any lawful purpose. Any condition that has such effect will mean the arrangement falls outside of the donation and subsidized supply arrangements exclusion (paragraph (1) of the offer health IT definition). Then, whether such non-excluded funding subsidy or donation arrangements would constitute the funding source offering health IT would have to be evaluated to determine whether the conduct constitutes holding out for sale, resale, license, relicense, or otherwise providing or supplying health information technology for deployment by other individual(s) or entity(ies).

To note, any third-party health IT developer of certified health IT or HIN/HIE that may be engaged in funding subsidy arrangements related to providing, configuring, or otherwise supporting health IT will want to bear in mind that their engagement in any practice they know or should know is likely to *interfere with* access, exchange, or use of EHI could constitute information blocking on the part of the actor (unless an applicable law requires or an exception set forth in 45 CFR part 171 is satisfied by such practice). This includes scenarios where the practice occurred at the direction of or on behalf of a funding subsidy source. This would be true for the health IT developer of certified health IT or an HIN/HIE regardless of whether the funding subsidy source or recipient is also an actor, and regardless of whether the funding subsidy source or recipient also engaged in conduct meeting the information blocking definition.

Comments. Several commenters recommended we adopt a policy under which a health care provider would not be considered to offer health IT, or be considered only a health care provider and excluded from the ''health IT developer of certified health IT'' definition, even if they ''extend their EHRs'' or otherwise donate or provide health IT on terms more affordable to a recipient than those available from other vendors of health IT items or services. Several commenters suggested such provision of health IT be excluded from the definition of offer health IT. A commenter that is a health system advocated for an explicit exclusion in situations where a health care provider hosts instances of a particular developer's EHR for other health care providers. A developer of certified health IT advocated to exclude from the definition of offer health IT any health IT resale or relicensing arrangements on non-discriminatory bases between health care providers or HIPAA covered entities. The developer's comment acknowledged the potential for organizations hosting or otherwise reselling health IT to make configurations or other implementation decisions potentially implicating the information blocking definition but asserted they had not observed this to have occurred among the providers reselling the developer's health IT.

Response. We appreciate commenters' sharing their experiences and perspectives. We did not propose that the donation and subsidized supply arrangements exclusion from the offer health IT definition would apply to a health care provider selling, licensing, or otherwise providing or supplying certified health IT (whether such health IT is self-developed by the provider offering it or obtained from a third-party developer) to other health care providers on a subsidized, discounted, or other basis. We decline to do so for reasons we discuss in this response and in Section IV.B.2 of this preamble below.

We cannot be certain whether commenters' reference to providers who ''extend their EHRs'' or similar wordings are meant to describe the donor health care provider entity selling, reselling, licensing, relicensing, or otherwise providing or supplying the health IT itself for deployment by the recipient providers. Therefore, to ensure clarity, we note that we perceive a clear distinction between two kinds of conduct. One distinct kind of conduct is donating, giving, or otherwise making available to a recipient funding to cover costs of an item or service (such as health IT that includes one or more Health IT Modules certified under the Program). A distinctly separate kind of conduct is the sale, resale, licensing, relicensing, or otherwise providing or supplying of the item or service itself to the recipient.

We proposed that the donation and subsidized supply arrangements exclusion (paragraph (1)) to encompass arrangements where ''an individual or entity donates, gives, or otherwise makes available funding to subsidize or fully cover the costs of a health care provider's acquisition, augmentation, or upkeep of health IT'' (88 FR 23915). We stated in the HTI–1 Proposed Rule that the proposed donation and subsidized supply arrangements exclusion ''would remove from the definition of *offer health information technology* or *offer health IT* the provision of subsidies, in the form of funding or cost coverage subsidy arrangements for certified health IT'' (88 FR 23859). We have finalized the donation and subsidized supply arrangements exclusion (paragraph (1)) of the offer health IT definition (§ 171.102) as proposed. Thus, the finalized first exclusion of the definition encompasses furnishing monetary resources (as described at 88 FR 23859, ''subsidies, in the form of funding or cost coverage subsidy arrangements'') for an item or service.

We reiterate that the donation and subsidized supply arrangements exclusion as proposed and as finalized in paragraph (1) of the offer health IT definition does *not* encompass any arrangement where an individual or entity does any of the following to or with any health IT that includes one or more certified Health IT Module(s):

- holds out the health IT for sale, resale, license, or relicense for deployment by or for other individual(s) or entity(ies);
- sells, resells, licenses, relicenses the health IT for deployment by or for other individual(s) or entity(ies); or
- otherwise provides or supplies the health IT for deployment by or for other individual(s) or entity(ies).

To prevent any potential confusion or misunderstanding about the significance of our reference to ''subsidized supply'' arrangements in the text of the exclusion in (paragraph (1) of the offer health IT definition, we note that this is included to explicitly recognize a type of arrangement whereby a donor or other subsidy source subsidizes or fully covers costs by payment of such costs to the individual or entity that develops or offers the health IT item(s) or service(s) subsidized.

For an example of a scenario in which the donation and subsidized supply arrangements exclusion (paragraph 1) applies: a health system arranges with a health IT developer that the health system will pay eighty-five percent of the cost of any contract for use of a (developer hosted) EHR product suite by any health care provider that gives the developer a particular code that was supplied to the health care provider by the health system. Note that in this example the EHR product suite includes one or more Health IT Modules certified under the Program (because the offer health IT definition is not met if health IT that is held out or that is provided or supplied does not include any such Health IT Module(s).) The health system gives the code to independent safety net providers in its service area as a means of making funding available to the safety net providers to cover part of the safety net providers' cost to obtain and maintain use of an EHR product suite. A critical part of an analysis of the application of the exclusion in this example is whether money covering (part of) the contract costs for health IT

is being supplied or whether the health IT itself is being supplied by the health system. Here the health system is only making a funding subsidy available. The health IT developer is supplying the health IT (EHR product suite).

In a different example, where a health system instead offers to host and support ONC-certified health IT for a safety net provider, the health system would be engaged in conduct to which the donation and subsidized supply arrangements exclusion (paragraph (1)) would not apply. Regardless of whether the entity doing the holding out or furnishing of health IT (or anyone else) would be subsidizing (in whole or in part) the costs of the health IT, the donation and subsidized supply arrangements exclusion (paragraph (1)) does not apply where an individual or entity holds out or, under any arrangement, provides or supplies for deployment by or for other individual(s) or entity(ies) any health IT product(s) that include one or more Health IT Modules certified under the Program.

We recognize that some health care providers, or other individuals or entities, may choose to engage, on a subsidized basis for the recipient or as a donation to the recipient, in conduct that is not encompassed by the exclusion in paragraph (1) but to which another exclusion to the offer health IT definition applies. In the interest of providing such individuals and entities certainty, we note that if any exclusion to the offer health IT definition applies to any particular conduct, it does not matter whether one or more other exclusion(s) do or do not also apply. If at least one exclusion applies to any particular conduct, that conduct is excluded from the offer health IT definition.

Finally, we note again that donation and subsidized supply arrangements can implicate other laws, including the Federal Anti-Kickback Statute and nothing in this final rule should be construed as creating an exception to any fraud and abuse laws.

We further discuss below, in the context of the health IT developer of certified health IT definition (section IV.B.2), our current position regarding health care providers who choose to engage in conduct that meets the offer health IT definition. However, it is important for providers and other individual(s) or entity(ies) interested in engaging in any conduct that meets the offer health IT definition to note that engaging in such conduct makes the individual or entity one that offers health IT. This means such an individual or entity will meet the health IT developer of certified health IT definition regardless of whether the individual or entity also happens to engage in any other conduct that is encompassed by an exclusion from the definition or that otherwise does not meet the offer health IT definition.

Comments. A commenter requested we confirm that subsidy arrangements where the funding source is not otherwise a § 171.102 actor are encompassed by the exclusion. The comment cited, as an example, subsidies from health plans to providers. Another comment recommended that we clarify the offer health IT definition excludes subsidy arrangements between healthcare entities, such as a health plan and community provider. Other comments suggested that we should reiterate that engaging in activities described in exclusion (1) is not a way for an individual or entity that is otherwise a § 171.102 actor to opt out of being subject to information blocking regulations.

Response. The finalized donation and subsidized supply arrangements exclusion (paragraph (1)) applies to the arrangements it describes. It does not specify characteristics that the source of the subsidy must have (or not have) for the arrangement to be excluded from the offer health IT definition. If any person engages in conduct described in paragraph (1), that means the excluded conduct does not fall within the definition of offer health IT. Thus, engaging in conduct described in paragraph (1) of the offer health IT definition will not turn an individual or entity who does not otherwise meet the § 171.102 actor definition into an ''actor'' for purposes of the information blocking regulations.

It is important to remember, however, that engaging in conduct described in the donation and subsidized supply arrangements exclusion (paragraph 1) simply has no effect on whether a person is not or is considered an actor as defined in § 171.102 for purposes of 45 CFR part 171. Even if an individual or entity that is otherwise an actor engages in conduct described in subparagraph (1) of the offer health IT definition, the person is still an actor. For example, if any entity meets the § 171.102 definition of health care provider then that entity is a health care provider regardless of whether it also happens to engage in conduct described in the donation and subsidized supply arrangements exclusion from the offer health IT definition. Also, any entity meeting the § 171.102 definition of health IT developer of certified health IT through any of its activities is a health IT developer of certified health IT regardless of whether it also happens to engage in conduct described in the donation and subsidized supply arrangements exclusion (paragraph 1).

A health care provider or health IT developer of certified health IT would remain subject to the information blocking regulations for any of their conduct that meets the definition of information blocking in § 171.103, including when that conduct occurs in the course of activities that fit the description of any exclusion from the offer health IT definition. Similarly, when and to the extent a health plan, health plan issuer, or any other entity engages in conduct meeting the functional definition of health information network or health information exchange (HIN/HIE), then that entity is a HIN/HIE regardless of whether the entity also happens to engage, at the same time, in conduct described in any exclusion from the offer health IT definition.[239]

Comments. A commenter who referenced experience with donation of hospital equipment noted it is important for recipients of donated technology to have access to design documents, data schema, and other resources needed to facilitate the use of donated health IT systems through maintenance, process improvement, and interoperability concerns. This commenter encouraged ONC to provide a broad dissemination of publicly available user manuals, access to spare parts, and consumable resources to facilitate the use of donated equipment. A commenter suggested we consider adjusting conditions of the donation and subsidized supply arrangements exclusion to address the impact of discontinued subsidies on the recipient's ability to maintain the health IT over time.

Response. We appreciate the concerns raised by these comments. Specific to Health IT Modules certified under the ONC Health IT Certification Program, our Program regulations in 45 CFR part 170 provide for public availability of certain information and documentation about the technology. (*See* 45 CFR 170.523 disclosures applicable to certified Health IT Modules, 45 CFR 170.404(a)(2) transparency conditions for Certified API Technology.) To the extent documentation needed to effectively use health IT products that include non-certified items and services in complement to one or more Health IT Module(s) certified under the Program, such documentation would fall outside

[239] The *health information network* or *health information exchange* definition is a functional definition. *See* 45 CFR 171.102, *see also* 85 FR 25800 through 85 FR 25803.

the scope of the Program's disclosures and transparency requirements. However, we believe the information blocking regulations discourage an actor from inappropriately withholding access to such documentation from recipients of their health IT. If an actor's practice of denying the recipients of health IT such information is likely to interfere with access, exchange, or use of EHI, that practice could implicate the information blocking definition. It is not clear what consumable supplies or spare parts relevant to health IT were referenced by the comment advocating ONC provide broad access to them. It is also not clear what is meant by the commenter advocating ONC ''provide access'' to spare parts and consumables. We note that the information blocking regulations maintain policies supportive of the access, exchange, and use of EHI and include policies under which the individuals and entities who actually supply health IT (donated or otherwise) for deployment by or for other individuals or entities generally continue to be subject to enforcement under the information blocking regulations as health IT developers of certified health IT.

Concerns specific to a supplier of technology withholding access to documentation and resources needed to use systems represents one example of conduct likely to interfere with a recipient's access, exchange, or use of EHI. This concern illustrates just one of many possible practices any individual or entity that engages in conduct meeting the finalized offer health IT definition would have opportunity to engage in that would be likely to interfere with customers' and others' ability to access, exchange, or use EHI in or through the health IT ''offered.'' Such opportunities to interfere with customers' access, exchange, or use of EHI are among the reasons we believe it would be inappropriate to exclude from the offer health IT definition the sale, resale, licensing, or relicensing of any Health IT Module based on such offering being subsidized by the offeror or a third party. Therefore, such conduct will generally continue to fall within the offer health IT definition. By engaging in any conduct falling within the offer health IT definition, the individual or entity engaged in the conduct meets the health IT developer of certified health IT definition and is subject to information blocking regulations accordingly.

We further note that this comment highlights the importance of prospective recipients of technology donations carefully considering the full terms of both the donation or subsidy arrangement and any contracts or other agreements with a developer, seller, reseller, licenser, or relicenser of the technology involved. For example, and for practical reasons entirely independent of the information blocking regulations, it is important for a recipient to know what items and services are included in the subsidy or donation and the level, extent, and duration of support for those items or services that the donation commits the funding source to cover. The information blocking regulations do not eliminate the need for anyone contemplating adopting health IT items or services pursuant to a donation or subsidy arrangement to consider and plan for their ability to maintain the health IT in good working order, or successfully transition away from it, at the end of a one-time donation or subsidy arrangement or in the event an arrangement providing an ongoing subsidy were to be discontinued (or not renewed). This would be true for adoption of initial, additional, upgraded, or replacement health IT items or services.

We also note that whether, as potential recipients of subsidized health IT or as a customer paying the full cost or market price themselves, all prospective recipients of any health IT will likely find it important to know and understand the terms of all agreements with the developer or offeror of health IT items or services they obtain. For example, a customer contemplating adoption of any health IT item or service would want to consider the potential that they may want to replace that particular product with another product in the future. Such a customer would want to look closely at how any data the product stores will be returned to the customer at the end of the agreement with the developer or other offeror of the health IT, and what support may be available, and on what terms, to help the customer (or a health IT developer or support contractor of the customer) import the data into the next product the customer will use to access, exchange, or use that data.

Recipients of donated health IT, like all customers of health IT, will also find it important to know whether technology they are considering for adoption includes any Health IT Module(s), or if the developer or offeror that would provide the technology has any Health IT Module(s), certified under the Program. An individual or entity that develops or offers health IT, but who does not develop or offer any certified Health IT, might not be subject to information blocking regulations unless the individual or entity is a health care provider or a HIN/HIE as defined in § 171.102.[240]

Summary of finalized policy—donation and subsidized supply arrangements exclusion (paragraph 1): After consideration of the comments received that are relevant to, and within the scope of, this proposal, we finalized the policy, as proposed. Provision of funding to a recipient who will use it to cover some or all of the recipient's health IT acquisition, augmentation, or upkeep cost is explicitly excluded from the offer health IT definition. Likewise, arrangements whereby a funding source (whether or not referenced or styled as a ''donor'') pays, remits, or otherwise transfers to a third-party funds covering the cost (in whole or part) of a health care provider's acquisition, augmentation, or upkeep of health IT are explicitly excluded from the offer health IT definition to the extent they are consistent with paragraph (1). However, the text of paragraph (1) explicitly and intentionally limits application of the donation and subsidized supply arrangements exclusion to those arrangements whereby the source of the subsidy makes available funding to cover costs of acquisition, augmentation, or upkeep of health IT. The finalized paragraph (1), donation and subsidized supply arrangements exclusion from the offer health IT definition, does *not* apply to sale, licensing, resale, relicensing, or provision or supply of the health IT itself—regardless of whether such provision or supply is on subsidized or other terms.

We reiterate that no individual or entity that otherwise meets the definition of any type of actor in § 171.102 can opt out of being subject to information blocking regulations by engaging in any activity excluded from the offer health IT definition.

b. Implementation and Use Activities That Are Not an Offering of Health IT

In the ONC Cures Act Final Rule, we noted that there are certain actions taken by health care providers who self-develop health IT for their own use that we do not interpret as them offering or supplying certified health IT to others (85 FR 25799). Specifically, we noted that ''some use of a self-developer's health IT may be made accessible to individuals or entities other than the self-developer and its employees without that availability being

[240] The § 171.102 health care provider and HIN/HIE definitions do not have a definitional component related to certified health IT. An individual or entity can meet either or both of these definitions without having, using, or offering any certified health IT.

interpreted as offering or supplying the health IT to other entities in a manner inconsistent with the concept of 'self-developer,' and we provided examples of activities that we do not consider offers (85 FR 25799). Some of the examples we noted (85 FR 25799) were discussed in the context of practices amongst hospitals that purchase commercially marketed health IT as well as self-developer hospitals.

While the examples focus on self-developers, these examples would not be considered ''offering'' health IT regardless of who developed the certified health IT. We also believe there are examples of activities we did not discuss that should not be considered offers of health IT. We, therefore, proposed in paragraph (2) of the offer health IT definition (*see* 88 FR 23860 and 88 FR 23915) to explicitly exclude from the definition of offer health IT certain implementation and use activities of a health care provider or other entity (such as a HIN/HIE, health plan, or public health authority). We refer readers to the HTI–1 Proposed Rule (88 FR 23860) discussions of the activities explicitly listed within the implementation and use activities exclusion from (paragraph (2) of) the definition of offer health IT we have now finalized within § 171.102.

We sought comment on this proposal, including whether we should consider revising or refining any of the descriptions or wordings of the functionalities, features, actions, or activities listed in the draft regulation text or whether we should consider explicitly excluding additional activities, actions, or health IT functionalities from what it means to offer health IT.

Comments. Comments referencing this exclusion supported the provision. Several commenters recommended specific refinements to the wording or clarifications to the intended scope of the exclusion. Comments were received that recommended the implementation and use activities exclusion encompass each of the following as implementation and use activities:

- a health care provider organization or other entity uses pre-production staging or test environments for certified health IT;
- use of health IT for purposes of clinical education and improvement activities, including in simulation environments where no care is furnished to actual patients;
- a health care provider providing a public health authority's employees or contractors with access to its health IT systems;
- providing access to registries and similar data services that are provided by public health authorities, regardless of the route used to request/access/receive data (*e.g.,* through direct logon to a public health information system, via an app or third-party tool, or via HIN/HIE).

Response. We appreciate the comments received on the proposed implementation and use exclusion. In response to comments received, we have revised the wording of the finalized regulation text in the offer health IT definition (as discussed in section IV.B.1 of this rule, above) and have also revised the wording of subparagraphs within paragraph (2) (discussed in the *summary of finalized policy—implementation and use exclusion (paragraph (2))* at the end of this section, IV.B.1.b, of this rule).

As discussed in section IV.B.1 of this final rule, we reviewed the wording of the offer health IT definition in light of a HITAC comment about providing access to registries and similar data services provided by public health authorities, regardless of the route used to request/access/receive data. We believe the change in the offer health IT definition's wording from ''for use by'' to ''for deployment by or for'' better aligns the wording of this definition with the definitions of ''API User'' and ''API Information Source'' previously established in § 171.102 by cross-reference to § 170.404(c) (as discussed in section IV.B.1 of this rule, above). We also believe this wording change removed a need to catalog within paragraph (2) all of the various manners in which access, exchange, or use of EHI with public health entities and with others might be accomplished without the individual or entity in the API Information Source role (or equivalent role for non-certified API technology or other manners of access, exchange, or use) meeting the offer health IT definition.

The excluded activity descriptions in subparagraphs (2)(ii), (iii), and (iv) are intended to accommodate current heterogeneity in how individuals and entities who deploy health IT (such as health care providers) make EHI available for access, exchange, or use by their information sharing partners. With the minor changes in wording that we mention above, we believe it is clear that subparagraphs (ii) through (iv) of paragraph (2) in conjunction with the revision to the offer health IT definition's wording accomplish this intent. Although subparagraph (2)(ii) discusses APIs and (2)(iii) discusses online portals, we believe that they, when taken together with subparagraph (2)(iv), provide for extensive heterogeneity in the manners of information sharing available now or in the future to those who access, exchange, or use EHI. Moreover, we believe the wording change that we discuss above from ''for use by'' to ''for deployment by or for'' also addresses commenters' concerns about whether the offer health IT definition does or does not include interactions with or use of pre-production or other non-production instance(s) of API technology.

We also reiterate that, as we stated in the HTI–1 Proposed Rule (88 FR 23860), we do not believe it is necessary to define a production instance because we observe health IT developers, resellers, and customers generally using and understanding a production instance as a particular implementation of a given health IT product that has ''gone live'' in a production environment (without needing to specify, for this purpose, whether such instance is single- or multi-tenant). Production environments, in turn, we observe are generally understood as being the setting where health IT is implemented, run, and relied on by end users in day-to-day conduct of their profession (such as medicine, nursing, or pharmacy) or other business (such as a payer processing healthcare reimbursement claims or a patient managing their health and care).

Summary of finalized policy—implementation and use activities exclusion (paragraph 2): After consideration of comments, we have finalized the proposed implementation and use activities exclusion (paragraph (2)) with revisions. As described in more detail below, we have refined how we describe several types of activities within the exclusion.

We have struck from subparagraph (2)(i), (ii), (iii), and (iv) the parenthetical ''as defined in this section'' following the terms ''electronic health information'' and ''health information network or health information exchange.'' The § 171.102 definitions of these terms apply throughout 45 CFR part 171 unless otherwise specified in a particular subpart or section. Thus, the presence or absence of this parenthetical has no effect on the meaning of the subparagraphs noted above and has been removed from the final text.

The wording of the activity description in subparagraph (2)(i) has been revised to remove reference to employees or contractors using the individual's or entity's health IT to access, exchange, or use EHI in the course of their employment. Instead, the exclusion lists a variety of types of

activities that an individual's or entity's employees or contractors might do within the scope of their employment or contract duties specific to, or otherwise requiring use of, access to the health IT. The finalized wording of subparagraph (2)(i) explicitly includes use, operation, configuration, testing, maintenance, update, and upgrade activities for an individual's or entity's health IT system(s) or specific application(s) within such systems. It also includes explicit reference to the individual's or entity's employees or contractors giving or receiving training on the health IT.

We believe this explicit list of purposes for which employees or contractors might need to use an individual's or entity's deployed health IT provides the clarity some commenters sought regarding a health care provider maintaining non-production instances of health IT for various purposes other than supporting care delivery, documentation, or billing of healthcare. We believe this clarity is achieved by the rewording of subparagraph (2)(i) in complement to the change from ''for use by'' to ''for deployment by or for'' others in the offer health IT definition.

We have finalized subparagraph (2)(ii) with one revision to its wording: we have removed the parenthetical statement ''(whether certified or not)'' to improve readability. The deletion of ''(whether certified or not)'' has no effect on the substance of subparagraph (2)(ii) because the description references API technology in general. As used in subparagraph (ii) of the implementation and use activities exclusion, ''application programming interface (API) technology'' encompasses ''Certified API Technology'' as defined in 45 CFR 170.404(c) as well as any other API technology.

As proposed, subparagraph (2)(ii) referenced production instances and did not reference pre-production instances. We have retained reference to ''production instances'' of API technology in the excluded activity description in the finalized definition as the finalized offer health IT definition's wording change from ''for use by'' to ''for deployment by or for'' makes it unnecessary to explicitly encompass pre-production instances within subparagraph (2)(ii) of exclusion (2). Specifically, the revised wording of the offer health IT definition makes it clear that deploying any instance(s) of API technology with which independent, outside persons participating in testing activities might interact (in the course of testing or QI activities, or in the role of API User as defined in § 171.404(c) or an analogous role for health IT other than ''Certified API Technology'' as defined in § 171.404(c)) does not, in and of itself, meet the offer health IT definition. By contrast, the holding out, or the providing or supplying, for deployment by or for other individuals or entities under any arrangement not described in exclusion (3)(iii) of health IT that includes one or more Health IT Module(s) would meet the offer health IT definition, regardless of whether such other individual(s) or entity(ies) were to deploy (or have deployed on their behalf) production instance(s), pre-production instance(s), or any combination of production and pre-production instances of the offered health IT.

We have removed from the finalized text of subparagraph (2)(iii) a comma that immediately followed the word ''clinicians.'' This comma was a typographical error that has been corrected so that the finalized text describes making portals available to any or all of the following: patients, clinicians or other health care providers, or public health entities. We use ''public health entities'' here to encompass public health authorities, their employees, and their contractor(s) acting in the scope of the contract to the public health authority.

Specific to implementation and use activities of entities that need to share information with public health authorities, the revised wording of the offer health IT definition (from ''for use by'' to ''for deployment by or for,'' as discussed in section IV.B.1 of this preamble) renders the presence or absence of specific reference in subparagraph (2)(iii) or (iv) to public health authorities' contractors largely moot, because the activities subparagraphs (iii) and (iv) describe (as proposed and finalized) do not involve or include supplying health IT for deployment. However, we proposed the implementation and use activities exclusion (paragraph (2)) for the purpose of giving health care providers (and others) who use certified health IT certainty that implementing certain health IT features and functionalities, as well as engaging in certain practices that are beneficial in an EHR-enabled healthcare environment, will not be considered ''offering'' certified health IT (regardless of who developed that health IT) (88 FR 23858). Therefore, we have finalized subparagraph (2)(iv) with addition of explicit reference to public health authorities' contractors to better serve subparagraph (2)(iv)'s purpose.

By contrast, the activity described in subparagraph (2)(iv) was not proposed to, and as finalized does not, encompass supplying health IT for deployment by or for public health authorities or any other individual(s) or entity(ies). Holding out, providing, or supplying health IT that includes one or more certified Health IT Module(s) for deployment by or for a public health authority will meet the offer health IT definition. (*see also* the discussion of deployment versus use of health IT in section IV.B.1 of this preamble.)

We have modified the wording of subparagraph (v) of exclusion (2) in response to comments seeking explicit clarity regarding the implications of a healthcare facility potentially allowing independent healthcare professionals who furnish services in a healthcare facility to use the facility's health IT for clinical education and improvement activities or to receive training in the use of the healthcare facility's health IT systems. Specifically, following ''furnishing, documenting, and accurately billing for that care,'' we have added: ''participating in clinical education or improvement activities conducted by or in the healthcare facility; or receiving training in use of the healthcare facility's health IT system(s).'' With the clarification of the wording of the offer health IT definition (as discussed above in section IV.B.1 of this final rule) from ''for use by'' to ''for deployment by or for'' other individuals, we believe the distinction is clear between supplying independent healthcare professionals with health IT to deploy in their outside practice(s) or other endeavors and merely enabling independent healthcare professionals to use a healthcare facility's health IT systems in the course of the professional's engagement in patient care and other activities conducted by or in the healthcare facility.

As is the case for subparagraph (2)(iv), we have nevertheless decided to finalize subparagraph (2)(v) to serve the purpose for which we proposed it: giving health care providers (and others) who use certified health IT certainty that implementing certain health IT features and functionalities, as well as engaging in certain practices that are beneficial in an EHR-enabled healthcare environment, will not be considered ''offering'' certified health IT (regardless of who developed that health IT) (*see* 88 FR 23858 and 88 FR 23860).

We believe that patients generally benefit when independent healthcare professionals who practice in a particular facility participate in such activities as training for use of the facility's health IT and other equipment. We believe patients also generally benefit when independent healthcare professionals are able to participate in a facility's clinical education activities,

and we note that this includes the independent clinician conducting or leading clinical education or quality improvement activities in a facility for or with other professionals. Quality improvement and clinical education activities conducted in, but not necessarily by, the healthcare facility could include activities that occur in the facility that are partly or largely conducted by third parties (such as a professional specialty society, Patient Safety Organization (PSO),[241] Medicare's Quality Innovation Network—Quality Improvement Organization (QIN–QIO),[242] public health authorities (federal, state, or tribal), or similar entities). Prior to issuing the HTI–1 proposed rule, we had not had indications that healthcare facilities were experiencing uncertainty specific to allowing independent healthcare professionals to use the facility's systems in the course of clinical education or quality improvement activities in the facility—which could, from a health IT perspective, potentially make use of pre-production, production, or a mix of production and pre-production instance(s) of one or more system(s) or application(s).

Based on comments received in response to our proposing subparagraph (2)(v), we are concerned that codifying subparagraph (2)(v) with wording that explicitly references only furnishing, documenting, and billing for care in the facility would risk creating new uncertainty specific to independent professionals' use of a facility's health IT in the course of quality improvement and clinical education activities in the facility. By explicitly referencing clinical education and quality improvement activities conducted by or in a facility in addition to explicitly referencing furnishing, documenting, and accurately billing for care an independent healthcare professional furnishes to patients in a facility, we believe the finalized wording of subparagraph (v) is beneficial.

We reiterate, however, that the holding out, provision, or supply of health IT *for deployment by or for* other individual(s) or entity(ies) is not encompassed by any subparagraph of the implementation and use activities exclusion (paragraph (2)). (Again, we refer readers to the discussion of deployment versus use of health IT in section IV.B.1 of this preamble.)

c. Consulting and Legal Services Exclusion From the Offer Health IT Definition

In defining what it means to offer health information technology or offer health IT, we also considered whether it would be beneficial to explicitly establish an exclusion of certain management consulting services that play important roles in some providers' approaches to operational management of their practice, clinic, or facility. The bundled exclusions we proposed in paragraph (3) of the offer health IT definition address ''consulting and legal services,'' including:

- legal services furnished by attorneys that are not in-house counsel [243] of the provider (commonly referred to as ''outside counsel'');
- health IT expert consultants' services engaged to help a health IT customer/user (such as a health care provider) define their business needs and/or evaluate, select, negotiate for or oversee configuration, implementation, and/or operation of a health IT product that the consultant does not sell/resell, license/relicense, or otherwise supply to the customer; and
- clinician practice or other health care provider administrative or operational management consultant services where the clinician practice or other health care provider's administrative or operational management consulting firm effectively stands in the shoes of the provider in dealings with the health IT developer or commercial vendor, and manages the day-to-day operations and administrative duties for health IT and its use alongside other administrative and operational functions that would otherwise fall on the clinician practice or other health care provider's partners, owner(s), or staff.

We refer readers to the HTI–1 Proposed Rule (88 FR 23860 through 23864) for discussion and examples of services that would be excluded under each of subparagraphs (3)(i) through (3)(iii) of the proposed offer health IT definition.

Comments. Six commenters referenced this exclusion and expressed general support for the proposal. Some, however, recommended specific modifications or clarifications to the described activities. (Comments specific to each particular subparagraph of paragraph (3), the consulting and legal services exclusion, are summarized below.)

Response. We appreciate commenters' sharing their perspectives on this proposal through the public comment process. We have finalized the consulting and legal services exclusion (paragraph 3) with minor clarifications and revisions to each subparagraph, as discussed in detail below under sub-headings specific to each of these subparagraphs.

Legal Services Furnished by Outside Counsel

At subparagraph (3)(i) in the proposed offer health IT definition, we proposed to explicitly exclude legal services furnished by outside counsel (88 FR 23861). As we explained, this proposed exclusion would: codify how we already view, in the context of the definitions currently codified in § 171.102, legal services furnished by outside counsel in certain matters and remove an ambiguity that could, at least in theory, otherwise have unintended effects on how parties may in the future assess the best available options and mechanisms for efficient, cooperative discovery. The proposed exclusion for legal services furnished by outside counsel, like the proposed exclusion of health IT expert consulting services, would focus on the services provided and *not* on the type of organization providing them (88 FR 23861).

Comments. Several comments expressing support for the consulting and legal services exclusion (subparagraph (3)(i)) acknowledged the explicit exclusion of legal services furnished by outside counsel. No comments expressed opposition or concern and no comments recommended particular revisions or clarifications to the legal services description in subparagraph (3)(i).

[241] Patient Safety Organizations (PSOs) collect and analyze data voluntarily reported by healthcare providers to help improve patient safety and healthcare quality. PSOs provide feedback to healthcare providers aimed at promoting learning and preventing future patient safety events. Under the Patient Safety and Quality Improvement Act of 2005 (the Patient Safety Act), the Agency for Healthcare Research and Quality (AHRQ) certifies and lists PSOs. (*https://pso.ahrq.gov/,* retrieved Nov 24, 2023.)

[242] Administered by CMS, the Quality Improvement Organizations (QIO) Program is one of the largest federal programs dedicated to improving health quality for Medicare beneficiaries. The QIO Program's Quality Innovation Network-QIOs (QIN–QIOs) bring Medicare beneficiaries, providers, and communities together in data-driven initiatives that increase patient safety, make communities healthier, better coordinate post-hospital care, and improve clinical quality. By serving regions of two to six states each, QIN–QIOs are able to help best practices for better care spread more quickly, while still accommodating local conditions and cultural factors. (*https://www.cms.gov/medicare/quality/quality-improvement-organizations,* retrieved Nov 24, 2023.)

[243] As noted in the HTI–1 Proposed Rule (*see* 88 FR 23860 and 23861 (footnote 407)), in-house counsel would for purposes of the offer definition be considered ''employees'' of the provider. Furnishing use of the provider's health IT to in-house counsel would no more be an offer of that health IT than would be furnishing use of that same health IT to members of the provider's nursing or medical records staff.

Response. After considering comments received on the offer health IT definition and the consulting and legal services exclusion, we have finalized subparagraph (3)(i) of legal services furnished by outside counsel arrangements. We have, however, revised the text of subparagraph (3)(i) to remove unnecessary words and improve readability. These revisions are detailed below, under the *summary of finalized policy—consulting and legal services exclusion (paragraph (3))* heading.

Health IT Consultant Assistance With Selection, Implementation, and Use of Health IT

At subparagraph (3)(ii) in the proposed offer health information technology or offer health IT definition, we proposed to explicitly exclude the work of health IT expert consultants engaged to help a health IT customer/user (such as a health care provider, health plan, or HIN/HIE) do any or all of the following with respect to any health IT product that the consultant does not sell or resell, license or relicense, or otherwise supply to the customer under any arrangement on a commercial basis or otherwise: define their business needs; evaluate or select health IT product(s); negotiate for the purchase, lease, license, or other arrangement under which the health IT product(s) will be used; or oversee configuration, implementation, or operation of a health IT product(s) (88 FR 23862).

Comments. Comments regarding the arrangements described in subparagraph (ii) of the consulting and legal services exclusion (paragraph 3) were generally supportive. Several comments recommended clarification as to whether the description encompassed the full scope of informatics consulting practice. One of these comments requested additional detail as to specific domains and tasks within the practice of clinical informatics. Several comments requested clarification as to whether the exclusion applied to a consultant configuring, implementing, or operating health IT on the customer's behalf, or whether it was limited to a consultant overseeing such activities conducted by others.

Response. After consideration of comments received, we have finalized the description of health IT consultant assistance arrangements in subparagraph (3)(ii) with revised wording to provide additional clarity. Specifically, we have:

- clarified the wording of the subparagraph's heading to read ''health IT consultant assistance with selection, implementation, and use of health IT'' (in the HTI–1 Proposed Rule (88 FR 23915) the omission of the word ''with'' was a typographical error, which we believe made the heading less readable); and
- modified the wording of subparagraph (3)(ii)(C) from ''oversee'' to ''oversee or carry out'' so that the exclusion's wording explicitly includes carrying out as well as overseeing configuration, implementation, or operation of health IT products.

We believe the revised wording (''oversee or carry out'') in subparagraph (3)(ii)(C) provides certainty and clarity to clinical or biomedical informaticists and other consultants that they can take an active role in configuring, implementing, or operating health IT on the customer's behalf, as well as or instead of overseeing such activities conducted by others, without the consultant's activities meeting the definition of offer health IT.

As proposed and now finalized, subparagraph (3)(ii) is agnostic to what specific domains of expertise, or what specific knowledge, skills, or abilities, the consultant might apply to any of the activities described in subparagraphs (3)(ii)(A) through (C) with respect to any health IT product(s) that the consultant does not hold out or supply to the customer under any arrangement. We do not at this time believe it is necessary to limit the applicability of subparagraph (3)(ii) by adding to it a catalog of specific domains in which a health informaticist might be practicing when, or in order to be considered to be, engaged in activities described in any of subparagraphs (3)(ii)(A) through (C) under arrangements consistent with subparagraph (3)(ii).

A definition of ''health informatics'' that is often attributed to the National Library of Medicine [244] indicates that ''health informatics'' is ''the interdisciplinary study of the design, development, adoption and application of IT-based innovations in healthcare services delivery, management and planning.''[245] In our observation, there is today considerable heterogeneity in what health informaticists do, how they do it, and under what arrangements they engage with employers, customers, or clients. Therefore, we believe it would be more cumbersome than helpful to attempt to catalog all, and difficult to identify an appropriately representative sampling, of the tasks that a practitioner of health informatics might oversee or conduct without themselves selling, reselling, licensing, relicensing, or otherwise supplying the customer with health IT that includes one or more Health IT Modules certified under the Program. Such a catalog of tasks or domains of health informatics practice would risk rapidly becoming more limiting than we intend the exclusion to be. Therefore, we decline to do so. Instead, we emphasize that whether any activity or conduct in the course of practicing clinical, biomedical, public health, or any other variation of health informatics (or any other profession) is encompassed by the consulting and legal services exclusion under subparagraph (3)(ii) depends on whether the activity or conduct is consistent with subparagraph (3)(ii).

We reiterate that if an individual or entity who engages in an activity or arrangement encompassed by an exclusion from the offer health IT definition happens to otherwise be an § 171.102 actor, that individual or entity is an actor subject to the information blocking provision in section 3022 of the PHSA. If such actor engages in conduct that meets the definition of information blocking in § 171.103, that actor could be subject to enforcement action under the information blocking provision in section 3022 of the PHSA even if they engaged in the practice(s) meeting the information blocking definition in the course of an activity that would not, itself, meet the offer health IT definition.

For example, a clinical informaticist who is a doctor of medicine (MD) or osteopathy (DO) might provide consulting services consistent with subparagraph (3)(ii) of the offer health IT definition. The services in this example do not meet the offer health IT definition. Therefore, these services do not cause the informaticist to meet the health IT developer of certified health IT definition. But the clinical informaticist, as an MD or DO, meets the

[244] *See e.g.,* University of Michigan School of Information (*https://www.si.umich.edu/programs/master-health-informatics,* retrieved 10/25/2023); University of Pittsburgh School of Health and Rehabilitation Sciences blog post ''Why Health Informatics Is Its Own Discipline,'' Oct. 7, 2021 (*https://online.shrs.pitt.edu/blog/why-health-informatics-is-its-own-discipline/,* retrieved Oct. 25, 2023).

[245] The definition including this quote appeared in frequently asked questions (FAQs) for ''Health Services Research Information Central'' updated Apr. 23, 2014, on a web page of the National Library of Medicine's National Information Center on Health Services Research and Health Care Technology (NICHSR). The quote's attribution and citation on that web page read ''Procter, R. Dr. (Editor, Health Informatics Journal, Edinburgh, United Kingdom). Definition of health informatics [internet]. Message to: Virginia Van Horne (Content Manager, HSR Information Central, Bethesda, MD). 2009 Aug 16 [cited 2009 Sept 21]. [1 paragraph].'' (*https://wayback.archive-it.org/7189/20170515160548/https://www.nlm.nih.gov/hsrinfo/hsric_topic_definitions.html,* retrieved Oct. 25, 2023).

§ 171.102 definition of a health care provider. Thus, the physician in this example is a § 171.102 actor and, were this physician to be determined by OIG to have committed information blocking, the physician would be subject to appropriate disincentives consistent with section 3022(b)(2)(B) of the PHSA.

If, however, an individual or entity who practices ''health informatics'' is not otherwise a § 171.102 health care provider, health IT developer of certified health IT, or HIN/HIE, and would only meet the § 171.102 actor definition by offering health IT chooses to only engage in conduct that does not meet the offer health IT definition, then the individual or entity would not be considered an actor.

Comprehensive and Predominantly Non-Health IT Administrative or Operations Management Services

In subparagraph (3)(iii), we proposed to exclude from the offer health IT definition comprehensive clinician practice or other health care provider administrative or operational management consultant services where the administrative or operational management consulting firm effectively stands in the shoes of the provider in dealings with the health IT developer or commercial vendor, and manages the day-to-day operations and administrative duties for health IT and its use alongside a comprehensive array of other administrative and operational functions that would otherwise fall on the clinician practice or other health care provider's partners, owner(s), or staff (88 FR 23862).

Alone among the three proposed exclusions of consulting and legal services arrangements, the exclusion of clinician practice or other health care provider administrative or operational management consulting services would be likely to include arrangements where the health IT deployed by or for the health care provider is supplied to them by the consultant—for example, as part of a comprehensive (''turn key'') package of practice management or other provider administrative or operations management services. In proposing the exclusion from the offer health IT definition of the activities specified in subparagraph(3)(iii), we noted its implication for health care providers' accountability for acts or omissions of their consultants operating under the exception—particularly health care providers' administrative or operational management services consultants—that implicate the definition of information blocking in § 171.103 (88 FR 23862). We refer readers to the HTI–1 Proposed Rule for the rationale for the comprehensive and predominantly non-health IT management services exclusion and explanation of how it operates (88 FR 23862 through 23864). The explanation includes the key factors that differentiate excluded clinician practice or other health care provider administrative or operational management consultant services from IT managed service provider (MSP) services and arrangements (88 FR 23863).

The HTI–1 Proposed Rule preamble discussion may include one or more instances of a typographical error in how subparagraph (iii) of exclusion (3) is referenced. This typographical error results in citing the paragraph as (3)(c) instead of (3)(iii). These typographical errors in how the paragraph is cited in the HTI–1 Proposed Rule preamble have no bearing on the substance of the proposal.

We solicited comment on this proposal, including specifically whether:

- this exclusion is more beneficial than harmful or confusing to the public, including the regulated community (health care providers, other information blocking ''actors,'' and those who may be more likely to be considered a ''health IT developer of certified health IT'' in the absence of this exclusion); and
- different or additional criteria should factor into differentiating whether a particular arrangement is a practice/operational management services arrangement that happens to include health IT as one of many necessities to operate as a health care provider rather than an arrangement for the supply of health IT that happens to include additional services (88 FR 23864).

Comments. We received comments discussing or referencing the proposal to exclude arrangements for comprehensive and predominantly non-health IT clinician practice or other health care provider administrative or operations management services from four commenters. No comments expressed opposition to excluding these activities from the *offer health IT* definition. One comment expressed appreciation for the clarity the proposal provides. Two comments recommended revising the exclusion to encompass additional types of arrangements. One comment advocated changing the effect of an activity's exclusion so that an individual or entity that meets the actor definition through other activities (such as by participating as a developer in the Program) would not be considered an actor while engaging in the excluded activity. One commenter shared thoughts specifically in response to the HTI–1 Proposed Rule's prompt for comments on potential benefits and harms of the proposal and potential additional criteria for differentiating between a practice/operational management services arrangement that happens to include health IT and an arrangement for the supply of health IT that happens to include additional services.

Response. Upon consideration of comments received, we have finalized the exclusion of comprehensive and predominantly non-health IT clinician practice or other health care provider administrative or operations management services (subparagraph (iii) of paragraph (3)). We have revised the wording of subparagraph (3)(iii) to improve its readability and clarity. We summarize and respond to specific, detailed comments below.

Comments. A commenter advocated that we expand the exclusion to explicitly encompass reselling and hosting certified health IT under a particular vendor-specific model.

Response. A health care provider who wishes to stand in the shoes of another provider in dealings with the health IT developer or commercial vendor, in managing the day-to-day operations and administrative duties for the health IT, or both, as part of a comprehensive array of predominantly non-health IT administrative and operational functions, can do so without meeting the offer health IT definition. Such conduct would be excluded from the offer health IT definition to the extent the arrangement is consistent with the comprehensive and predominantly non-health IT management services exclusion (subparagraph (3)(iii)). We refer readers to the HTI–1 Proposed Rule explanation of the key factors that differentiate excluded clinician practice or other health care provider administrative or operational management consultant services from IT managed service provider (MSP) services and arrangements (88 FR 23863). Although this discussion of key factors includes an instance of the typographical error whereby subparagraph (3)(iii) is cited as ''(3)(c)'', the key factors discussed (88 FR 23863) apply to the arrangements described by subparagraph (3)(iii), as proposed and as now finalized.

We discuss in context of the health IT developer of certified health IT definition preamble below (section IV.B.2) additional concerns we would have for a potential policy under which health care providers who choose to sell

or resell certified health IT under additional types of arrangements would not be considered health IT developers of certified health IT. Because of these concerns (discussed in IV.B.2, below) we do not believe it would be appropriate to expand the exclusions from the offer health IT definition to include the vendor-specific resale model cited by this commenter.

Comments. Some comments cited potential risks, such as of anti-competitive effects or conflicts of interest arising as a result of exclusions potentially encouraging entities in the health sector or beyond to develop consulting operations to supply health IT to customers without the consulting operation being subject to the information blocking regulations, as compared to entities that offer similar services but also meet the health IT developer of certified health IT definition. A comment recommended we ensure sufficient protections are in place but did not suggest specific additional criteria or considerations for determining which arrangements are or should be encompassed by the comprehensive and predominantly non-health IT management services exclusion (subparagraph (3)(iii) and which should instead meet the offer health IT definition.

Response. We appreciate receiving a response to our request for comment on these points. Subparagraph (3)(iii) explicitly indicates that the consultant providing these services *acts as the agent of the health care provider or otherwise on behalf of the health care provider* in dealings with the health IT developer or vendor, day-to-day operations and administration of the health IT, or both. This means that for any (individual or entity) consultant's services to be consistent with subparagraph (3)(iii), the consultant cannot also be the developer of any included health IT items or services. For subparagraph (3)(iii) to apply, the consultant also must explicitly provide comprehensive and predominantly non-health IT administrative or operations management services. Thus, the exclusion cannot apply if the consultant is simply furnishing health IT managed service provider (MSP) services and arrangements or any bundle of exclusively or predominantly health IT items and services to the health care provider.

We believe excluded bundles of predominantly non-health IT services are distinguishable from health IT MSP services and arrangements and bundles of predominantly health IT items and services based on their characteristics. For an arrangement to be consistent with the comprehensive and predominantly non-health IT management services exclusion (subparagraph (3)(iii)), the bundle of business administrative and operational management services must demonstrate all of the differentiating factors described at 88 FR 23863:

- The individual or entity furnishing the administrative or operational management consulting services acts as the agent of the provider or otherwise on behalf of[246] the provider in dealings with the health IT developer(s) or commercial vendor(s) from which the health IT the client health care providers ultimately use is obtained;
- The administrative or operational management consulting services must be a package or bundle of services provided by the same individual or entity and under the same contract or other binding instrument, and the package or bundle of services must include a comprehensive array of business administration functions, operations management functions, or a combination of these functions that would otherwise be executed by the health care provider;[247]
- The bundle of business administrative and operational management consulting services must include multiple items and services that are not health information technology as defined in 42 U.S.C. 300jj(5); and
- The non-health IT services must represent *more than half* of each of—
  - the person hours per year the consultant (individual or entity) bills or otherwise applies to the services bundle (including cost allocations consistent with Generally Accepted Accounting Principles), and
  - the total cost to the client for, or billing from, the consultant per year (including pass-through costs for the health IT items and services).

These factors that differentiate comprehensive and predominantly non-health IT management services tailor subparagraph (3)(iii) so that it cannot be satisfied by a simple rebranding of health IT resale models or managed service provider (MSP) services or by tacking a few non-health IT service(s) onto a bundle of predominantly (half or more) health IT items and services. Thus, we believe subparagraph (3)(iii) as finalized is appropriately tailored to guard against misuse of the exclusion in the market today.

We recognize, however, the potential for the market to evolve in ways that would increase risk of unintended consequences or abuse of this exclusion from the offer health IT definition. Although we have finalized the exclusion of arrangements consistent with subparagraph (3)(iii) without limiting its applicability based on characteristics, features, or factors beyond those we proposed, we note that we may consider amending the offer health IT definition (including any or all of its exclusions) in future rulemaking in response to experience with the definition in practice or other appropriate factors such as changing market conditions.

Comments. A commenter that is a commercial developer of certified health IT advocated that entities otherwise meeting the health IT developer of certified health IT definition should be able to operate a consulting entity that would engage in conduct excluded from the offer health IT definition without the consulting entity's conduct in the course of those activities implicating the developer as an actor. The commenter suggested that a developer could otherwise be at a competitive disadvantage specific to these consulting services compared to consulting entities that engage only in activities excluded from the offer health IT definition and do not otherwise meet the health IT developer of certified health IT definition.

Response. Achieving the effect recommended by this comment would require altering the structure and nature of the health IT developer of certified health IT definition rather than the offer health IT definition. Such modification of the health IT developer of certified health IT definition would be beyond the scope of the wording update we proposed in the HTI–1 Proposed Rule (*see* 88 FR 23864 and 23915). Therefore, we interpret the comment primarily as a response to our Request for Information on whether we should consider proposing in future rulemaking any additional exclusions from the offer health IT definition (section IV.C.1 of the HTI–1 Proposed Rule, starting at 88 FR 23873). We summarize and respond to this specific comment here because we believe, in light of comments received from the health IT customer community (including one addressed immediately below), it may be helpful

[246] At 88 FR 23863, we used ''stands in the shoes of'' instead of ''on behalf of, to parallel the wording of the subparagraph as presented in the Proposed Rule. We have updated the statement of this factor here to match the wording of the finalized subparagraph (3)(iii).

[247] At 88 FR 23863, we referenced one example type of health care provider (clinician practice) and various roles individuals might have within health care provider organizations. We also used the more colloquial ''fall on'' than ''be executed by.'' We used that wording at 88 FR 23863 to parallel the wording of the subparagraph as presented in the Proposed Rule. We have updated the statement of this factor here to match the wording of the finalized subparagraph (3)(iii).

to both health IT developers of certified health IT and their customers for us to provide an overview of certain features and implications of the information blocking regulations within which the finalized subparagraph (3)(iii) of the offer health IT definition appears.

A baseline feature of information blocking regulations in place since the ONC Cures Act Final Rule (85 FR 25642) is that the health information network or health information exchange (HIN/HIE) definition is currently the only § 171.102 actor type definition that is functional. As we stated in the ONC Cures Act Final Rule, ''the individual or entity would be considered a HIN/HIE under the information blocking regulations for any practice they conducted while functioning as a HIN/HIE'' (85 FR 25802). In contrast, both the health care provider and health IT developer of certified health IT definitions in § 171.102 are categorical, in the sense that an individual or entity either meets one of these definitions or they do not. For example, an individual or entity that meets the health IT developer of certified health IT definition in any of its activities is considered to be a health IT developer of certified health IT for any of its practices that otherwise meet the information blocking definition in 45 CFR 171.103—regardless of whether health IT involved in a specific practice is certified. To read more about the health IT developer of certified health IT definition's scope, including applicability of the Cures Act's information blocking provision to a developer's non-certified health IT, please see the ONC Cures Act Final Rule preamble starting at 85 FR 25795.

We recognize that in a variety of circumstances developers and offerors of certified health IT have business lines or other entities that market various services also marketed by competitor entities that do not develop or offer any certified health IT. We also recognize, and would encourage customers to be aware, that any individual or entity that (1) offers health IT products or consulting services in a way that satisfies the exclusion, (2) does not engage in any other conduct within the offer health IT definition, and (3) does not otherwise meet the § 171.102 actor definition would not be subject to the information blocking regulations.

We believe any perceived competitive disadvantage a ''health IT developer of certified health IT'' may experience as a result of meeting the definition in § 171.102 is offset by customers' potential preferences to receive services from consultants who are § 171.102 actors. For example, in choosing among otherwise competitive bids from a non-actor and a health IT developer of certified health IT to serve in a specific consulting role, a customer might weigh as favorable to a vendor or consultant that is a § 171.102 actor the fact that the actor could be subject to enforcement action under section 3022 of the PHSA if (except as required by law or covered by an exception) the actor engages in conduct they know or should know is likely to interfere with the access, exchange, or use of EHI. We also refer readers to the discussion in the ONC Cures Act Final Rule (85 FR 25795 through 25796) of a related concern about the potential impact of the Cures Act's information blocking provision (42 U.S.C. 300jj–52) on health IT developers' decisions to participate in the Program.

Comments. A commenter expressed concern about the risk of customers being uncertain as to which entities offering consulting services excluded from the *offer health IT* definition are subject to information blocking regulations and which are not, and about other entities' ability to support needs for data sharing within the healthcare space.

Response. We appreciate the commenter sharing this concern. We recognize that whether a consultant has the skills and expertise to deliver what the customer needs and expects for data sharing and other activities involving or relying on data, is a foundational question. Answering it, we believe, will continue to be something customers do by assessing prospective consultants' qualifications against their specific needs and priorities. Knowing that a consultant is an actor subject to information blocking regulations is a useful piece of information for customers to have, but a consultant meeting the § 171.102 actor definition does not guarantee the consultant has the level of particular knowledge, skills, abilities, or other capacity that the customer wants or needs from a consultant or other vendor.

We also recognize that customers who prefer to obtain services that are excluded from the definition of offer health IT from an entity that is subject to the information blocking regulations may need to engage in fact-finding to ascertain the status of entities that provide these services. We note that it may be somewhat easier to identify the actor status of a consultant where the consultant is also a developer participating in the Program, or a health care provider, than where they are not. This is because, for example, both individual and organizational health care providers must typically be licensed in jurisdiction(s) where they furnish healthcare. Most health care providers in the United States will also have a National Provider Identifier (NPI). Online directories of licensed health care providers are available from or for U.S. states, and CMS supports an online search utility for the NPI registry (available to the public free of charge at *https://npiregistry.cms.hhs.gov/search*). Similarly, a search of ONC's Certified Health IT Products List (CHPL) (*https://chpl.healthit.gov/#/search*) will indicate whether an entity has listed under its name one or more Health IT Module(s) certified under the Program. By contrast, an entity that only resells Health IT Module(s) without having responsibility for the certification status of any such Health IT Module(s) will not be listed on the CHPL. It is also important to remember that entities' choices to engage in different lines of business under different names may mean that the name under which consulting services are furnished differs from the name(s) under which: a developer of certified health IT is associated with any CHPL-listed product(s); or an individual or entity that meets the § 171.102 health care provider definition may be listed in any registry, listing, or database of individual and organizational health care providers. Therefore, a customer may need to refer to additional sources of information, including those provided by the prospective consultant, and may want to consider addressing the consultant's § 171.102 actor status in the process of selecting the consultant or contracting with the consultant for their services (such as through representations and warranties).

One expectation we have for the improved clarity provided by the offer health IT definition is that it will help customers to differentiate between consultants who clearly are § 171.102 actors and those who might not be actors. With this clarity, we believe customers will be in a better position to assess what additional information, representations, or warranties they will require from a consultant before making or finalizing a decision to engage the consultant.

Summary of finalized policy—consulting and legal services exclusion (paragraph (3)): After considering comments received, we have finalized the substance of the consulting and legal services exclusion. The finalized text of paragraph (3) includes minor revisions to subparagraphs (i), (ii), and (iii) to improve clarity, address a typographical error, and improve readability (as discussed above):

- Revised the second sentence of subparagraph (i) to remove unnecessary

words, increase precision, and improve readability, as follows:

○ Removed unnecessary words from ''if or when facilitating limited access or use of the client's health IT or the EHI within it,'' resulting in the revised phrase reading ''when facilitating limited access or use of the client's health IT.''

○ Revised the phrase ''to independent expert witnesses engaged by counsel'' for readability and precision to read, as revised: ''by independent expert witnesses engaged by the outside counsel.''

○ Revised the final phrase of the sentence from ''as necessary or appropriate to legal discovery'' to ''as appropriate to legal discovery.''

• Revised the wording of the subparagraph (3)(ii) heading to read ''health IT consultant assistance with selection, implementation, and use of health IT,'' correcting the typographical error that had omitted ''with'' from the text as published in the HTI–1 Proposed Rule (88 FR 23915).

• Revised the wording of subparagraph (3)(ii) to improve readability by removing unnecessary reference to services being potentially provided by an individual or a firm, and to ''expert.'' As discussed in response to comments, subparagraph (3)(ii) applies to the activities it describes. Application of subparagraph (3)(ii) does not depend on the consultant having or applying specific type(s) or level(s) of expertise, knowledge, or skills in furnishing expert services to help the customer do (or do for the customer) the activities described in subparagraph (3)(ii)(A) through (C). The revision is from the HTI–1 Proposed Rule's wording ''. . . provided by an individual or firm when furnishing expert advice and consulting services to a health IT customer or user that help the customer or user, or on the customer's behalf, do . . .'' to ''. . . advice and consulting services furnished to a health IT customer or user to do (or on behalf of a customer or user does).''

• Revised wording of subparagraph (3)(ii)(A) to improve readability, from ''define the customer or user business needs; evaluate or select health IT product(s),'' as presented in the HTI–1 Proposed Rule, to the finalized wording of: ''define the business needs of the customer or user or evaluate health IT product(s) against such business needs, or both.''

• In response to public comments, modified the wording of subparagraph (3)(ii)(C) from ''oversee'' to ''oversee or carry out'' so that, on its face, the wording provides immediate and explicit clarity that the exclusion encompasses carrying out as well as overseeing configuration, implementation, or operation of health IT products.

• To improve readability of subparagraph (3)(iii), we have revised its wording in the following ways:

○ Split the paragraph into two sentences instead of one. The second sentence, as finalized, opens with ''To be consistent with this subparagraph, such services must be furnished'' to connect this to the preceding paragraph and ensure it remains clear that services are not consistent with subparagraph (3)(iii) unless they are furnished as part of a comprehensive array of predominantly non-health IT services (as discussed above, in responses to comments).

○ From the first revised sentence, removed unnecessary reference to clinician practice and other unnecessary words to improve readability. This change is from ''provided by an individual or entity when furnishing a clinician practice or other health care provider administrative or operational management consultant services where the management consultant acts as the agent of the provider or otherwise'' to the finalized wording: ''when an individual or entity furnishes a health care provider with administrative or operational management consultant services and the management consultant acts as the agent of the provider or otherwise.''

○ Replaced in the first finalized sentence of the subparagraph the phrase ''stands in the shoes of the provider'' with less colloquial phrase ''acts on behalf of the provider.''

○ Revised description of dealings with health IT developers and vendors to strike unnecessary adjective (''commercial'') and improve facial clarity that the dealings could be with one or more developers or vendors. This change in text is from ''in dealings with the health IT developer or commercial vendor'' to ''in dealings with one or more health IT developer(s) or vendor(s).''

○ At the end of what is, as finalized, the first sentence of the subparagraph, we replaced ''and/or in managing the day-to-day operations and administrative duties for the health IT,'' with ''or managing the day-to-day operations and administrative duties for the health IT, or both.''

○ Replaced in the second clause of the finalized second sentence of the subparagraph the phrase ''fall on'' with less colloquial phrase ''be executed by'' and struck unnecessary reference to a specific type of health care provider entity, and unnecessary reference to different roles within provider organizations. The affected portion of the subparagraph as presented in the HTI–1 Proposed Rule read: ''as part of a comprehensive array of predominantly non-health IT administrative and operational functions that would otherwise fall on the clinician practice or other health care provider's partners, owner(s), or staff.'' As a result of the revisions described here, the second sentence of the subparagraph reads as a whole: ''To be consistent with this subparagraph, such services must be furnished as part of a comprehensive array of predominantly non-health IT administrative and operational functions that would otherwise be executed by the health care provider.''

We reiterate here, because we believe it is worth amplifying, a point we noted in the HTI–1 Proposed Rule (88 FR 23862) specific to the comprehensive and predominantly non-health IT management services arrangements (subparagraph (3)(iii)). That point is its implication for health care providers' accountability for acts or omissions of health care providers' administrative or operational management services consultants operating under the exception that implicate the definition of information blocking in § 171.103: where an administrative or operations management services firm would not be considered to offer health IT for which they contract on behalf of one or more practices (or facilities or sites of care) *because they are acting as the provider's agent or otherwise standing in the shoes of the provider* in selecting and contracting for a variety of services and supplies—including, but not limited to, the health IT that includes at least one certified Health IT Module—we would view the provider as retaining accountability for any information blocking conduct that the management services company perpetrates while thus acting on the provider's behalf. We recognize this may have implications for how providers may wish to structure administrative and operational services contracts in the future, potentially including a provider seeking representations and warranties giving the provider assurance that the administrative or operations management services company will not, without the provider's direction, knowledge, or approval, engage in any practice not required by law or covered by an information blocking exception that is likely to interfere with access, exchange, or use of EHI and could be unreasonable. However, subparagraph (3)(iii) of the consulting and legal services exclusion from the offer health

IT definition is not intended to have the effect of regulating or otherwise interfering with contracting relationships between health care providers and entities that do, or might, furnish them with practice, facility, location, or site management consulting and operational services packages.

We also remind, again, any individual or entity otherwise meeting the § 171.102 actor definition that engaging in activities that are explicitly excluded from the offer health IT definition under paragraph (1), (2), or (3), will *not* change the fact that they are a § 171.102 actor. Where an individual or entity meets the actor definition, that actor's having also engaged in any one or more activities that satisfies an exclusion from the offer health IT definition does not mean the individual or entity is no longer an actor. The fact that an actor may engage in some conduct that is consistent with an explicit exclusion from the offer health IT definition does not mean that conduct on the actor's part is not subject to the information blocking definition. The fact that particular conduct of an individual or entity meets any exclusion from the offer health IT definition only means that specific conduct does not meet the definition of offer health IT.

2. Health IT Developer of Certified Health IT: Self-Developer Health Care Providers

For reasons discussed in the ONC Cures Act Final Rule (85 FR 25799 through 25800), health care providers who self-develop certified health IT ''for their own use'' were excluded from the health IT developer of certified health IT definition. However, under that definition, if a health care provider responsible for the certification status of any Health IT Module(s) were to offer *or supply* those Health IT Module(s) on any terms to other entities for those entities' use in their own independent operations, that would be inconsistent with the concept of the health care provider self-developing health IT ''for its own use.'' As we explained in the ONC Cures Act Final Rule (at 85 FR 25799), we use the term ''self-developer'' in this context as the term has been used in the ONC Health IT Certification Program (Program) and as described in section VII.D.7 of the Cures Act Proposed Rule (at 84 FR 7507).

In the HTI–1 Proposed Rule, informed by our proposal to define ''offer health IT,'' we proposed to modify the health IT developer of certified health IT definition in § 171.102. To ensure it would be immediately clear from the face of the regulations' text that we had put all health care providers that engage in activities consistent with the exclusions in paragraphs (1) through (3) of the offer health IT definition on the same footing regardless of who develops the health IT involved in these activities, we proposed to replace in the health IT developer of certified health IT definition the phrase ''other than a health care provider that self-develops health IT for its own use'' with the phrase ''other than a health care provider that self-develops health IT not offered to others'' (*See* 88 FR 23864).

Comments. A majority of comments specific to this proposal supported the proposal. Several comments stated that self-developer health care providers should not be considered health IT developers of certified health IT. Several comments stated that self-developer health care providers who offer health IT should be included health IT developers of certified health IT definition alongside other individuals and entities that offer certified health IT.

Response. We appreciate all comments received. Having considered the comments, we have finalized our proposal to align the self-developer health care provider exclusion from the health IT developer of certified health IT definition with our finalized definition of ''offer health IT.'' Stated another way, health care providers who self-develop certified health IT that is not offered to others are excluded from the health IT developer of certified health IT definition unless they ''offer health IT'' as now defined in § 171.102. We have made one revision to the wording of the finalized updated text of the definition for readability, specifically from ''other than a health care provider that self-develops health IT not offered to others'' to ''other than a health care provider that self-develops health IT that is not offered to others.'' We summarize and respond to additional comments related to the health IT developer of certified health IT definition below.

Comments. We received several comments advocating that we exclude all providers who host EHRs for other providers (sometimes characterizing it as extending the host provider's EHR) from the health IT developer of certified health IT definition. These comments have been discussed in section IV.B.1 because several of them discussed this recommendation as an extension, clarification, or addition to the proposed exclusions from the offer health IT definition. Some commenters, however, connected the suggestion to the health IT developer of certified health IT definition. Commenters' rationales for excluding from the health IT developer of certified health IT definition health care providers who ''extend their EHRs'' or otherwise provide certified health IT to other providers included: health care providers are already actors under the information blocking regulations (§ 171.102); recipient providers would be unable to afford interoperable health IT obtained from other sources; and the developer should be held accountable for design defects in health IT. Several other commenters, representing the health care provider as well as the ONC Health IT Certification Program-participating developer perspectives, explicitly supported our proposal to have all entities that offer health IT (as we have defined such action) continue to meet the definition of health IT developers of certified health IT regardless of whether such health IT was self-developed or obtained from a third-party developer.

Response. Whether done by a health care provider or anyone else, hosting EHR systems, otherwise providing or supplying health IT items and services, or holding out any certified health IT to health care providers generally meets the offer health IT definition. Such actions are excluded from the offer health IT definition only when and to the extent it is consistent with subparagraph (3)(iii) of the offer health IT definition. Any individual or entity, regardless of whether they also meet the § 171.102 definition of health care provider, who engage in conduct meeting the offer health IT definition meet the health IT developer of certified health IT definition on the basis of that conduct.

We had not proposed, and we have not made, revisions to ''carve out'' health care providers who offer health IT from the health IT developer of certified health IT definition. We included in section IV.C.1 of the HTI–1 Proposed Rule (88 FR 23873) a request for information on additional exclusions from the offer health IT definition but did not propose to exclude supply of health IT for deployment by or for others from the offer health IT definition based on the supplier being a health care provider. Further, as noted above, we received comments supporting the health IT developer of certified health IT approach we proposed. Therefore, any further exclusions from the offer health IT definition are deferred for future consideration.

Regarding concerns about design flaws in the software created by the developer of certified health IT, as a § 171.102 actor, the developer would be subject to information blocking penalties for software design flaws to the extent such flaws constitute information blocking. As we did in the ONC Cures Act Final Rule (*see* 85 FR

25798 through 25799), we again refer commenters concerned about holding offerors that do not develop health IT accountable for the conduct of the developer (or others) to section 3022(a)(6) of the PHSA, which states that the term ''information blocking,'' with respect to an individual or entity, shall not include an act or practice other than an act or practice committed by such individual or entity. Where the individual or entity that develops health IT is different from the individual or entity that offers certified health IT, each such individual or entity is only liable for the acts and practices that it commits.

In the ONC Cures Act Final Rule (85 FR 25798–25800), we explained that any that any individual or entity that develops health IT, except for health care providers that self-developed certified health IT for their own use, meet the definition of health IT developer of certified health IT while they have one or more Health IT Modules certified under the ONC Health IT Certification Program. We also explained that individuals or entities meet the health IT developer of certified health IT definition if they offer certified health IT. This remains true with the conclusion of this rulemaking. Under the policies finalized in this rule, any individual or entity, including a self-developer health care provider or any other health care provider, that offers health IT (as defined in § 171.102) meets the definition of health IT developer of certified health IT.

Comments. A commenter requested that we clarify what the term health care provider means as used within the health IT developer of certified health IT definition.

Response. The term health care provider is defined for purposes of the information blocking regulations in 45 CFR 171.102. To help interested parties better understand the definition, we make information blocking resources available through our website, *HealthIT.gov*. These resources include a fact sheet titled ''Health Care Provider Definition'' that provides, in a single document, a copy of the full text of the health care provider statutory definition (PHSA section 3000) cited in § 171.102 and the text of statutory cross-references within the PHSA section 3000 definition of health care provider.[248]

Summary of finalized policy—health IT developer of certified health IT definition: After consideration of comments received, we have finalized the revision to the definition substantively as proposed. We have made a non-substantive change to the wording of the finalized revised definition of health IT developer of certified health IT in comparison to the HTI–1 Proposed Rule; specifically, in the clause excluding self-developer health care providers to the extent their self-developed health IT is not offered to others. In the HTI–1 Proposed Rule, that clause read: ''other than a health care provider that self-develops health IT not offered to others.'' As finalized, we added ''that is'' immediately before ''not offered to others'' to improve readability of the finalized text.

We emphasize that any individual or entity that chooses to offer health IT (as defined in § 171.102) will meet the finalized revised § 171.102 health IT developer of certified health IT definition regardless of who developed the certified health IT that the individual or entity offers to others, and regardless of whether the health IT is offered at or below cost, market rate, or other benchmark price for the same or similar health IT items or services. This includes individuals and entities that offer health IT while also meeting the definition of health care provider, as both terms are defined in § 171.102, regardless of whether such individuals or entities also self-develop any health IT (certified or otherwise) deployed only within their own organization or operations. Regarding health care providers who might engage in activities consistent with one or more exclusion(s) from the offer health IT definition without also engaging in activities or arrangements that meet the offer health IT definition, we note that all such health care providers will stand on the same footing regardless of whether they also self-develop health IT that is not offered to others.

3. Information Blocking Definition

As finalized in the ONC Cures Act Final Rule (85 FR 25642) and the Cures Act Interim Final Rule (85 FR 70085), the information blocking definition (§ 171.103) and the Content and Manner Exception (§ 171.301(a)) were limited for a period of time to a subset of EHI that was narrower than the EHI definition finalized in the ONC Cures Act Final Rule in § 171.102. The narrower subset included only the EHI identified by the data elements represented in the United States Core Data for Interoperability (USCDI) for the first 18 months (until May 2, 2022) after the applicability date for 45 CFR part 171 (November 2, 2020) (85 FR 25792). The Cures Act Interim Final Rule extended the applicability date of 45 CFR part 171 to April 5, 2021 (85 FR 70069). This extended the end of the first 18 months of applicability of 45 CFR part 171 until October 6, 2022 (85 FR 70069).

Because October 6, 2022, has passed, we proposed to revise the information blocking definition (§ 171.103) to remove the paragraph designating the period of time for which the information blocking definition was limited to EHI that consists of the data elements represented in the USCDI (88 FR 23864 and 88 FR 23916). This time period designation was codified in § 171.103(b), as finalized in 2020, and removal of this paragraph allows for redesignation of remaining paragraphs within § 171.103 as shown in the HTI–1 Proposed Rule (at 88 FR 23916).

Similarly, because we included the same date in two paragraphs of the Content and Manner Exception (§ 171.301(a)(1) and (2)), we proposed to revise § 171.301 to remove the existing § 171.301(a)(1) and (2) as no longer necessary (88 FR 23864 through 23865 and 88 FR 23916). The proposed revised version of § 171.301 refers simply to EHI. We further proposed to renumber several of the existing provisions in § 171.301 accordingly and rename the exception as the ''Manner'' exception.

Comments. Comments received on our proposal to remove obsolete text from the information blocking definition (§ 171.103) generally supported this proposal. Comments noted that the information blocking definition prevents practices that hinder access to EHI, supports improved access to EHI for patients and health care providers, facilitates interoperability and encourages actors to prioritize interoperability, and promotes transparency and accountability in the healthcare ecosystem. A commenter stated the information blocking regulations are beneficial to underserved, underrepresented patient populations and the health care providers who serve them. This commenter advocated for collaborative efforts among various parties interested in information sharing, characterizing such efforts as crucial to ensuring that the information blocking regulations effectively support the goal of equitable access to high-quality healthcare for underserved populations. No commenters opposed this proposal. However, some commenters did note general concerns about the importance of balancing information sharing goals with patient privacy and data security.

Response. We appreciate commenters' feedback and have finalized the update to the information blocking definition

[248] *Health Care Provider Definition and Cross-Reference Table,* available at: *https://www.healthit.gov/sites/default/files/page2/2020-08/Health_Care_Provider_Definitions_v3.pdf* (Retrieved Jun 28, 2023.)

(§ 171.103), as proposed. The topic of balancing information sharing goals with patient privacy and security of patients' health information is out of scope for this proposal, but it was also raised in comments on other proposals. We discuss, at the beginning of section IV of this final rule (above), comments raising general concerns about a perceived conflict between the goals of maximizing information sharing and appropriately protecting patients' privacy interests. We agree that information sharing can help improve many aspects of health care for all patients throughout the United States. We look forward to continued engagement with actors, patients, and others who support information sharing that contributes to improved care and health for individuals, families, and communities.

Comments. We received one comment that expressed concern about requirements to share mental health notes that were historically blocked from the rest of the record. The comment identified as an issue having all health care providers being able to access all mental health notes when they may not be immediately relevant to the patient at the point of care.

Response. In the HTI–1 Proposed Rule, we did not propose to modify existing exclusions from the § 171.102 definition of EHI for purposes of the information blocking regulations. Psychotherapy notes as defined in the HIPAA Privacy Rule at 45 CFR 164.501 are explicitly excluded from the 45 CFR 171.102 definition of electronic health information (EHI) for purposes of the information blocking regulations. We have posted on our website information resources to help actors understand the EHI definition and consider whether particular data is EHI for purposes of 45 CFR part 171 (see *https://www.healthit.gov/topic/information-blocking*).

We note, and remind actors, that persons who engage in inappropriate uses and disclosures of individuals' health information may be violating other laws, including, but not limited to, the HIPAA Privacy Rule, 42 CFR part 2, or state or tribal laws. Persons using or disclosing individuals' health information in violation of one or more such law(s) would be subject to the consequences for violating those laws.

Comments. A commenter advocated for further revision of the information blocking definition to specify who must be affected by a practice that is otherwise consistent with the definition in order for the practice to be considered information blocking. The comment suggested as an example adding to paragraph (2)(b) of § 171.103 an explicit statement that the action can affect EHI access by physicians as well as by patients.

Response. We did not propose such a revision in § 171.103 and decline to adopt it here. We reiterate that an actor's practice meeting the information blocking definition is considered to be information blocking regardless of whether it affects access, exchange, or use of EHI by a patient, health care provider, health plan, or other person (as defined in § 171.102) that seeks access, exchange, or use of EHI for any permissible purpose (as defined in § 171.102).

Comments. A commenter requested we retain ''Content and Manner'' as the title of the exception codified in § 171.301 and retain wording specific to limiting the content fulfilled for a request to recognize the potential for an actor to be able to fulfill access, exchange, or use of some, but not all, EHI in a particular requested manner. Another commenter characterized our proposal to remove reference to the period of time and limited EHI in § 171.301 as removing a safe harbor protection for limiting the content of a response. This commenter stated that an actor may be able to satisfy § 171.301 for only some of the EHI requested. This commenter also stated that the proposed revision to § 171.301 creates uncertainty as to whether the Manner Exception can be satisfied where an actor can fulfill access, exchange, or use of only some EHI in the manner requested or in an alternative manner consistent with § 171.301.

Response. We decline to retain the prior title of the Manner Exception. We note that the ''content'' condition we have removed from regulatory text through this final rule has been moot since October 6, 2022, and we did not propose to re-instate it in the HTI–1 Proposed Rule. In section IV.A, we discuss an example situation where multiple exceptions could be used to provide an actor with certainty that their practices in responding to a request for access, exchange, or use of EHI will not be considered to be information blocking. Similarly, an actor might be able to satisfy the Manner Exception for only some of the EHI requested in a particular situation. In such instances, an actor may want to consider whether another exception is applicable to any other requested EHI.

Summary of finalized policy: After consideration of comments, we have finalized the proposed removal of references to the USCDI, as well as the time period designation, from §§ 171.103 and 171.301. We have also finalized corresponding redesignations of paragraphs, as proposed.

C. Exceptions

1. Infeasibility

a. Infeasibility Exception—Uncontrollable Events Condition

We established the Infeasibility Exception in the ONC Cures Act Final Rule (85 FR 25865 through 25870, 85 FR 25958; 45 CFR 171.204). The Infeasibility Exception includes conditions under which an actor's practice of not fulfilling requests for EHI access, exchange, or use due to infeasibility will not be considered information blocking. One of the conditions of the Infeasibility Exception, finalized by the ONC Cures Act Final Rule in § 171.204(a)(1), is the *uncontrollable events* condition. Under the *uncontrollable events* condition, an actor's practice of not fulfilling a request to access, exchange, or use EHI that is infeasible for the actor to fulfill as a result of events beyond the actor's control (listed in § 171.204(a)(1)) will not be considered information blocking provided such practice also meets the condition in § 171.204(b). In the HTI–1 Proposed Rule, we proposed to revise § 171.204(a)(1) to add clarity to the *uncontrollable events* condition (88 FR 23865).

In the HTI–1 Proposed Rule (88 FR 23865), we reminded readers that under the *uncontrollable events* condition, an actor's practice of not fulfilling a request to access, exchange, or use EHI as a result of a natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority (§ 171.204(a)(1); 85 FR 25874) will not be considered information blocking provided such practice also meets the condition in § 171.204(b). We explained that the fact that an uncontrollable event specified in § 171.204(a)(1) occurred is not a sufficient basis alone for an actor to meet the *uncontrollable events* condition of the Infeasibility Exception. Rather, the use of the words ''due to'' in the *uncontrollable events* condition (paragraph (a)(1) of § 171.204) was intended to convey, consistent with the Cures Act Proposed Rule, that the actor must demonstrate a causal connection between the actor's inability to fulfill access, exchange, or use of EHI and the uncontrollable event. As we illustrated in the HTI–1 Proposed Rule (88 FR 23865), a public health emergency is listed as an uncontrollable event under § 171.204(a)(1). If the federal

government or a state government were to declare a public health emergency, the mere fact of that declaration would not suffice for an actor to meet the condition. To meet the condition, the actor would need to demonstrate that the public health emergency actually caused the actor to be unable to provide access, exchange, or use of EHI for the facts and circumstances in question. The emergency need not be the *only* cause of a particular incapacity, but the actor needs to demonstrate that the public health emergency did in fact negatively impact the feasibility of that actor fulfilling access, exchange, or use in the specific circumstances where the actor is claiming infeasibility.

While the *uncontrollable events* condition (§ 171.204(a)(1)) has always required causal connection between the actor's inability to fulfill the request and the natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority, we proposed to revise the condition by replacing the words ''due to'' with ''because of'' (88 FR 23865). We welcomed comments on this proposal, including whether alternative or additional refinements to the wording of the condition may make the causal connection requirement more immediately obvious from the face of the text in § 171.204(a)(1) (88 FR 23865).

Comments. In general, commenters expressed support for clarifying the *uncontrollable events* condition by stating that the actor's inability to fulfill the request is ''because of'' one of the events listed. Commenters noted that the extra clarity adds certainty for actors and demonstrates a clear causation requirement. Some commenters supported the change but noted that ''due to'' and ''because of'' mean the same thing and the change would not have any resulting implications for actors. Another commenter agreed with the intent but did not believe that the change of wording from ''due to'' to ''because of'' provides any more clarity. This commenter asked what change in impact or obligation stemmed from the change, recommending a clear statement of the causal connection between the uncontrollable event and the impact on the actor. A commenter requested clarification as to how ONC believes the ''due to'' and ''because of'' differ in terms of implications for—or obligations now expected of— actors. A commenter recommended we make a clear statement about the causal connection between the uncontrollable event and the impact on the actor but did not suggest where, or in what words, we should consider making the statement.

Response. We appreciate the support expressed by many commenters and as discussed more fully below; we have finalized a revision of § 171.204(a)(1) with modifications to the regulation text to provide additional clarity. As noted in the preamble to the HTI–1 Proposed Rule, the words ''due to'' convey that the actor must demonstrate a causal connection between not providing access, exchange, or use of EHI and the uncontrollable event (88 FR 23865). We proposed to change the term to ''because of'' to provide further clarity. The revised language was not intended to change the substance of the condition, its implications, or what would be required of an actor for purposes of meeting the condition.

We did not receive comments suggesting specific additional refinements to the condition's text, or recommending specific alternative wording for ''because of,'' to make the causal connection requirement more immediately obvious from the text of the *uncontrollable events* condition (§ 171.204(a)(1)). However, having considered commenters' feedback, adding text to the finalized revision to § 171.204 will help actors and other interested persons immediately recognize that a causal connection is required between the uncontrollable event and the infeasibility of the actor's fulfilling a request for EHI access, exchange, or use. We have, therefore, finalized the proposed revision to § 171.204(a)(1) with the additional clause ''that in fact negatively impacts the actor's ability to fulfill the request'' at the end of the condition. This additional text is consistent with our statement in the preamble of the HTI–1 Proposed Rule that ''the actor must demonstrate a causal connection between not providing access, exchange, or use of EHI and the uncontrollable event'' (88 FR 23865). We intend for this additional clause to reinforce clarity that the actor must demonstrate an actual negative impact of the uncontrollable event on their ability to fulfill the requested access, exchange, or use of EHI for the *uncontrollable events* condition to be met. To reiterate, the finalized change to the wording of § 171.204 is only intended to improve clarity for actors and other interested parties in comparison to the previous wording rather than to make any change to the substance of the policy that it codifies.

Comments. A commenter recommended that ONC expand the definitions within the *uncontrollable events* condition to include impediments of data access, exchange, or use because of any disaster or emergency declared by an authorized governmental entity, noting that in addition to declared emergencies, this would include response and recovery periods associated with natural disasters that impacted the availability of providers' information systems or data.

Response. We did not propose to change the list of uncontrollable events or further define them, nor do we believe it is necessary to revise the references to disasters and emergencies to refer to a governmental declaration of that status or recovery or restoration periods. The events listed in the condition include acts of ''military, civil, or regulatory authority'' as well as natural or human-made disasters and other types of events or emergencies that might prompt a governmental authority to issue a declaration of disaster or emergency. However, consistent with the scope of the proposal, we emphasize that a key component of this condition is that an actor must demonstrate that a request for access, exchange, or use is infeasible because the uncontrollable event negatively impacts the actor's ability to fulfill the request.

Comment. A commenter recommended that we consider reporting flexibilities for this condition similar to those that other HHS programs put in place for declared emergencies, citing waivers issued in the context of public health emergencies for requirements of programs administered by the Centers for Medicare & Medicaid Services (CMS).

Response. We did not propose to create such a reporting system as suggested by the commenter nor is there currently a requirement for actors to routinely report to ONC which of their practices they believe they have structured to satisfy any information blocking exception(s). We thank the commenter for the suggestion.

Comment. A commenter noted the importance of minimizing administrative burden on health care providers, and specifically physicians delivering care in context of an emergency or disaster.

Response. The commenter did not specify the types of administrative burden it was concerned about, but we suspect the concern is related to documenting compliance with the conditions of the Infeasibility Exception, including § 171.204(b). We emphasize that the *uncontrollable events* condition does not require specific documentation to be satisfied, and we did not propose specific documentation requirements for an

actor to satisfy the *uncontrollable events* condition in paragraph (a)(2). We also did not propose to change the requirements of the *responding to requests* condition (§ 171.204(b)). Both conditions remain the same in this regard. The *responding to requests* condition (§ 171.204(b)) does not include specific documentation requirements, but does require the actor to provide the requestor, in writing, the reason(s) why the request is infeasible within ten business days of receipt of the request. An actor has flexibility in demonstrating how they met the *uncontrollable events* and the *responding to requests* conditions of the Infeasibility Exception.

Comments. A commenter asked about an actor's burden of proof with respect to this exception.

Response. As noted in the response to the comment above, we did not propose in the HTI–1 Proposed Rule specific documentation requirements for an actor to satisfy the *uncontrollable events* condition or the *responding to requests* condition of the Infeasibility Exception. In the ONC Cures Act Final Rule (85 FR 25821), we stated that an actor seeking an exception needs to meet all relevant conditions of the exception at all relevant times. For the Infeasibility Exception, an actor seeking to satisfy the exception would need to demonstrate it satisfied one of the conditions in § 171.204(a) and the condition in § 171.204(b). Further, as we noted in the HTI–1 Proposed Rule, the actor would need to produce evidence and ultimately prove that complying with the request for access, exchange, or use of EHI in the manner requested would have imposed a clearly unreasonable burden on the actor under the circumstances (88 FR 23865, citing 85 FR 25866). We also refer readers to the ONC Cures Act Final Rule (85 FR 25819) for additional discussion on establishing that an actor's practice(s) meet the conditions of an exception.

Comments. Some comments we received discussed the *responding to requests* condition (§ 171.204(b)) as new or pending or in other ways that suggested some commenters may not have reviewed the full text of the existing Infeasibility Exception (§ 171.204) prior to commenting on the HTI–1 Proposed Rule.

Response. We thank all commenters for their feedback. We appreciate the opportunity to remind actors, and any persons who may seek EHI access from actors, where and how to find all the information blocking exceptions, and to discuss a bit further here the Infeasibility Exception's structure and its requirements.

First, we note that actors seeking to satisfy an exception, or other persons interested in when an exception applies, should review the exception's full regulatory text (found in the exception's section of 45 CFR part 171). In addition, the requirements and conditions of each exception set forth in subparts B, C, and D of 45 CFR part 171 should be read in context with the subpart's ''availability and effect of exceptions'' section (45 CFR 171.200, 45 CFR 171.300, and 45 CFR 171.400, respectively), as well as the general provisions in subpart A of 45 CFR part 171. The conditions under which each exception can be satisfied are specified in 45 CFR part 171. Where the conditions include any requirements the actor's practice must satisfy for an exception to apply, these requirements are included in that exception's section of 45 CFR part 171. For example, all of the conditions and requirements for the Infeasibility Exception to apply to an actor's practice of not fulfilling requested EHI access, exchange, or use due to the infeasibility of the request are specified in § 171.204. The general provisions in subpart A indicate the statutory basis and purpose of the information blocking regulations, the applicability of the regulations, and definitions of certain terms used in 45 CFR part 171.

Specific to the Infeasibility Exception, the requirement that, for this exception to apply, the actor's practice must satisfy at least one condition in paragraph (a) and also satisfy the condition in paragraph (b) of § 171. 204 has been in place since the Infeasibility Exception (§ 171.204) was established in the ONC Cures Act Final Rule (85 FR 25869 and 85 FR 25958; *see also* 85 FR 25867). Thus, as is the case for a practice meeting any of the conditions codified in § 171.204(a), an actor's practice consistent with the § 171.204(a)(1) *uncontrollable events* condition would also need to meet the requirements of § 171.204(b), the *responding to requests* condition, for that practice to fully satisfy the Infeasibility Exception.

Comments. A few commenters suggested that 10 business days may not be enough time for an actor severely impacted by a disaster to become aware of and respond to requests received around the time the disaster occurred, or that actors may need time to recover from an event before they are able to respond to requests for EHI. One of these commenters cited the potential for some events to be sufficiently disruptive and that the actor would lose the ability to access requests received before and during the disruption. The commenter noted that a 10-day response time may be unreasonable in the middle of a major hurricane involving power outage, facilities damage, and displacement of staff members key to processing requests. A comment suggested specific changes to the *responding to requests* condition so that an automated notice a system is down be considered as sufficient ''notice'' to satisfy the exception.

Response. We did not propose in the HTI–1 Proposed Rule to change any aspect of the *responding to requests* condition (§ 171.204(b)) and decline to do so in this final rule. However, as it applies to actors' practices of not fulfilling requests that are infeasible because an uncontrollable event has, in fact, negatively impacted the actor's ability to fulfill access, exchange, or use of EHI, we welcome the opportunity to clarify that the *responding to requests* condition (§ 171.204(b)) does not focus on when the requestor sends or attempts to make the request. Rather, the *responding to requests* condition (§ 171.204(b)) specifies the ''receipt of the request.'' Satisfying the *responding to requests* condition, therefore, requires providing the reason for infeasibility in writing within ten business days of the actor *receiving* the request rather than counting ten business days from when a requestor may have sent or attempted to send the request.

Comments. A commenter supported the Infeasibility Exception and asked that ONC consider further examples and definitions of extreme and uncontrollable circumstances to prevent abuse of the condition.

Response. We appreciate the support. We note that the finalized revision to § 171.204(a)(1) includes the following additional clause at its end: ''. . . that in fact negatively impacts the actor's ability to fulfill the request.'' This new additional clause makes it clear that in order for the actor's not fulfilling a request to satisfy the § 171.204(a)(1) *uncontrollable events* condition, the uncontrollable event must, in fact, have had an adverse impact on the actor's ability to fulfill a request for EHI access, exchange, or use. We believe the clarifying modification will help prevent abuse of the condition because it will enable actors to more confidently and accurately assess when and how the *uncontrollable events* condition could be satisfied, thus deterring actors from asserting they cannot fulfill a request merely because an uncontrollable event that did not negatively impact the actor's ability to fulfill the request had occurred.

Summary of finalized policy—uncontrollable events condition of the Infeasibility Exception (§ 171.204(a)(1)):

After consideration of comments received, we have finalized the revised *uncontrollable events* condition to the Infeasibility Exception with modifications to the proposed regulatory text. We have finalized our proposal to replace ''due to'' with ''because of'' in § 171.204(a). As discussed in response to comments, we have also added to the end of the text of § 171.204(a) the following: ''that in fact negatively impacts the actor's ability to fulfill the request.'' This addition is intended to improve the clarity with which the text conveys that to meet this specific condition of the Infeasibility Exception with respect to any request, an actor cannot simply assert that they cannot fulfill a request because an event consistent with § 171.204(a) occurred. To meet the condition, the actor must demonstrate that the uncontrollable event, in fact, negatively impacted the actor's inability to fulfill a request.

b. Infeasibility Exception—Third Party Seeking Modification Use

In the HTI–1 Proposed Rule (88 FR 23865 through 23867), we proposed to renumber the Infeasibility Exception's (45 CFR 171.204) *infeasible under the circumstances* condition from paragraph (a)(3) to paragraph (a)(5) and to codify at (a)(3) a new condition *third party seeking modification use.* We proposed, as discussed in section IV.B.1.c below, another new condition that would be codified as paragraph (a)(4) of § 171.204. We received no comments expressing a particular view on the redesignation of *infeasible under the circumstances* condition as subparagraph (a)(5) and have, based on finalization of proposed new conditions in (a)(3) and (a)(4), finalized the redesignation of the *infeasible under the circumstances* condition as (a)(5).

We proposed that the § 171.204(a)(3) *third party seeking modification use* condition would apply in certain situations where the actor is asked to provide the ability for a third party (or its technology, such as an application) to modify EHI that is maintained by or for an entity that has deployed health information technology as defined in § 170.102 and maintains within or through use of that technology any instance(s) of any electronic health information as defined in § 171.102. As a reminder, to fully satisfy the exception in § 171.204, an actor's practice must meet one of the conditions in paragraph (a) of § 171.204 and the requirements in paragraph (b) of § 171.204 (''. . . the actor must, within ten business days of receipt of [a] request, provide to the requestor in writing the reason(s) why the request is infeasible'').

We proposed (88 FR 23865 through 23867) that the *third party seeking modification use* condition of the Infeasibility Exception would be limited to situations when ''[t]he request is to enable use of EHI in order to modify EHI (including, but not limited to, creation and deletion functionality), provided the request is *not* from a health care provider requesting such use from an actor that is its business associate'' (88 FR 23916, emphasis added).

In § 171.102, we define ''use'' for purposes of the information blocking definition to mean ''the ability for electronic health information, once accessed or exchanged, to be understood and acted upon.'' We stated in the ONC Cures Act Final Rule that ''acted upon'' within the final ''use'' definition ''encompasses the ability to read, write, modify, manipulate, or apply the information. . . .'' (85 FR 25806). Therefore, in § 171.204(a)(3), we proposed to use ''*third party seeking modification use*'' as a descriptive title for the new proposed condition of the Infeasibility Exception applicable to an actor's denial of requests from a third party for ''modification use'' of EHI. In particular, this new condition focuses on requests to modify EHI held by or for a health care provider and is not applicable to third-party requests for other activities that would fall within the § 171.102 definition of the broader term ''use.'' For example, the new *third party seeking modification use* condition would not apply to any request involving only the ability to read or apply the information, which are other activities in the broader definition of *use* we used in the ONC Cures Act Final Rule. The *third party seeking modification use* condition is also not applicable to any request for ''access'' or ''exchange'' (as these terms are defined in § 171.102) of EHI.

The information blocking definition (§ 171.103) refers to the ''access, exchange, or use'' of electronic health information, and each of these terms is defined for purposes of 45 CFR part 171 in § 171.102. In this portion of the preamble, as in the HTI–1 Proposed Rule (88 FR 23865), we use the term ''modify'' or ''modification use'' to describe the particular type of ''use'' covered by this new condition. We do so to avoid confusion between this ''modification use'' and the definition of the broader term *use* in § 171.102. It is important to note that the term ''modification use'' in the proposed and finalized § 171.204(a)(3) refers to a specific type of use within the § 171.102 definition of the term *use.*[249] Modification use focuses on actions on the EHI that change it in some way. Specifically, the condition focuses on requests to modify EHI held by or for a health care provider, but not to other types of ''use,'' such as the ability for EHI to be understood by a third party. The *third party seeking modification use* condition does not implicate, indicate, or imply any change to the definition of *use* in § 171.102 for any other purpose under 45 CFR part 171, or to any definition or other provision of the HIPAA Rules in 45 CFR parts 160 and 164. We recognize that HIPAA covered entities and business associates have an obligation under the HIPAA Privacy Rule to only disclose or use, in the sense of ''use'' as defined in 45 CFR 160.103, PHI as and when permitted or required under subpart E of 45 CFR part 164 or subpart C of 54 CFR part 1600 (see 45 CFR 164.502(a)). We have structured the information blocking regulations, including this finalized revision to the Infeasibility Exception, to accommodate that obligation.[250] We note that the *third party seeking modification use* condition does not imply or indicate any change to the HIPAA Rules (*see* 88 FR 23865).

We proposed to add a definition of *business associate* to § 171.102 because we use the term in the *third party seeking modification use* condition. We proposed that the definition of *business associate* in § 171.102 would, by cross-reference to 45 CFR 160.103, be the same as the HIPAA Rules' definition of ''business associate.'' We emphasize that the § 171.204(a)(3) *third party seeking modification use* condition does not operate to change a business associate's rights or responsibilities under their business associate agreement (BAA) with any HIPAA covered entity. We also reiterate that the information blocking regulations do not require actors to violate BAAs or associated service level agreements. However, as we also previously explained in the ONC Cures Act Final Rule (85 FR 25812) and in information blocking FAQ28 (available at *HealthIT.gov*[251]), terms or provisions of

[249] In § 171.102, we define ''use'' for purposes of the information blocking definition to mean ''the ability for electronic health information, once accessed or exchanged, to be understood and acted upon.''

[250] We discuss information blocking regulations' accommodation of HIPAA and other privacy laws in section 4.A, general comments.

[251] IB.FAQ28.2.2021APR: ''Do the information blocking regulations require actors to violate existing business associate agreements in order to not be considered information blockers?'' (Available at *https://www.healthit.gov/faq/do-information-*

BAAs could constitute an interference (and thus could be information blocking) if used in a discriminatory manner by an actor to forbid or limit access, exchange, or use of EHI that otherwise would be a permitted disclosure under the HIPAA Privacy Rule. To determine whether there is information blocking, the actions and processes (*e.g.,* negotiations) of the actors in reaching the BAA and associated service level agreements would likely need to be reviewed to determine whether there was any action taken by an actor that was likely to interfere with (''prevent, materially discourage, or otherwise inhibit''; § 171.102) the access, exchange, or use of EHI, and whether the actor had the requisite intent (85 FR 25812).

Comments. Comments received on the proposed § 171.204(a)(3) *third party seeking modification use* condition were generally supportive. Comments supporting this proposal commended the proposal's alignment with the policy goals expressed in the HTI–1 Proposed Rule, including reducing the burden on actors to document each modification use request in the same way that an actor would need to document its actions for the *infeasible under the circumstances* condition of the Infeasibility Exception. Some commenters supportive of this proposal also expressed appreciation for the proposal's applicability to situations where an actor may be concerned about the accuracy or reliability of data that a third party would like to add to an individual's designated record set maintained by the actor. A few commenters also noted that the proposed condition would simplify the handling of certain requests for EHI. A few commenters expressed support for the proposal's exclusion of requests that come from health care providers to their business associates.

Response. We appreciate the support expressed by many commenters. We have finalized the § 171.204(a)(3) *third party seeking modification use* condition with the minor modification of deleting the parenthetical ''(including but not limited to creation and deletion functionality)'' from the regulatory text in § 171.204(a)(3). This is done solely for readability purposes. The requests covered by this condition, as finalized, are to enable a third party EHI modification use functionality, including, but not limited to, creation and deletion functionality.

Comments. A few of the commenters did not support the proposal. Some of these commenters expressed concern that the proposal could potentially inhibit care coordination by making it too easy for an actor holding EHI to simply refuse modification use requests from third parties who also furnish services to the same patient(s). Some of these commenters expressed concern that certain actors, such as health IT developers of certified health IT, may seek to misuse the proposal to restrict access to EHI in an overly broad manner.

Response. We thank commenters for bringing to our attention their concerns about access, exchange, and use of EHI in support of care coordination. In developing our discrete proposal to provide further certainty to actors and now in finalizing this proposal, we have considered these concerns. In the HTI–1 Proposed Rule discussion of the reasons why this condition is not available to an actor when the actor is a business associate of a health care provider who is making the modification use request, we noted that there is often a level of trust and contractual protections between covered entities and business associates that removes certain concerns, such as security and data provenance, that led us to propose this new condition as structured (88 FR 23866). Many of these matters are addressed in business associate agreements, including security, as well as the permitted uses of the EHI (ePHI) that the covered entity grants the business associate. Further, the HIPAA Privacy and Security Rules place certain obligations on covered entities and their business associates that protect the privacy and security of EHI (and other PHI). For these reasons, we finalized this condition, as proposed, which permits actors to deny requests to modify EHI provided the request is not from a health care provider for which the actor is the business associate.

This condition was not proposed to apply, and as finalized does not apply, to an actor's practice of refusing to receive or process EHI via health information exchange or refusing to make EHI available for access, exchange, or use for permissible purposes. Where the manner or means of EHI use sought by a third party would not involve enabling a third party to modify (such as by adding to, creating, overwriting, editing, or deleting) EHI, then the condition does not apply even if the request is from someone other than a health care provider to whom the actor is a business associate. We also clarify that the *third party seeking modification use* condition applies only where a third party seeks modification use functionality for EHI within the records or systems maintained by the actor. This condition cannot be satisfied where a third party seeks access or exchange of EHI, even if the actor is certain that the requestor will or may make ''modification use'' of the EHI once it (or a copy of it) is in the requestor's possession, custody, or control. For example, the condition does not apply to situations where a health care provider, or their health IT developer chooses not to accept and process (such as through an EHR's receive and incorporate functions) EHI from a patient's health plan or prior health care provider or another of the patient's current health care providers. The condition also does not apply to read-only access (such as through API technology certified to any of the criteria in § 170.315(g)(7) through (10)), or to an actor's practice of refusing to make a patient's EHI available for access, exchange, or use by care coordination partners for permissible purposes. ''Permissible purposes'' is defined for purposes of the information blocking regulations in § 171.102.

Regarding commenters' concerns about entities potentially abusing the *third party seeking modification use* condition to restrict access, exchange, or use of EHI, the limited circumstances for which this condition applies, as described above and below, will mitigate any potential for abuse. This condition does not pose a problem for care coordination because it is very narrowly focused only on a particular manner of modification use of EHI (88 FR 23866) that the health care provider or the business associate would not have to enable, and it does not apply to a wide variety of manners by which health care providers routinely access, exchange, and use EHI for care coordination purposes. However, any abuse of this condition or any component of the information blocking regulations would be of concern to ONC, and we encourage anyone who believes they may have experienced or observed information blocking by any health care provider, health IT developer of certified health IT, or health information network or health information exchange to share their concerns with us through the Information Blocking Portal [252] on ONC's website, *HealthIT.gov*.[253]

blocking-regulations-require-actors-violate-existing-business-associate. Retrieved Sep 14, 2023.)

[252] URL *https://inquiry.healthit.gov/support/plugins/servlet/desk/portal/6* (URL confirmed current and operational as of Sep 14, 2023).

[253] URL to Information Blocking topic section of *HealthIT.gov: https://www.healthit.gov/topic/information-blocking.* (URL confirmed current and operational as of Sep 14, 2023.)

Information received by ONC through the Information Blocking Portal as well as the Health IT Feedback and Inquiry Portal [254] also helps inform the development of resources we make publicly available on ONC's website, *HealthIT.gov*.

Comments. A few commenters requested that ONC provide further guidance on specific use cases where the *third party seeking modification use* condition could apply, including materials such as FAQs, scenario-based guidance, and examples of documenting use of the condition, including for behavioral health providers. One commenter recommended that documentation requirements for the condition be minimal.

Response. We thank commenters for their feedback. We release educational resources on an ongoing basis. ONC-published resources can be found on *HealthIT.gov* and to date include for the HTI–1 rulemaking: recorded webinars (both general and tailored for particular topics and audiences), fact sheets, measurement spec sheets, blog posts, and a new website hub for links to various materials and educational resources. In addition to the examples we provided in the HTI–1 Proposed Rule and provide in this final rule describing the applicability of this condition, we will continue to provide resources such as infographics, fact sheets, webinars, and other forms of educational materials and outreach. Resources specific to the information blocking regulations in 45 CFR part 171, across this and other ONC rules, are available on *HealthIT.gov.* The short URL that redirects to the information blocking landing page is: *healthit.gov/informationblocking.*

Regarding documentation requirements, we have not proposed or finalized a specific documentation requirement for the *third party seeking modification use* condition. In general, actors have flexibility to determine what documentation to create or keep in the event that they seek to claim an exception. However, as also discussed under the *uncontrollable events* condition above, an actor would need to demonstrate for each practice for which the Infeasibility Exception is sought on the basis of the *third party seeking modification use* condition (§ 171.204(a)(3)) that the condition was met at all relevant times and that the condition in § 171.204(b) was also met.

Comments. One commenter stated that the exceptions in subparts B and C of 45 CFR 171 are too complex for small health care providers, do not provide additional clarity, and that ONC should provide separate, simplified exceptions for health care providers.

Response. As we noted in the ONC Cures Act Final Rule, (85 FR 25819), we tailor information blocking exceptions and provide significant detail within each exception to clearly explain what an actor must do to meet each exception. For each exception, we typically propose and finalize conditions that can be consistently applied across all actors. However, there are conditions within certain exceptions that apply to one or a subset of actors, as applicable (85 FR 25819). As we stated in the ONC Cures Act Final Rule, the clearest and most equitable approach to the exceptions is to make all of the exceptions apply to all actors (85 FR 25819). Therefore, we decline the commenter's recommendation to provide ''separate, simplified exceptions for health care providers.''

We believe that our explanations of the exceptions, as included in the ONC Cures Act rulemaking and in the HTI–1 Proposed Rule and this final rule provide the necessary clarity for health care providers, including small health care providers, to understand and apply the exceptions. As discussed throughout this final rule, we also invest in educational outreach to interested parties, including small health care providers and associations that represent them, in an effort to further explain the exceptions through presentations and written resources such as fact sheets.

We also note that the exceptions are voluntary and offer an actor certainty that a practice that satisfies all of the relevant conditions of an exception will not be considered information blocking. Further, we reiterate that failure to meet an exception does not necessarily mean a practice meets the definition of information blocking. By satisfying an exception, an actor gains the assurance that the actor's practice does not constitute information blocking. An actor's practice that does not meet the conditions of an exception does not automatically constitute information blocking, as the practice must still meet all the elements of the information blocking definition to be considered information blocking, including that the practice is likely to interfere with the access, exchange, or use of EHI, and that the actor acted with the requisite intent (85 FR 25820).

Comments. A few commenters responded to our request for comment on whether the condition should be of limited duration, and specifically, whether we should consider proposing to eliminate the condition if, at some point in the future, health information technology is capable of supporting lawful third-party modification use of EHI by any party with no or minimal infeasibility or other concerns. The majority of comments on this subject stated either that the proposal should not have a sunset date, or that it would be premature to establish a sunset date at this time. Two commenters stated that the condition should or could be eliminated in the future if the future technology is capable of supporting the aforementioned modification use of EHI, with no or minimal infeasibility or other concerns.

Response. We thank the commenters for their feedback. We agree that it would be premature to establish a sunset date for the condition because the appropriateness of eliminating the condition depends on the continued development of health IT's capability to support lawful third-party modification use of EHI by any party and with no or minimal infeasibility or other concerns. Because the pace of that continued health IT development is difficult to predict, we are not establishing a sunset date for § 171.204(a)(3) at this time. If advances in health IT capabilities or other changes in the interoperability and information sharing environment indicate to us that this condition should be modified or sunset, we would anticipate proposing such a change in a future rulemaking.

Comments. Three commenters expressed a concern that, as written, the condition would not apply to requests to ''exchange'' EHI by adding new EHI to a system through exchange from a third party. The commenters stated that ONC should add ''exchange'' of EHI to the condition.

Response. We thank the commenters for their feedback. The *third party seeking modification use* condition of the Infeasibility Exception is available to most actors to address situations where a third party's request is to modify EHI stored or maintained by an actor (88 FR 23866). The condition focuses on requests for a third party to have functionality to make modification use of EHI while, and as, it is held in the records or systems of the actor. We did not propose the condition to apply, and it cannot be met, where a third party is seeking to exchange EHI with the actor or to access a copy of EHI, even if the actor may know or reasonably suspect that the third party may modify (or have modified) EHI that is in records, applications, or systems maintained by the third party.

[254] URL *https://inquiry.healthit.gov/support/plugins/servlet/desk/portal/2* (URL confirmed current and operational as of Sep 14, 2023).

In situations where an actor receives EHI via exchange from a third party, whether that EHI is reconciled and incorporated into the record (''added'' to the record) is a determination for the health care provider and potentially its business associates. Any such exchange of EHI and subsequent determinations to reconcile and incorporate EHI into the record (or not) is not within the scope of the proposed condition. Such practices and scenarios may implicate the information blocking definition, but there may also be other conditions or exception that apply depending on the specific facts and circumstances.

Comments. Commenters stated that the limitation to this condition is not broad enough, and that ONC should expand the limitation of this condition to also apply when the actor's customers are not HIPAA covered entities, or are not health care providers, but are maintaining EHI in systems licensed by an actor. Two commenters stated that the § 171.204(a)(3) *third party seeking modification use* condition should not apply in circumstances where the actor is a business associate or contractor of the organization that has licensed the interoperability elements or systems responsible for maintaining EHI. Along these lines, two other commenters expressed a concern that an actor, such as a health IT developer of certified health IT, that maintains EHI on behalf of an HIN/HIE could use this condition to deny an HIN/HIE's request, using third-party technology, for modification use of EHI maintained by the HIN/HIE. The commenters suggested that ONC clarify that the condition does not apply where a HIN/HIE requested modification use of EHI held by a health care provider or their health IT developer.

Response. We thank the commenters for their feedback. We finalized the limitation to this condition to apply when the actor is a business associate of a health care provider making the modification use request, and we are not at this time expanding the limitation of the condition as some commenters suggested. As we noted in proposing this condition, there is often a level of trust and contractual protections between covered entities and business associates that removes certain concerns, such as security and data provenance, that led us to propose this new condition (88 FR 23866). We explained in the HTI–1 Proposed Rule discussion of the limitation of this condition that covered entities (health care providers) and their business associates (as permitted by their BAA) need to access and modify relevant EHI held by other business associates of those covered entities on a regular basis (88 FR 23866). Because our proposal focused on the obligations that the HIPAA Privacy and Security Rules place on covered entities and their business associates to protect the privacy and security of EHI (and other PHI), we decline to expand the limitation of the condition at this time.

Regarding the commenters' concern about the application of the condition, we note that if the request for modification use is from the health care provider requesting such use from an actor that is the health care provider's business associate, the condition would not apply. Even if the actor who is a business associate of a health care provider could provide, or currently provides, items or services or engages in activities similar or identical to those the health care provider wants the third party to have modification use of EHI to accomplish, the condition does not apply when the actor is the business associate of the health care provider requesting modification use of EHI. Likewise, the finalized condition does not apply to an actor's denial of modification use by a third party where the actor is a subcontractor of any business associate to a health care provider, and the health care provider requests such use of EHI maintained by or on behalf of the health care provider. A ''business associate'' is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to PHI (§ 171.102). A ''business associate'' is also a subcontractor that creates, receives, maintains, or transmits PHI on behalf of another business associate.

For purposes of the provision ''carving out'' requests from a health care provider to an actor that is its business associate from application of § 171.204(a)(3), it does not matter whether the health care provider merely licenses or otherwise obtains from the actor use of interoperability elements that would be necessary to enable a third party's modification use of EHI that the health care provider maintains, or the health care provider contracts with the actor to maintain and manage on the health care provider's behalf. If the actor is a business associate of the health care provider and the provider requests modification use by a third party of EHI, then the condition does not apply to the actor's denial of that request. [255]

For these reasons, and in consideration of these and all comments received on our discrete proposal, we finalized, as proposed, a condition that permits actors to deny requests to modify EHI provided the request is not from a health care provider for which it is the business associate. We have not at this time expanded the limitation to the condition as the commenters requested. However, we note that we may consider amending the *third party seeking modification use* condition or taking other appropriate steps in future rulemaking in response to changing market conditions, experience with the condition in practice, or other signals that suggest amending the condition may be appropriate.[256]

As a reminder, the *third party seeking modification use* condition does not operate to change an actor's contractual obligations to their customers. When an actor engages in a practice to deny modification use of EHI under the *third party seeking modification use* condition, they may also wish to consider whether the practice violates any of their existing contractual obligations.

Comments. Several commenters raised issues that are out of scope for this proposal, including:

- asking ONC to reiterate that actors cannot claim this exception to prevent requests from an individual or their personal representatives to amend the individual's PHI or record as permitted by the HIPAA Privacy Rule;
- a request for ONC to study what entities have access to health care providers' EHRs, why those entities may request to access or change authenticated documents or clinical notes, how health care providers evaluate the accuracy of data a third party wants to add to an individual's EHI, the potential benefits and harms of incorporating such data, and whether this condition would be possible in a future environment in which the Trusted Exchange Framework and Common Agreement (TEFCA) is actively exchanging data;
- asking ONC to consider whether patients should be consulted before data from another health care provider is incorporated into their EHI;

[255] Whether other conditions in § 171.204(a) or another exception codified in subpart B or C of 45 CFR part 171 could be or have been satisfied in a particular situation would depend on the specific facts and circumstances of the case.

[256] Patterns described to us in claims or suggestions of possible information blocking submitted through the Report Information Blocking Portal illustrate just one example of such signals coming to our attention. (The Report Information Blocking Portal's URL as of Jul 28, 2023, is: *https://inquiry.healthit.gov/support/plugins/servlet/desk/portal/6*).

• asking ONC to consider what annotation mechanisms are or should be in place to create an audit trail for modifications to EHI;
• asking ONC to establish incentives for third-party applications to utilize best practices regarding maintaining the integrity and security of electronic health information;
• a request that the ten-business day timeline established in § 171.204(b) should be revised to be longer;
• a request to include in the certification criteria for health IT the functionality to alert an actor when a third party seeks modifications to EHI in the actor's system(s);
• recommending that ONC update certification criteria to better support health care providers' ability to use third-party apps maintained in certified health IT, utilizing existing APIs and support for user-created fields, while minimizing risks to data security and EHR performance;
• requesting examples of how providers should store information from a third party separate from the medical record, and requesting ONC work with health IT developers to implement a mechanism for providers to maintain data that has not been integrated into the medical record.

Response. We thank commenters for their input and reiterate our continued commitment to supporting EHI sharing consistent with patient preferences and applicable law. Whether received as out-of-scope comments on a proposed rule or through informal channels, the feedback, and questions we receive, are appreciated and help to inform our development of information resources that we make publicly available on *HealthIT.gov.* Informal channels include, for example, the Health IT Feedback and Inquiry Portal [257] that is available year-round and not tied to the comment period for a proposed rule.

Regarding the relationship between the finalized § 171.204(a)(3) *third party seeking modification use* condition and the HIPAA Rules, we note again, as we did in the HTI–1 Proposed Rule, that the *third party seeking modification use* condition does not imply or indicate any change to the HIPAA Rules (*see* 88 FR 23865). Actors should note and should operate with awareness that a practice satisfying any information blocking exception in 45 CFR part 171 simply means that practice is not considered to be ''information blocking'' as defined in § 171.103. Any actor (as defined in 45 CFR 171.102) that is also subject to any provision(s) in 45 CFR parts 160, 162, or 164 must continue to comply with such provision(s) when and to the extent such provisions of the HIPAA Rules are applicable to the actor's conduct.

Summary of Finalized Policy: Third Party Seeking Modification Use Condition

As noted above and for the reasons stated above and in the HTI–1 Proposed Rule, we have finalized the condition as proposed with a non-substantive edit to simplify the regulation text by removing the parenthetical ''(including, but not limited to, creation and deletion functionality).''

We note that for purposes of this condition, an actor may choose to verify that the modification use request came from the health care provider themselves or accept the third party's representation of a request as coming from a health care provider. Any actor considering whether to potentially avail themselves of the certainty offered by this exception will have flexibility to structure their communications approaches and operating procedures for communicating with the health care provider of which the actor is a business associate, or with third parties representing themselves as business associates of such health care provider. This flexibility enables actors to operate and communicate efficiently while complying with the actor's obligations under the HIPAA Privacy Rule, other applicable law, and its binding agreements (including its BAAs) with the health care providers who choose to request modification use for a third party functionality either directly from the actor or through one of the health care provider's business associates. As discussed above under comments on documentation, an actor would need to demonstrate for each practice for which the Infeasibility Exception is sought on the basis of the *third party seeking modification use* condition (§ 171.204(a)(3)), that it met the *third party seeking modification* condition and also met the § 171.204(b) *responding to requests condition* at all relevant times.

As with every other condition in § 171.204(a), we note that the § 171.204(a)(3) *third party seeking modification use* condition stands alone. This means an actor's practice could meet it without needing to meet any other § 171.204(a) condition. It also means an actor's practice that fails to meet the § 171.204(a)(3) *third party seeking modification use* condition could nevertheless satisfy another of the conditions, such as the *infeasible under the circumstances* condition in § 171.204(a)(5).

We emphasize that other conditions within § 171.204(a) and all of the other exceptions would remain available for consideration by the actor as to their applicability to the situation and request where the finalized § 171.204(a)(3) *third party seeking modification use* condition of the Infeasibility Exception would not be available.

c. Infeasibility Exception—Manner Exception Exhausted

In the HTI–1 Proposed Rule, we proposed to renumber the Infeasibility Exception's (45 CFR 171.204) ''*infeasible under the circumstances*'' condition from paragraph (a)(3) to paragraph (a)(5) and to codify at (a)(4) a new ''*manner exception exhausted*'' condition (88 FR 23867). We stated that the proposed *manner exception exhausted* condition would apply where an actor is still unable to fulfill a request for access, exchange, or use of EHI after having exhausted the exception in § 171.301 (which we have in this rule renamed Manner Exception, see Section IV.A.1), including offering all alternative manners in accordance with § 171.301(b), so long as the actor does not currently provide to a substantial number of individuals or entities similarly situated to the requestor the same requested access, exchange, or use of the requested EHI (88 FR 23867).

In the ONC Cures Act Final Rule (85 FR 25642), we finalized the Infeasibility Exception with modifications from the proposal (84 FR 7542 and 7603) to address concerns raised by commenters (*see* 85 FR 25866 through 25870). We finalized (85 FR 25858) three conditions that more specifically address situations where the Infeasibility Exception would be appropriately used. One of the conditions we finalized, *infeasible under the circumstances,* requires the actor to demonstrate, through a contemporaneous written record or other documentation, its consideration, in a consistent and non-discriminatory manner, of certain factors that led to its determination that complying with the request would be infeasible under the circumstances. The Infeasibility Exception (§ 171.204), as finalized in the ONC Cures Act Final Rule, provides assurance to an actor that if it meets applicable conditions of the exception at all relevant times, its practice will not be considered information blocking.

Also, in the ONC Cures Act Final Rule, we finalized the ''Content and Manner Exception'' (now the Manner Exception) (45 CFR 171.301). Under § 171.301, for the Manner Exception to apply, an actor must fulfill a request for

[257] URL *https://inquiry.healthit.gov/support/plugins/servlet/desk/portal/2* (URL confirmed current and operational as of Sep 14, 2023).

access, exchange, or use of EHI in any manner requested, unless the actor is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request (45 CFR 171.301(b)(1)(i), as originally codified). If an actor and requestor reach agreeable terms and the actor fulfills a request described in the manner condition in any manner requested: (1) Any fees charged by the actor in relation to its response are not required to satisfy the Fees Exception in § 171.302; and (2) any license of interoperability elements granted by the actor in relation to fulfilling the request is not required to satisfy the Licensing Exception in § 171.303 (45 CFR 171.301(b)(1)(ii), as originally codified) (85 FR 25877).

Section 171.301(b)(2) (original codification, redesignated in this final rule as § 171.301(b)) provides for fulfilling a request to access, exchange, or use EHI in a manner other than the manner requested. If an actor does not fulfill a request in any manner requested because it is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request, the actor must fulfill the request in an alternative manner agreed upon with the requestor consistent with § 171.301(b)(2) (original codification, now redesignated § 171.301(b)) in order to satisfy the exception (85 FR 25877). The Manner Exception offers certainty that an actor's practices that fully satisfy the Manner Exception's conditions will not be considered information blocking and is meant to incentivize offering an alternative manner (with priority to interoperable manners based on HHS-adopted and available open standards) when the actor is unable to fulfill access, exchange, or use of the requested EHI in the manner initially requested.

As discussed in the HTI–1 Proposed Rule, actors expressed uncertainty to ONC as to whether they have satisfied the *infeasible under the circumstances* condition in instances where they contended that fulfilling a request for access, exchange, or use of EHI would be infeasible (85 FR 23867). Under the Infeasibility Exception, the *infeasible under the circumstances* condition requires the actor to demonstrate that complying with the request is infeasible when considering, among other things, the financial and technical resources available to the actor and why the actor was unable to provide access, exchange, or use of EHI consistent with the Manner Exception. Specifically, actors have expressed concern about circumstances where the actor's inability to satisfy the Manner Exception's conditions rests solely on the requestor refusing to accept access, exchange, or use in *any* manner consistent with § 171.301, and fulfilling the request in the manner requested would require substantial technical or financial resources (or both) in the view of the actor, including significant opportunity costs. We have observed this being more of a concern for actors with significant skills and other resources for developing unique technical solutions or new technological capabilities (*e.g.,* EHR developers or HIN/HIEs) than for actors with few to no such resources (*e.g.,* small clinician office practices or safety net clinics), because, as noted, the *infeasible under the circumstances* condition of the Infeasibility Exception (§ 171.204(a)(5); previously § 171.204(a)(3)) requires actors to demonstrate their consideration of the financial and technical resources available to them, as well as why the actor was unable to provide access, exchange, or use of EHI consistent with § 171.301.

Among those actors with substantial skills and other resources to develop new, unique or unusual manners of supporting access, exchange, or use of EHI, we see actors who appear to be experiencing a problematic level of uncertainty about whether they will be engaging in information blocking if they decline demands from requestors for non-standard or non-scalable solutions that they do not currently support *even after* they have offered to provide access, exchange, or use of EHI in the same manner(s) the actor makes generally available to its customers or affiliates, *and* through standards-based manners, consistent with § 171.301—including offering terms for such manners that are consistent with the Fees (§ 171.302) and Licensing (§ 171.303) Exceptions. We anticipate that this uncertainty will lead actors who, again, have already exhausted the Manner Exception (§ 171.301), to divert their development capacity to fulfilling requested manners of access, exchange, or use of EHI that they *could* invent to meet the demands of a requestor determined to accept only the original manner they specified and who are unwilling or unable to agree to terms consistent with the Fees (§ 171.302) and Licensing (§ 171.303) Exceptions for their requested manner or any alternative manner consistent with the Manner Exception (§ 171.301) (88 FR 23868).

We stated in the HTI–1 Proposed Rule (88 FR 23868) that this new condition is necessary to ensure actors reasonably allocate resources toward interoperable, standards-based manners rather than allowing requestors, who, for whatever reason, do not build their products for compatibility with open consensus standards or other industry standards to attempt to force use of non-standard or non-scalable solutions by simply refusing to accept access, exchange, or use of EHI in any other manner. This diversion of resources away from standards-based and scalable manners of exchange detracts from, instead of supporting, achievement of key policy goals such as increased interoperability and innovation in use of open consensus standards to achieve secure, seamless exchange. Where novel approaches to system interfaces or other aspects of access, exchange, or use of EHI represent improvements over other available approaches, we anticipate these approaches will not need to be forced upon the industry but will instead find a natural foothold and diffuse according to a normal innovation curve.

Therefore, to reduce confusion and provide more certainty to actors, we proposed and have finalized at § 171.204(a)(4) a new condition in the Infeasibility Exception, the *manner exception exhausted* condition. Actors will be able to satisfy this exception when they have ''exhausted'' the *manner requested* condition and *alternative manner* condition of the Manner Exception and meet the other requirements of the new condition. If an actor either technically cannot provide the access, exchange, or use of EHI in the manner requested, or the actor and requestor cannot reach agreeable terms on the manner requested, then the actor must attempt to fulfill the request using the alternative manners in § 171.301(b) (85 FR 25877) (previously § 171.301(b)(2)(i)). Under the Manner Exception, for any alternative manner, the requestor must either specify the manner they would accept (§ 171.301(b)(2)(i)(A) and (B)) or specifically agree with the machine-readable format that they would accept (§ 171.301(b)(2)(i)(C)). In situations where an actor offers the alternative manners and the requestor does not specify or agree to receive the EHI via the offered alternative manners (as may be the case if the requestor does not want to receive the EHI in such a manner or cannot receive the EHI in such a manner), an actor may now seek to satisfy the new finalized *manner exception exhausted* condition of the Infeasibility Exception.

Previously, an actor who offered all the alternative manners would likely look to the *infeasible under the circumstances* condition of the Infeasibility Exception, which requires actors to demonstrate that complying with the request is infeasible when

considering many factors, including the cost to the actor of complying with the request in the manner requested and the financial and technical resources available to the actor. The newly finalized *manner exception exhausted* provides actors the option of satisfying the Infeasibility Exception without needing to assess whether they *could* meet the requestor's particularized demands regarding the manner and/or terms in which they want to obtain access, exchange, or use of the requested EHI.

Comments. Most commenters were supportive of ONC's proposal to add the *manner exception exhausted* condition to the Infeasibility Exception. Commenters stated that it would reduce burden and allow actors to focus on innovation. Many commenters appreciated that the condition encourages use of standards-based mechanisms, and that it removes the uncertainty that could come about if it is technically infeasible for an actor to fulfill a request or when the actor has offered the alternative manners, but the requestor has not specified or agreed, as applicable, to access, exchange, or use of the EHI in any of those manners. Many commenters also appreciated ONC's acknowledgment that interoperable, standards-based exchange should be favored over expensive, resource-intensive, one-off solutions. Other commenters expressed appreciation that the condition allows health IT developers of certified health IT and other actors the opportunity to reach agreement on market-based terms and pricing to protect investments, while still promoting interoperability. A few commenters also expressed appreciation that the condition can be met without the actor needing to demonstrate they considered the resources available to the actor, and that exchanging entities will be protected from costly technical changes or solutions made solely to avoid claims of information blocking.

Alternately, a few commenters expressed general disagreement with the proposed condition. One commenter expressed concerns that the condition could be interpreted to allow actors to remain in exchange patterns that do not expand interoperability across a range of requestors and use cases. Another commenter noted that atypical requests may be necessary to achieve a particular use of EHI that is not adequately supported by existing standards.

Response. We thank commenters for their thoughtful feedback. Upon consideration of all comments received related to this proposal, we have finalized the condition as proposed with two modifications discussed below. We agree that the *manner exception exhausted* condition prioritizes interoperability and encourages efficiency by applying the Infeasibility Exception under circumstances where the actor cannot meet, or cannot be certain that they have met, the *infeasible under the circumstances* condition. We recognize that custom, one-off solutions can be costly and inhibit investment in innovative, scalable approaches to interoperability and exchange. We also recognize that atypical requests may be necessary to achieve a particular use of EHI and note that nothing in the information blocking regulations would prevent a requestor and actor from coming to an agreement to achieve innovative solutions to interoperability challenges or atypical use cases. To this point, we previously established the *manner requested* condition of the Manner Exception, now codified in § 171.301(a), which permits actors and requestors to come to terms on access, exchange, and use of EHI without such terms necessarily satisfying the § 171.302 Fees Exception or § 171.303 Licensing Exception.

In response to concerns that this may allow actors to remain in exchange patterns that do not expand interoperability, we note that satisfying the finalized *manner exception exhausted* condition of the Infeasibility Exception requires the actor to offer a standards-based method of exchange, either through certified health IT or using technology and transport standards published by the federal government or a standards developing organization accredited by the American National Standards Institute (ANSI). Both methods would support interoperability, and the use of certified health IT incrementally expands interoperability through certification to new and revised certification criteria that include new and updated standards and capabilities.

How many alternative manners are required to satisfy the condition?

In the HTI–1 Proposed Rule, we stated that it is important that the Manner Exception not be considered exhausted if the actor offers only one alternative manner, or only the least-interoperable ''alternative machine-readable format'' now codified in § 171.301(b)(1)(iii) (88 FR 23869). Therefore, we proposed a second factor requiring actors to have offered all three alternative manners in accordance with § 171.301(b) (88 FR 23869). We requested comments on how many of the alternative manners an actor should be required to offer in order to satisfy the proposed *manner exception exhausted* condition of the Infeasibility Exception: one, two, or all three alternative manners.

As explained below, we have finalized the *manner exception exhausted* condition of the Infeasibility Exception with a requirement that an actor offer two alternative manners, at least one of which must be either the alternative manner in § 171.301(b)(1)(i) or (b)(1)(ii). These alternative manners are, respectively, ''[u]sing technology certified to standard(s) adopted in part 170 that is specified by the requestor'' (in other words, via health IT certified under the ONC Health IT Certification Program, 45 CFR part 170) or, ''[u]sing content and transport standards specified by the requestor and published by: (A) the Federal Government; or (B) a standards development organization accredited by the American National Standards Institute'' (45 CFR 171.301(b)(1)). An actor may offer both of these alternative manners to satisfy this particular factor of the *manner exception exhausted* condition, or only one of these two *and* the manner specified in § 171.301(b)(1)(iii), which is ''[u]sing an alternative machine-readable format, including the means to interpret the electronic health information, agreed upon with the requestor.'' If the actor offers the EHI in at least two manners including one of either (b)(1)(i) or (b)(1)(ii), then this factor of the finalized *manner exception exhausted* condition is satisfied.

Comments. Responses to our request for comment on how many alternative manners an actor should be required to offer before this condition would be available reflected a broad range of perspectives. Many commenters said two alternative manners should be enough. Other commenters said just one, and a couple of commenters suggested requiring actors to exhaust all of the actor's *own* manners of exchange prior to making use of the condition. Another commenter requested that an actor be required to demonstrate that they have inventoried all of the information sharing tools available that could be offered as an alternative manner and require the actor to have made those available to the requestor before they can satisfy the condition. One commenter asked for a specific carve-out for health care providers that would only require them to offer access, exchange, or use in the manners supported by their certified health IT or any other manner that requires minimal effort. Another commenter suggested a specific carve-out for health care providers who do not use certified health IT, stating that it should be

enough for such actors to offer access, exchange, and use only in a machine-readable manner. One commenter suggested that ONC require actors to offer a minimum of two manners for USCDI data elements, and only one alternative manner for any EHI beyond USCDI.

Response. After reviewing all comments, in § 171.204(a)(4)(ii), we have finalized the regulatory text so that the *manner exception exhausted* condition can be satisfied when an actor (who was unable to fulfill a request for access, exchange, or use of EHI because they could not reach an agreement with a requestor or were technically unable to fulfill the request in the manner requested) offered the requestor at least two alternative manners, one of which must use either technology certified to standard(s) adopted in part 170 that is specified by the requestor (§ 171.301(b)(1)(i)) or published content and transport standards consistent with § 171.301(b)(1)(ii).

By requiring actors to offer at least one of the first two alternative manners (as listed in § 171.301(b)(1)(i)–(iii)), we are balancing the interest of the actor in achieving certainty that the practice will fulfill the new condition, while also ensuring that interoperable, standards-based exchange remains favored over other methods of exchange. We believe that requiring all three alternative manners, as originally proposed, would place an unequal burden on actors who are not required by other government regulations or incentivized by any public or private program to use certified health IT. We believe that requiring two alternative manners, one of which must be more interoperable than is typically the case with a machine-readable format (*i.e.,* § 171.301(b)(1)(iii)), ensures that the condition will not have the undesirable effect of dampening actors' or requestors' enthusiasm for adopting and advancing standards-based interoperability.

The finalized requirement for the actor to have offered at least two alternative manners also balances the interests of those commenters who requested the condition be satisfied with just one alternative manner and those who wanted all three alternative manners. While nothing would stop an actor from offering a requestor all available manners at its disposal, we believe making that a requirement to satisfy the *manner exception exhausted* condition would render the condition impractical for many actors to satisfy and defeat at least a portion of our purpose in proposing it: to offer actors a simpler option for certainty than was already available in the *infeasible under the circumstances* condition. We also note that an actor could respond to a request by providing as much of the EHI as possible via any manner requested or an alternative manner, and still make use of the *infeasible under the circumstances* condition for any other EHI that they are technically unable to offer via an alternative manner, so long as the practice satisfies all the requirements of that condition (now § 171.204(a)(5)). As a reminder, to meet the Infeasibility Exception as a whole, actors will still, regardless of the condition(s) satisfied in paragraph (a) in § 171.204, also need to satisfy the condition in paragraph (b): *responding to requests.*

Comments. Some commenters expressed confusion over what exactly is an ''alternative manner.'' One commenter stated that, taken literally, ''all alternative manners'' would force an actor to offer tens or hundreds of possible technical solutions.

Response. We appreciate the comments and the opportunity to address the confusion. When referring to ''alternative manners'' we do not mean all possible manners of exchange other than the manner requested. Rather, we specifically mean only manners that would be consistent with subparagraph (i), (ii), or (iii) of § 171.301(b)(1). Offering as few as one option per category is sufficient to satisfy either paragraph (b)(1) of the *alternative manner* condition of the Manner Exception (§ 171.301) or the ''at least two alternative manners'' requirement finalized as part of this *manner exception exhausted* condition (subparagraph (a)(4)) of the Infeasibility Exception (§ 171.204).

Comments. A commenter asked that ONC clarify that responding actors are responsible to exchange EHI for the purpose and in the manner requested, if they are able to do so, even if they are not accustomed to utilizing the requested transaction pattern.

Response. We appreciate the opportunity to clarify. The commenter is incorrect. An actor may satisfy any of the exceptions to the information blocking definition in order to have certainty that their practice is not information blocking. Under the *manner requested* condition (now § 171. 301(a)) of the Manner Exception, an actor responding to a request to exchange EHI for a certain purpose and in a certain manner must only do so if they are technically able to and reach an agreement with the requestor. If they are not technically able to do so, or cannot reach agreement with the requestor, then an actor seeking certainty that their practice would not be information blocking would need to either satisfy the other conditions of the Manner Exception or satisfy a different exception to the information blocking definition. The exceptions to the information blocking definition are voluntary and offer an actor certainty that a practice that satisfies all of the applicable requirements and conditions of an exception at all relevant times will not be considered information blocking.

The *manner exception exhausted* condition is *not* available when exchange is technically feasible and can be accomplished consistent with the Manner Exception, whether because the parties have agreed to terms for fulfillment in the manner requested (*manner requested* condition) or because the requestor has specified and/or agreed to accept access, exchange or use consistent with the Manner Exception's *alternative manner* condition—even if the actor is not accustomed to utilizing the requested manner to support access, exchange, or use of the EHI the requestor seeks, in general or for the same or similar permissible purpose a particular requestor seeks EHI access, exchange, or use. In other words, this condition would *not* be available if a responding actor is able to exchange EHI in the manner requested, and the parties have either reached agreeable terms for such access, exchange, or use; or the requestor has specified and/or agreed to accept such access, exchange or use in an alternative manner consistent with the Manner Exception. We emphasize that nothing about the *manner exception exhausted* condition prevents an actor from providing a requestor with a custom build for access, exchange, or use of EHI. Rather, this condition has been adopted to alleviate actor uncertainty as to whether they must provide the custom build or otherwise be considered to have engaged in information blocking.

We note that in cases where a requestor seeks a specific alternative manner of access, exchange, or use consistent with § 171.301(b)(1), and the actor declines to offer that manner (even if the actor is able to accommodate the requested alternative manner) and instead offers a different alternative manner, the OIG may consider this as a factor in determining whether information blocking has occurred, particularly if the requestor is unable to access, exchange or use the EHI in the offered alternative manner. For example, if a requestor specifies a FHIR-based API as its preferred alternative manner of access, exchange, or use, and the actor is capable of doing so, then the

actor should prioritize fulfilling the request via FHIR, even if the actor is also capable of fulfilling the request via another alternative manner, such as C–CDA document exchange. ONC has consistently maintained this policy approach because it best ensures that EHI is made available where and when it is needed (for further discussion, *see* the ONC Cures Act Final Rule at 85 FR 25877).

Comments. A commenter stated that if an actor is unable to reach agreeable terms with a requestor for access, exchange, or use of EHI, or is technically unable to fulfill a request in the manner requested, and then proceeds to offer one or more alternative manners and the requestor is still not satisfied, then the burden should shift to the requestor to demonstrate and justify why the alternatives proposed by the actor are infeasible or otherwise insufficient to meet their needs. Further, the commenter stated that the actor who received the request should have a duty to respond to the requestor only after receiving a written statement setting forth such justification.

Response. We appreciate the comment. We decline to adopt this suggestion, however, because we find it inappropriate to entirely shift the burden to the requestor. Our information blocking regulatory scheme, consistent with the statutory information blocking definition, supports policy goals of discouraging interference with EHI access, exchange, or use, and encouraging routine, interoperable EHI sharing for permissible purposes consistent with patients' privacy preferences. Although we recognize there is substantial variation in actors' and requestors' circumstances, we do not believe our policy goals would be well served by identifying as ''reasonable and necessary'' any actor's practice of demanding a requestor to justify to the actor their need or preference for a different manner of EHI access, exchange, or use than the actor prefers to offer (42 U.S.C. 300jj–52). A key aim of our information blocking regulatory scheme is to discourage information blocking by actors and make it easier for requestors to obtain, for any permissible purpose, EHI access, exchange, or use in a manner that meets the requestor's needs. The condition, as finalized, requires the actor to offer only two alternative manners, at least one of which is standards-based. It, therefore, allows the actor enough flexibility to avoid developing one-off, unique, custom solutions unless the actor wants to do so. The actor who satisfies the § 171.301 Manner Exception by meeting the *manner requested* condition would not need to also satisfy any condition in the § 171.204 Infeasibility Exception, assuming all requested EHI was provided consistent with the Manner Exception. The § 171.301(a) *manner requested* condition also, we reiterate, allows the actor and requestor to come to any mutually agreeable terms, thereby allowing for those requestors, able and willing to do so, to satisfy any financial incentive the actor would require to develop any requested manner, however unique or one-off, the requestor might want developed.

Comment. At least one commenter stated that this condition should still be available in circumstances where the only applicable option is a ''machine-readable format,'' in other words, § 171.301(b)(1)(iii).

Response. We appreciate the comment. As stated above, we have finalized this condition with a requirement that the actor offer at least two ''alternative manners'' from § 171.301(b)(1)(i)–(iii), one of which must be either the alternative manner in § 171.301(b)(1)(i) or (b)(1)(ii). Because a machine-readable format is the option of last resort, and the least-interoperable of all the alternative manners, we believe that allowing a requestor to offer only a machine-readable format would be at odds with the purpose of the new condition. We note that an actor who is able only to offer access, exchange, or use of EHI in a manner consistent with § 171.301(b)(1)(iii) would not be able to make use of this condition but could still conform its practice to another applicable condition (for example, the *infeasible under the circumstances* condition of the Infeasibility Exception) in order to have certainty that the practice would not constitute information blocking. Moreover, even a practice that does not satisfy any exception does not automatically constitute information blocking. The facts and circumstances of any situation or allegation would need to be evaluated, and whether the practice constitutes information blocking depends on the unique facts and circumstances of the practice.

What counts as a ''substantial number''?

We proposed, as the third factor of the *manner exception exhausted* condition, that the condition would be available only if ''the actor does not provide the same access, exchange, or use of the requested electronic health information to a *substantial number* of individuals or entities that are similarly situated to the requestor.'' In the HTI–1 Proposed Rule, we stated that ''this factor as a whole serves a similar function to the § 171.204(a)(5) (originally codified in § 171.204(a)(3)) *infeasible under the circumstances* condition's factor considering whether the actor's practice is non-discriminatory, and the actor provides the same access, exchange, or use of electronic health information to its companies or to its customers, suppliers, partners, and other persons with whom it has a business relationship'' (88 FR 23870). We noted that the intent of the third factor is to provide a basic assurance that actors would not be able to misuse the § 171.204(a)(4) *manner exception exhausted* condition to avoid supplying some particular requestor(s) with manner(s) of access, exchange, or use of the requested EHI that would be more accurately characterized as generally available than as new, unique, or unusual (88 FR 23870). Given that intent, we stated that the proposed regulatory language of subparagraph (iii) of the condition ''while on its face may seem indefinite and *is* designed to address *any* potential request, is intended to ensure that the actor offers any requestor . . . the same access the actor provides to a substantial number of its customers . . .'' (88 FR 23870). We requested comment on whether we should further define ''substantial number'' for purposes of this condition.

Comments. A few commenters responded to this proposed provision of the *manner exception exhausted* condition. Some suggested we keep the ''substantial number'' flexible and not further define it. One commenter suggested that we set a certain percentage such that an actor providing the same access, exchange, or use to a percentage of its customers would not be able to deny the requestor the same access, exchange, or use and still make use of this condition. Another commenter suggested that even one customer should be enough, because just one customer can constitute the bulk of an actor's business, or one customer can request a more innovative manner that should be made available to all requestors without the use of the condition to cover an actor's practice of denying such access, exchange, or use. One requestor stated that ''substantial number'' was an inappropriate metric for the factor, because ''generally available'' or other terms indicating the state of a product or service are not typically dependent on the number of users but rather the actor's ability to service any requests for such functionality. The same commenter noted that lack of adoption of a given feature may occur for many reasons that have no bearing on the usefulness of the

feature, and therefore any functionality that is considered usable by customers should be considered normal and customary practice, even if only one customer uses it. The commenter expressed concerns that the adoption level could be kept artificially low by telling initial requestors ''no,'' thereby preventing the particular feature from being considered ''generally available'' or similar. Another commenter said that if a functionality is considered usable by customers, then having any customer use it should be considered normal and customary practice, and it shouldn't matter if, for a time, they are the only customer using that feature.

Other commenters supported keeping the term ''substantial number'' without further specifying a specific number. These commenters stated that such an approach allows the right level of flexibility, with one commenter remarking that it permits actors to consider the specific means of access, exchange, or use of EHI contemplated by each request and the specific use case for which the request is made. Another commenter supported ONC's reasoning for not using a fixed number to define ''substantial number,'' referring to the reasoning laid out in the HTI–1 Proposed Rule (which is also discussed below).

Response. We thank the commenters for their feedback and input. We have finalized in § 171.204(a)(4)(iii) the term ''substantial number'' without further specificity. We believe this allows the appropriate amount of flexibility for all actor types, who may have very different numbers of requestors, to satisfy this condition based on what number of requestors is substantial for that actor. As we stated in the HTI–1 Proposed Rule, using ''substantial number'' rather than a specific number is important to recognize variation in actors' operational contexts, including their organizational sizes. What may be a trivial number to a large health IT developer of certified health IT might be an important or consequential (''substantial'') number for a small HIN/HIE (88 FR 23870). In addition, while we believe that calculating a percentage may be helpful to an actor in determining whether it provides a substantial number of customers the requested access, we do not believe establishing a specific percentage would be helpful given the wide variation in the number of customers an actor may have. For example, an actor with a large number of customers who provides the access to dozens of customers might only be providing such access to ten percent of its customers. Further, we did not propose such an approach for consideration.

In response to commenters who suggested we use a specific number, such as one, we note that in some cases, even one customer could be a substantial number, if, for example, it represents a large portion of the actor's deployments or is considered ''generally available'' as part of an actor's line of business (*see* below and 88 FR 23870 for a discussion of ''generally available/general availability''). Simply stating one, or more than one, could be overly broad and end up capturing one-off manners, custom builds, or highly customized deployments that are not easily replicable for another requestor without abandoning open consensus standards or interoperable manners. In other words, we believe that ''substantial number'' is flexible enough to include as few as one customer, when appropriate, and as many as all of a given actor's customers. Further, providing a fixed number could be considered arbitrary.

In response to commenters who noted that if a functionality is used by even one customer, it should be offered even if, for a time, there is only one customer using it. We agree that there may be instances where just one customer is using a particular functionality that is suitable and scalable for use by requestors beyond that one customer. However, in other instances, a functionality may be in use by only one customer because it is a custom build that would be difficult to replicate or scale, or because it is an obsolete product that this one customer continues to find sufficient for their needs. We, therefore, believe setting the standard that an actor cannot meet the *manner exception exhausted* condition if any one customer is using a requested build could too often prevent the condition from applying when a requestor seeks a manner that is not generally available or interoperable. Moreover, in the free market, especially useful features would be expected to attract the notice of developers and their customers, with the best features eventually being adopted by more than one customer.

Finally, in the HTI–1 Proposed Rule preamble, we stated that we chose to structure the § 171.204(a)(4)(iii) factor to align with the concept of whether the manner requested, including involved interoperability elements, is in a stage of development or overall lifecycle that would roughly approximate the ''general availability'' phase of the software release lifecycle, or a conceptually analogous phase for non-software interoperability elements (88 FR 23870). However, we recognize that not all actors are developers, and we intend this condition of the Infeasibility Exception to be available for all types of § 171.102 actors. As we stated in the HTI–1 Proposed Rule, health care providers, for example, do not typically develop software for the market and, in our observation, are likely to characterize components of their health IT systems in more operational terms—such as what has ''gone live'' in their particular implementation—than in software release lifecycle terms. We believe avoiding the specific lifecycle term also avoids potential for misunderstandings among actors and requestors, or for gamesmanship on the part of actors, around when different actors consider a particular interoperability element to enter or to be withdrawn from ''general availability'' as the term is widely used in the software sector. We finalize ''substantial number'' with the same analysis and guidance found in the HTI–1 Proposed Rule (see 88 FR 23870 through 23871).

What does ''provide'' mean in this context?

Comments. We received three comments requesting clarification of the term ''provides'' as used in the *manner exception exhausted* condition. A couple of commenters asked ONC to clarify that this condition includes only current methods of sharing data, and not former, replaced, or outdated methods of exchange. Another commenter noted that clarification of the term ''provide'' in this context is even more important, given other proposals related to information blocking that also include concepts like ''making available'' or ''providing.'' One comment speculated the definition of *provide* included in the HTI–1 Proposed Rule at § 171.102 (information blocking definitions) was included for purposes of this condition, indicating that it was unclear why the definition was proposed and that if finalized in the proposed form, it may add confusion to the provisions of the conditions of information blocking exceptions in general.

Response. We thank commenters for their feedback. We use the word ''provide'' in § 171.204(a)(4)(iii) without further definition. We unintentionally included a definition of *provide* in § 171.102 (information blocking definitions) in the HTI–1 Proposed Rule. We have not finalized any definition of the word ''provide'' in § 171.102. Further, we emphasize that the definition of *provide* finalized in § 170.102 (health information technology certification program

definitions) is not applicable for 45 CFR part 171.

We offer the following points of clarification specific, and limited in effect, to our use of the word ''provide'' in § 171.204(a)(4)(iii). First, as we stated in the preamble of the HTI–1 Proposed Rule, our use of ''provide'' in the present tense is both precise and deliberative. This factor tests for whether the actor currently provides the same manner to a substantial number of individuals or entities who are similarly situated to any given requestor. Looking only at what the actor *currently* provides excludes manners that are nearing or have exceeded the end of their supported life cycles (88 FR 23870). We recommend reviewing the examples in the HTI–1 Proposed Rule related to ''provide'' in context of § 171.204(a)(4)(iii) and note that they remain appropriate as further explanation of our finalized policy (88 FR 23870).

How should ''similarly situated'' be determined?

In the HTI–1 Proposed Rule, we discussed that the concept of ''similarly situated'' is familiar because we also use the phrase in the Fees Exception (§ 171.302) and Licensing Exception (§ 171.303). We noted that it would serve here, as it does there, to indicate that different specific individuals or entities within a class of such individuals or entities who are similarly situated to one another should be treated in a consistent and non-discriminatory manner (88 FR 23871). We also stated that it is not our intent for the ''individuals or entities that are similarly situated to the requester'' criteria of this new proposed condition to be used in a way that differentiates the same access to EHI simply based on the requestor's status, such as individual (*e.g.,* a patient) or entity (*e.g.,* a healthcare system) (88 FR 23871).

Comments. A few commenters requested that ONC provide more specific information on the types of characteristics that would designate entities as similarly situated and provide examples or guidance on ways for actors to easily group and document that entities are similarly situated. One commenter expressed concern about the lack of clarity related to the ''similarly situated'' clause. Another commenter argued that the term was inappropriate and what should matter is not the requesting entity's circumstances but its intended purpose of use for the requested interoperability functionality, whether the use aligns with what the functionality was designed to support, and whether the use requires any substantially new development work.

Response. We appreciate the comments and have adjusted the finalized policy to address commenters' concerns. As we noted in the preamble to the HTI–1 Proposed Rule, ''similarly situated'' in the *manner exception exhausted* condition's third factor was meant to function in a fashion *similar* to the non-discrimination provisions in the Fees and Licensing Exceptions (88 FR 23871). However, with the use of the term ''similarly situated,'' we were proposing to permit certain discrimination of requestors based on the similarity of their situations to those already being provided access, exchange, or use. As a comparison, we did not permit any discrimination under a parallel construction of one of the factors used for the analysis under the *infeasibility under the circumstances* condition of the Infeasibility Exception (*compare* ''Whether the actor's practice is non-discriminatory and the actor provides the same access, exchange, or use of electronic health information to its companies or to its customers, suppliers, partners, and other persons with whom it has a business relationship;'' 45 CFR 171.204(a)(5)(i)(D)).

We provided guidance in the HTI–1 Proposed Rule on our thinking of how a determination of similarly situated would work. We first provided an example of categorizing requestors into ''similarly situated'' categories based on the size of the healthcare entity. We then specified that even within these different categories, requestors would not be treated differently based on extraneous factors, such as whether any of them may be competitors of the responding actor or may obtain more of their health IT from the actor's competitors than from the actor (88 FR 23871). Finally, we noted that it was not our intent for the ''individuals or entities that are similarly situated to the requester'' criteria to be used in a way that differentiates the same access to EHI simply based on the requestor's status, such as individual (*e.g.,* a patient) or entity (*e.g.,* a healthcare system).

Based on comments received and further consideration of our proposal and examples, we have revised the condition to exclude certain factors from a similarly situated determination and are providing additional clarification and guidance. Consistent with the HTI–1 Proposed Rule, we clarify that ''similarly situated'' cannot be used to discriminate against requestors based on whether the requestor is a competitor of the actor or whether the requestor will or might use the requested access, exchange, or use in a way that facilitates competition with the actor. Similarly, as we noted above and in the HTI–1 Proposed Rule (88 FR 23871), an actor cannot discriminate in providing a form of access, exchange, or use of EHI that it currently provides to a substantial number of individuals or entities solely based on the requestor's status. In this regard, we are specifically clarifying in regulation text (§ 171.204(a)(4)(iv)) that such statuses include requests by individuals, as we define that term in § 171.202(a), and the health care provider type and size. Regarding health care provider type (*e.g.,* radiology specialty practice or long-term post-acute care facility) and size, we believe further clarity is necessary based on comments and the example we provided in the HTI–1 Proposed Rule and recited above. While the example in the HTI–1 Proposed Rule may have suggested that size groupings are acceptable, we clarify that such groupings as ''similarly situated'' would be appropriate in terms of administering costs and licensing agreements under the respective Fees and Licensing Exceptions but would not be appropriate for discriminating in actually providing access, exchange, or use of EHI that the actor provides to a substantial number of individuals or entities. Costs associated with providing access, exchange, or use of EHI or costs associated with licensing interoperability elements, can logically vary based on the size of the entity, so it makes sense to use this category for the Fees and Licensing Exceptions. However, we don't see a similar reason to discriminate based on the entity's size when an actor seeks to satisfy this condition of the Infeasibility Exception because if an actor already provides such access to a substantial number of entities, there is not a parallel correlation that would make it infeasible to provide such access to a ''differently'' sized requestor.

As an example, if a solo practitioner requests access, exchange, or use of certain EHI in the same manner that an actor provides such access, exchange, or use of the same EHI to a large hospital system, then the actor would not be able to discriminate based on the difference between the requestors (large hospital system versus solo practitioner) and still use this condition to cover the practice.

Overall, these adjustments are responsive to comments and provide further clarity for the concept of ''similarly situated'' as it applies to this condition under the Infeasibility Exception.

Other Comments

Comment. One commenter asked that actors be required to report any requests that they have rejected.

Response. We appreciate the comment but decline to finalize such a policy at this time as we did not propose such an approach.

Comment. A few commenters asked ONC to explain why the first requirement of this new condition restates ''technical inability'' as the reason for the infeasibility under the Manner Exception when the Manner Exception itself provides that an actor must fulfill the EHI request in the manner requested ''unless the actor is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request in the manner requested.'' A commenter asked ONC to explain how this alternative requirement in the *manner exception exhausted* condition is materially different from the options for meeting the first requirement.

Response. There is no substantive difference between the ''technical inability'' under the Manner Exception and this new condition. However, this requirement has been restated as it falls under a new condition and under a different exception. ONC's intent in including the technical infeasibility requirement is to ensure that an actor who cannot, for technical reasons, fulfill a request for any access, exchange, or use of EHI in any manner requested is able to use this condition (provided all other relevant provisions are also met) *and* an actor who *does* have the technical capability to provide access, exchange, or use of EHI in the manner requested but cannot reach agreeable terms with the requestor may *also* make use of this new condition (provided all other relevant provisions are also met). In other words, an actor who can technically fulfill the request but cannot reach agreeable terms can still make use of this condition, so long as all other relevant provisions are met.

Comments. We received many comments in response to this new condition (and in response to other proposals in the HTI–1 Proposed Rule) advocating we review or revise paragraph (b) of the Infeasibility Exception, which requires an actor that does not fulfill a request for access, exchange, or use of EHI consistent with any of the conditions in paragraph (a) of § 171.204 ''provide to the requestor in writing the reason(s) why the request is infeasible'' within ten business days of receipt of the request. One commenter noted that requests often come in without the needed level of detail, meaning the developer must ask questions and wait for answers from the requestor before determining whether the request is feasible. In such instances, the commenter stated, the timeliness rests on the requestor and not the responding actor, and therefore a ten-day time frame is insufficient. The commenter further contends that the ten-day clock should ''toll'' until sufficient information about the request has been received. Other commenters expressed agreement that ten days was too short, too inflexible, and unrealistic. Another commenter asked ONC to clarify that where an actor intends to apply the *manner exception exhausted* condition of the Infeasibility Exception that the ten-day time frame begins only after the actor and requestor have not been able to agree on an acceptable alternative manner under the Manner Exception. Another commenter noted that the ten-day time frame was so unrealistic as to preclude the use of the exception in situations where it would otherwise be relevant.

Response. While we appreciate the comments, we did not propose any changes to the ten-day time frame in the HTI–1 Proposed Rule and are not finalizing any changes to paragraph (b) of § 171.204 in this final rule. We may consider these comments in relation to future regulatory action and guidance.

2. TEFCA Manner Exception

In the HTI–1 Proposed Rule, we proposed to add in § 171.301(c) a *TEFCA manner* condition to the proposed revised and renamed Manner Exception codified in 45 CFR 171.301. The proposed condition was stated as follows: ''If an actor who is a QHIN, Participant, or Subparticipant offers to fulfill a request for EHI access, exchange, or use for any purpose permitted under the Common Agreement and Framework Agreement(s) from any other QHIN, Participant, or Subparticipant using Connectivity Services, QHIN Services, or the specified technical services in the applicable Framework Agreement, then: (i) The actor is not required to offer the EHI in any alternative manner; (ii) Any fees charged by the actor in relation to fulfilling the request are not required to satisfy the exception in § 171.302; and (iii) Any license of interoperability elements granted by the actor in relation to fulfilling the request is not required to satisfy the exception in § 171.303'' (88 FR 23872).

In proposing this condition, we sought to offer actors certainty that fulfilling, or even attempting to fulfill, requests for EHI using Connectivity Services, QHIN Services, or the specified technical services in the applicable Framework Agreement (''TEFCA means'') would satisfy the Manner Exception when an actor and requestors are parties to the Common Agreement or a Framework Agreement under the Common Agreement. As proposed, this would have been the case even when the EHI may have exceeded the minimum data classes and elements *required* by the Common Agreement as of the date a particular request is fulfilled, assuming the TEFCA means could support the requested access, exchange, or use of the EHI. We stated that the proposed condition could be satisfied regardless of whether the requestor initially requested access, exchange, or use via TEFCA means or some other manner (88 FR 23872). We noted that another important feature of the proposal was that it could be satisfied by the actor either fulfilling or *offering to fulfill* the requestor's request for EHI, again, assuming the TEFCA means could support the requested access, and exchange, or use of the EHI. We stated that the approach aligns with the Cures Act's goals for interoperability and the establishment of TEFCA by acknowledging the value of TEFCA in promoting access, exchange, and use of EHI in a secure and interoperable way.

We stated that the proposed condition would identify as ''reasonable and necessary'' an actor's practice of prioritizing use of TEFCA means, in lieu of other feasible manners, for all EHI for which access, exchange, or use can be supported by TEFCA means for both the actor and requestor, so long as the requestor is a TEFCA entity (QHIN, Participant, or Subparticipant) and the purpose is permitted under the TEFCA governing agreements. This would be true regardless of whether the request is initially made through TEFCA means or otherwise; and regardless of whether all of the particular data classes or exchange purposes are yet required by TEFCA's governing agreements to be returned in response to a TEFCA request (88 FR 23873). The condition was designed to provide a clear, efficient regulatory path to prioritize exchange amongst QHINs, Participants, and Subparticipants in TEFCA using TEFCA means of sharing any and all EHI that TEFCA means can support.

We requested comment on this proposal and received a substantial number of responses from commenters. These comments are summarized and addressed below.

Summary of Finalized Policy

For the reasons explained below, rather than include this condition as part of the Manner Exception, we have

finalized a new subpart to the information blocking exceptions—Subpart D, ''Exceptions That Involve Practices Related to Actors' Participation in The Trusted Exchange Framework and Common Agreement (TEFCA).'' The new subpart consists of three sections, § 171.400 ''availability and effect of exceptions,'' which mirrors §§ 171.200 and 171.300, stating that a practice shall not be treated as information blocking if the actor satisfies an exception to the information blocking provision as set forth in this subpart D by meeting all applicable requirements and conditions of the exception at all relevant times. We have reserved § 171.401 for definitions in future rulemaking and reserved § 171.402 for future use as well. At § 171.403, we finalized a TEFCA Manner Exception that is based on the *TEFCA manner* condition proposed in the HTI–1 Proposed Rule.

Similar to the proposed condition, the new TEFCA Manner Exception (§ 171.403) provides that an actor's practice of limiting the manner in which it fulfills a request for access, exchange, or use of EHI to providing such access, exchange or use only via TEFCA will not be considered information blocking when the practice follows these conditions:

(a) The actor and requestor are both part of TEFCA;

(b) The requestor is capable of such access, exchange, or use of the requested EHI from the actor via TEFCA;

(c) The request for access, exchange, or use of EHI is not via the standards adopted in 45 CFR 170.215 or version approved pursuant to 45 CFR 170.405(b)(8); and

(d) Any fees charged by the actor and the terms for any license of interoperability elements granted by the actor in relation to fulfilling the request are required to satisfy, respectively, the Fees Exception (§ 171.302) and the Licensing Exception (§ 171.303).

The first condition, in § 171.403(a), that the actor and requestor are both part of TEFCA, simply means that *both* the actor *and* the requestor must be either a QHIN, Participant, or Subparticipant, as those terms are defined in the Common Agreement as published at 88 FR 76773. For brevity, in the preamble, we will refer to these three terms collectively as ''TEFCA entities'' or a ''TEFCA entity.'' This exception will not be available in any situation where the actor, *or the requestor,* is not a part of TEFCA.

The second condition, in § 171.403(b), requires that the requestor *must* be capable of receiving (accessing, exchanging, or using, depending on the requestor's request) the EHI from the actor, via TEFCA. In the Proposed Rule, we used the term ''TEFCA means'' to describe fulfilling requests for EHI using Connectivity Services, QHIN Services, or the specified technical services in the applicable Framework Agreement (88 FR 23872, as those terms are defined at 88 FR 76773). In this final rule and in the regulation text, we describe an actor's practice of responding to a request to access, exchange, or use EHI ''via TEFCA'' to indicate that an actor may use any of the services described by ''TEFCA means'' consistent with the terms that both the actor and requestor separately agreed to for access to such TEFCA means, and consistent with the other conditions of the exception.

As finalized in § 171.403(b), the exception's condition for responding to requests for EHI that the requestor can obtain from the actor via TEFCA uses ''via TEFCA'' to communicate that the actor makes the EHI available, and the requestor is able to obtain the requested access, exchange, or use of the requested EHI using—what we referenced in the HTI–1 Proposed Rule as making EHI available through ''TEFCA means'' (88 FR 23872). This includes where Participants and Subparticipants may be exchanging EHI within the same QHIN or across different QHINs. In cases where the requestor is *not* capable of accessing, exchanging, or using the EHI via TEFCA, for example because the requestor does not support such exchange methods or its QHIN does not, an actor would not be able to make use of this exception.

The third condition, in § 171.403(c), excludes requests from the exception where the requestor seeks to access, exchange, or use EHI via the ''Application Programming Interface Standards,'' (or API standards) (45 CFR 170.215) adopted by ONC on behalf of the Secretary or another version of those standards approved pursuant to the ''Standards Version Advancement Process'' (45 CFR 170.405(b)(8)) under the ONC Health IT Certification Program. When a requestor seeks to access EHI via those API standards (essentially FHIR-based standards), an actor *cannot* use this exception. In other words, the third condition functions as a carve-out in that the exception is not available if the requestor requested access, exchange, or use of EHI via the API standards.

The fourth and final requirement for this condition, in § 171.403(d), states that any fees an actor charges, and any licensing terms an actor sets, must comply with the Fees Exception (§ 171.302) and the Licensing Exception (§ 171.303). This exception in § 171.403 would not be available in any situations where all four of these conditions are not satisfied.

Rather than finalize the proposed definitions, in order to maintain consistency between the most current version of the Common Agreement and this regulation, we have decided to refer to the definitions used in the Common Agreement (88 FR 76773) for the terms used in this exception. The relevant definitions are similar to, or the same as, the terms we proposed to define in the proposed *TEFCA manner* condition. For example, when we refer to Framework Agreement(s), we mean any one or combination of the Common Agreement, a Participant-QHIN Agreement, a Participant-Subparticipant Agreement, or a Downstream Subparticipant Agreement, as applicable. A Qualified Health Information Network (QHIN) is, as defined in the most recent version of the Common Agreement, a health information network (as defined in § 171.102) that is a U.S. entity that has been designated by the Recognized Coordinating Entity (RCE) and is a party to the Common Agreement countersigned by the RCE. Both Participant and Subparticipant are defined as they are in the Common Agreement (88 FR 76773). In some cases, such as with the term Connectivity Services, the definition proposed is different from the most recent version of the Common Agreement, where it is defined as the technical services provided by a QHIN consistent with the requirements of the then-applicable QHIN Technical Framework and pursuant to the Common Agreement with respect to all Exchange purposes. The Common Agreement also defines Individual Access Services (IAS) as the services provided to an Individual by a QHIN, Participant, or Subparticipant that has a direct contractual relationship with such Individual in which the QHIN, Participant or Subparticipant, as applicable, agrees to satisfy that Individual's ability to access, inspect, or obtain a copy of that Individual's Required Information using TEFCA Exchange. We decided to reserve 171.401 for possible future use to incorporate these definitions into the regulatory framework.

Timeliness of Exception

Comments. Some commenters stated that it would be premature to adopt this proposal. Commenters noted that TEFCA is in its early stages and has not yet launched. Others suggested ONC take a ''wait and see'' approach, monitor TEFCA deployments for utility, completeness, timeliness, ease of access,

security, privacy, transparency, and consumer participation, and then finalize an exception only if real world experience demonstrates a need. A commenter noted that TEFCA is a voluntary program that does not support the full breadth of use cases for EHI, and that such an exception will designate other pathways as ''less interoperable'' even if they have equal or greater utility compared to exchange through TEFCA. Another commenter appreciated ONC's support for greater interoperability, but also stated it was too soon to establish this condition because it could result in less sharing of information in the early stages of TEFCA's development. The commenter suggested, as an alternative, that TEFCA-based exchange should be included as a preferred approach to sharing EHI, but not in a way that enables an actor to deny a request if the requestor cannot receive it via TEFCA-based exchange.

Response. We appreciate the feedback. The policy as proposed (88 FR 23873) and as finalized in the new TEFCA Manner Exception is only available when both the actor and the requestor are in TEFCA, which we believe eliminates the concerns about the timeliness of identifying as reasonable and necessary the practices that satisfy the exception. Entities will join TEFCA with the expectation that they will exchange EHI using TEFCA when possible. This exception reinforces that practice. No actor is required to join TEFCA, so those that do so will do so with the knowledge that this exception is available in certain circumstances. As a voluntary exception, no actor is required to make use of the exception—which we believe further negates the timeliness concerns. In addition, an actor will *not* be able to use this exception if, for whatever reason, the requestor is not capable of accessing, exchanging, or using the requested EHI via TEFCA. In such cases, an actor would need to provide the EHI in the manner requested, or in an alternative manner agreed upon with the requestor or use another exception to cover the practice to attain certainty that the actor's practice will not be considered information blocking.

Fees and Licensing Terms Concerns

Comments. Many commenters expressed concern that we did not propose to apply the restrictions found in the Fees Exception (§ 171.302) and the Licensing Exception (§ 171.303) to this condition. These commenters contended that, without such application, actors would be able to charge outrageous fees or set unreasonable licensing terms for interoperability elements. Other commenters noted that such fees could interfere with an individual's right to access their EHI. A couple of commenters asserted that, as proposed, the condition could result in applications that charge patients for their services as the only realistic way for patients to get their EHI. Some commenters further asserted that because the only fees that are prohibited in the Common Agreement are fees charged between QHINs, Participants and Sub-participants would be able to charge fees for exchange of EHI that would not need to satisfy the Fees Exception.

Response. We appreciate the comments and believe the commenters raised valid concerns. In fact, when proposing the *TEFCA manner* condition, we mistakenly assumed that all actors participating in TEFCA would have *already* reached overarching agreements on fees and licensing such that there would be no need for application of the Fees and Licensing Exceptions. (*See* 88 FR 23872, ''[the proposal] facilitates an actor reaching agreeable terms with a requestor to fulfill an EHI request and acknowledges that certain agreements *have been reached* for the access, exchange, and use of EHI (for example, by using standards consistent with the Common Agreement or applicable flow-down Framework agreements that the actor and requestor have agreed to abide by)'' (emphasis added)). In fact, the Common Agreement is silent on fees except to forbid QHINs from charging fees to other QHINs. Therefore, to correct our misunderstanding and in consideration of comments, we have finalized the exception to include that any fees charged by the actor, and any licensing of interoperability elements, must satisfy the Fees Exception (§ 171.302) and the Licensing Exception (§ 171.303). It was never our intent to permit fees or licensing agreements that would not satisfy the information blocking regulations, either by being agreed to ahead of time, as we presumed, or by satisfying the Fees and Licensing Exceptions.

Concerns Regarding EHI Accessibility and Fees for Individuals

Comments. Many requestors expressed concerns that the proposed TEFCA condition would interfere with an individual's access to their own EHI. One commenter stated that the condition could be used to elect out of participating in Individual Access Services in a national network capacity. The commenter stated that while responding to individual requests via TEFCA is required (by the Common Agreement), QHINs are not required to initiate support for Individual Access Services. One commenter expressed concerns that the exception will make it more difficult for patients to get provider and payer data, and that patients who do not understand how networks function will be disadvantaged compared to others. A few commenters expressed concern about patient matching within the TEFCA network. One commenter expressed concerns about sensitive data, citing reproductive health care as an example, and how a patient could control access to such EHI. Some commenters indicated they were especially concerned with patient privacy and the ability for applications to charge for access to patient data or possibly ''traffic'' EHI through ''dark data'' exchanges. A commenter encouraged ONC to focus on FHIR-based interoperability. A few commenters expressed concerns that the proposal would allow actors to charge individuals for access to their own data. Another commenter expressed significant concerns that the exception would permit charging fees to Individual Access Services (IAS) providers who are looking to access healthcare data on behalf of individuals.

Response. We appreciate the comments. Consistent with our proposal, the policy, as finalized, is applicable only when both the actor and the requestor are part of TEFCA (88 FR 23873, *see also* 88 FR 23917–23918). We would like to assure commenters that this exception cannot be used in any case when an individual is requesting EHI, because an individual cannot be a QHIN, Participant, or Subparticipant under TEFCA. If the individual is using TEFCA's Individual Access Services to query for or retrieve EHI via TEFCA instead of seeking to access, exchange, or use EHI directly from their health care provider's portal or FHIR APIs, then the QHIN, Participant, or Subparticipant, in its role as an IAS provider, would be querying via TEFCA, *not* the individual. Furthermore, as described previously, the finalized exception includes the requirement that any fees charged for the access, exchange, or use of the EHI must satisfy the Fees Exception (§ 171.302), which specifically prohibits charging a patient (including a third-party app on the patient's behalf) for API or other electronic access to the patient's EHI (§ 171.302(b)(1) and (2)). Regarding patient privacy, all § 171.102 actors are required to protect patients' privacy and restrict the access, exchange, and use of

EHI as required by all applicable law, including, but not limited to, the HIPAA Privacy Rule for actors to whom the HIPAA Privacy Rule applies.

Patient matching within TEFCA is addressed by applicable policy and technical procedures as well as associated agreements under TEFCA. For purposes of information blocking, any actor who receives a request for access, exchange, or use of EHI that the actor knows, or reasonably suspects, is misidentified or mismatched and who seeks certainty as to the conditions under which they can withhold such EHI without engaging in information blocking will want to consult the Preventing Harm Exception in 45 CFR 171.201, which recognizes this type of risk in § 171.201(c)(2).

Concerns Regarding Interoperability and FHIR APIs

Comments. Many commenters expressed concerns with the limited manner of exchange initially available in TEFCA and noted that when TEFCA officially launches, the Common Agreement will require only IHE document-based exchange. Commenters stated that restricting TEFCA entities to IHE document-based exchange would limit the use of EHI exchanged in that manner, would limit interoperability by not requiring the use of modernized exchange protocols like FHIR, and could even disincentivize joining TEFCA. Others noted that our proposal would push actors to one exchange mechanism over another, which would remove choice and optionality and could potentially eliminate or discourage use of other exchange options, such as FHIR APIs, that may be preferable for some use cases. A few commenters noted that many health IT developers of certified health IT plan to connect their customers to TEFCA such that their customers will have to actively choose to opt out. Commenters expressed concerns that most actors will likely be Participants or Sub-participants and, therefore, ''subject to this exception.'' As a result, one of these commenters stated that most of the information blocking regulations would be folded into the TEFCA framework, which lags behind today's use of FHIR APIs.

Other commenters noted that requestors may have practical reasons to ask for EHI in ways other than what TEFCA supports. Commenters encouraged ONC to advance support for HL7 FHIR within TEFCA as quickly as possible to allow third-party applications to access data more easily on behalf of individuals. A few commenters noted that section 4003(a) of the Cures Act defined interoperability as health information technology that enables the secure exchange of electronic health information with, and use of electronic health information from, other health information technology without special effort on the part of the user. The commenters claimed that the proposed TEFCA condition would require special effort on the part of the user, particularly with the use of IHE document protocol. Other commenters stated that entities should be able to choose the best interoperability mechanisms and request data in any format the current source can reasonably support using an exchange mechanism both can support. A commenter stated that, because there may be a delay before TEFCA widely implements the use of FHIR for all of the stated ''exchange purposes,'' organizations should be able to negotiate for the manner of access that best suits their requirements. In particular, the commenter stated that organizations should be allowed to prioritize using EHR systems' SMART on FHIR patient API endpoints, and for population-level use cases, bulk FHIR export, even if TEFCA supports access to such EHI in another manner.

Response. We thank the commenters for their feedback. Currently, TEFCA includes IHE document-based exchange, but publicly available documents note that FHIR exchange is a TEFCA priority and is planned for availability in 2024. IHE document-based exchange is a longstanding standard for exchanging EHI. For example, organizations supporting health information exchange nationally (*e.g.,* CommonWell Health Alliance, eHealth Exchange, Carequality) generally use IHE profiles such as Cross-Community Patient Discovery (XCPD) [258] and Cross-Community Access (XCA) [259] to enable clinical document exchange between disparate communities.[260] However, as many commenters pointed out, FHIR-based exchange has certain advantages over IHE document-based exchange. Over time, QHINs, Participants, and Subparticipants may well be required to support broader uses of FHIR-based exchange, but it is also likely that many Participants and Subparticipants will continue to use document-based exchange instead of FHIR-based exchange for several transition years.[261] In addition, the information blocking exceptions are all voluntary and are not ''required'' of any actor. The exceptions serve to offer certainty to actors that by conforming a practice to the conditions of an exception, such practice will not constitute information blocking. A Participant or Subparticipant in TEFCA is not ''subject to'' any exceptions, but if such entity is an actor (as defined in § 171.102), the new finalized exception would be available along with all the other exceptions.

In consideration of both our stated goal to incentivize TEFCA participation and comments suggesting that ONC should be promoting the use of FHIR-based APIs (for example, the standards codified in 45 CFR 170.215, ''Application Programming Interface Standards''), we have limited the finalized exception's availability. Specifically, in instances where an actor that is part of TEFCA receives a request to access, exchange, or use EHI via the API standards adopted in 45 CFR 170.215, including updated versions of such standards as may be approved for voluntary use in the ONC Health IT Certification Program pursuant to 45 CFR 170.405(b)(8), the Standards Version Advancement Process, the actor *cannot* meet the finalized TEFCA Manner Exception. We finalized this policy in § 171.403(c), providing a limitation on the use of the exception in that it does not apply to a request for access, exchange, or use of EHI via the standards adopted in 45 CFR 170.215, including version(s) of those standards approved pursuant to 45 CFR 170.405(b)(8). This approach ensures that requestors seeking to access, exchange, or use EHI via FHIR-based APIs can request such access and be assured that an actor cannot use the TEFCA Manner Exception to limit the manner in which it fulfills the request to only via TEFCA. As many commenters noted, FHIR APIs advance interoperability to a greater degree than IHE document-based exchange, which is a currently permitted exchange mechanism under TEFCA. With the goals of the proposed condition to acknowledge agreements reached by parties and to promote both interoperability and TEFCA adoption (88 FR 23872–23873), the FHIR-based API limitation in § 171.403(c) is necessary to achieve these goals.

[258] IHE Cross-Community Patient Discovery (XCPD) profile—available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: *https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf.*

[259] IHE Cross-Community Access (XCA) profile—available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: *https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf.*

[260] *https://rce.sequoiaproject.org/wp-content/uploads/2022/01/QTF_0122.pdf.*

[261] *https://www.healthit.gov/buzz-blog/tefca/coming-in-hot-tefca-will-soon-be-live-and-add-support-for-fhir-based-exchange.*

It is crucial to note that an actor (*e.g.,* a health IT developer of certified health IT) that participates in the ONC Health IT Certification Program cannot simply ''turn off'' API capabilities, outside of TEFCA, to avoid offering such access, exchange, or use to a requestor. Any developer that has chosen to participate in the Program is subject to the Conditions of Maintenance and Certification requirements in subpart D of 45 CFR part 170. The API Condition and Maintenance of Certification requirements in § 170.404 apply to health IT developers that certify health IT to FHIR-based API certification criteria. Such developers would not be compliant with the API Condition and Maintenance of Certification requirements if they do not, among other requirements, publish APIs and allow EHI access, exchange, and use through the APIs. Any actor with certified health IT who has deployed ''certified API technology'' (as defined in § 170.404(c)) or other API technology using the standards and implementation specifications adopted in § 170.215, who disables, disconnects, or otherwise ''turns off'' such API technology or requestors' connections in order to avoid offering such access, exchange, or use after joining TEFCA would do so explicitly outside the applicability of the TEFCA Manner Exception finalized in § 171.403 and such practices could constitute information blocking.

The TEFCA Manner Exception, as finalized, is not in conflict with the PHSA section 3000(9) definition of ''interoperability'' or with other ONC regulations. The exception only applies to entities that choose to voluntarily participate in TEFCA and agree to the interoperability means available under TEFCA, while also preserving the availability of interoperable FHIR APIs to requestors for the access, exchange, and use of EHI.

In sum, we believe that the proposed approach would not have led to most of the negative consequences for FHIR API adoption theorized by commenters. However, to address such confusion and concern and continue to incentivize TEFCA participation, in § 171.403(c), we have finalized the explicit limitation condition within the exception to remove any doubt about perceived conflicts between TEFCA and FHIR API adoption. ONC has been and will continue to be at the forefront of driving both TEFCA and FHIR API adoption across the industry and the Federal Government.

Comments. Many commenters noted that some EHI requestors who will likely be part of TEFCA may not have the technical capability to make requests or receive responses for certain permitted but optional exchange purposes.

Response. In situations where a requestor does not support the capability to make or receive requests or perform other transmissions for certain Exchange Purposes (including those that do not require a response), the TEFCA Manner Exception would not be available because the requestor would not have such access, exchange, or use of the EHI consistent with the *requestor capability* condition in paragraph (b) of § 171.403.

Comments. Some commenters stated that the proposed TEFCA manner condition could interfere with state reporting requirements, because, for example, some states require payers to exchange data within a specified network based on existing federal rules. One commenter stated that the condition risked discriminating against mechanisms of exchange and interoperability that are feasible and even required to be used by regional or local authorities. Another commenter stated that the inclusion of this exception demonstrates that there may be conflicting or confusing mandates under different federal programs, making compliance with information blocking regulations more difficult. The commenter urged ONC to continue to review how all federal and state laws, regulations, and programs interact to relieve the unnecessary burden of varying requirements that may not align. A commenter stated that the proposed condition risks discriminating against exchange mechanisms and interoperability pathways that are otherwise commercially and technically feasible, and in some cases, required under law. The commenter noted that a diversion of such exchanges to TEFCA would result in the loss of useful information that should be added to the patient's record to provide additional context for clinical care.

Response. We appreciate the comments. We remind commenters that the exceptions exist as a voluntary means for actors to gain assurance that their practice(s) does not constitute information blocking; and similarly, participating in TEFCA is voluntary. Compliance with an exception set forth in subpart B, C, or newly finalized D of 45 CFR part 171, would mean that an actor's practice does not meet the definition of information blocking in § 171.103. However, this would not, in or of itself, immunize the actor from any other consequences to which they are subject to for violating, ignoring, or otherwise failing to comply with other applicable laws.

In response to concerns that the exception risks discriminating against exchange mechanisms and interoperability pathways that are otherwise commercially and technically feasible, we note that a requestor can request EHI in any manner, and an actor may seek to satisfy the *manner requested* condition of the Manner Exception (§ 171.301(a)) and respond in that manner, if the actor and requestor can come to agreeable terms for the access, exchange, and/or use of the particular EHI. In such instances, the terms of the agreement need not satisfy the Fees Exception (§ 171.302) or the Licensing Exception (§ 171.303), and would meet the *manner requested* condition of the Manner Exception (§ 171.301). Using the TEFCA Manner Exception is voluntary, and in cases where a requestor would be unable to use its preferred exchange method it could negotiate with the actor under the *manner requested* condition (§ 171.301).

The TEFCA Manner Exception does not require actors to use TEFCA to meet public health reporting requirements under other applicable laws. Similarly, the TEFCA Manner Exception does prohibit the use of other exchange methods. Rather, it acknowledges an exchange method (manner) that both the actor and requestor have voluntarily chosen to use, and are capable of using, as a method that would be reasonable and necessary for purposes of not being considered information blocking. As noted above, actors are still responsible for their other legal obligations, such as under state law.

Regarding the concern about exchanging requested EHI only via TEFCA when doing so would result in the loss of some of the responsive EHI that the actor has and can (consistent with applicable law and patient privacy preferences) make available to the requestor for the purpose(s) applicable to the request, then this exception is not available to the actor. The finalized TEFCA Manner Exception applies only to the EHI that the actor is actually able to make available for access, exchange, or use via TEFCA and that the requestor is capable of accessing, exchanging, or using, as applicable, via TEFCA (§ 171.403(b)).

Incentivizing TEFCA Participation

Comments. Some commenters encouraged ONC to consider that while this condition will be useful for those already in TEFCA, it will not meaningfully incentivize participation in TEFCA. As an example, some state agencies that do not have the technological resources to adopt TEFCA technical services will contract with a

third-party entity and end up passing the cost of the contracts on to others, including health care providers. Some commenters asked for a ''safe harbor'' period to allow participants to fully embrace TEFCA. A commenter expressed concern that the condition will discourage third-party apps from joining TEFCA because they will have more flexibility to request data outside of TEFCA.

Many other commenters, however, agreed that the proposal will incentivize and accelerate use of the available, interoperable, and secure TEFCA technical services by TEFCA entities. Commenters noted that the proposal would reinforce the transition to standards-based exchange and prevent actors from unnecessarily devoting limited time and resources to fulfilling burdensome, customized solutions. A commenter appreciated strong regulatory incentives to join TEFCA.

A commenter expressed concern that the proposed condition could be used to coerce use of TEFCA or be used as a defense to evade fulfilling a request for access, exchange, or use of EHI when the requestor does not use TEFCA for a permitted purpose for data beyond USCDI v1. Another commenter suggested ONC use the policy exactly that way and require only the actor be a part of TEFCA. The commenter contended that if the requestor can receive the access, exchange, or use of EHI via TEFCA and is eligible to join TEFCA, the actor should only be required to offer EHI via TEFCA in order to satisfy the exception (in other words, make the requestor join TEFCA to get the requested access, exchange, or use of EHI).

Response. We appreciate the comments. We recognize that this condition incentivizes, to differing degrees for different actors, joining TEFCA, and that not all entities will be ready, willing, or able to join TEFCA as soon as the first technical services under TEFCA go ''live.'' However, we do not agree that a safe harbor period is needed, as both joining TEFCA and using the exceptions are voluntary and function only to offer actors certainty that their practices that meet all relevant conditions of an exception, at all relevant times, will not constitute information blocking.

At this time, we decline to use this exception as a means to propel requestors into joining TEFCA or to justify, to us or to actors, why they are not yet TEFCA entities. Such an approach is beyond what our proposal or finalized exception is intended to achieve and may actually undermine and frustrate the intent of the information blocking statute and implementing regulations. We also recognize the concern that some actors may wish to use the exception to evade fulfilling a request for access, exchange, or use of EHI when the requestor does not use TEFCA for a permitted purpose beyond USCDI v1. Attempts to misuse the exception in that way would not be successful because, for the exception to apply to an actor's practice of making EHI available only via TEFCA, the requestor must be capable via TEFCA of, as applicable, accessing, exchanging, or using the requested EHI from the actor. The condition in § 171.403(b), as finalized, addresses concerns about limits to what EHI requestors can access via TEFCA by ensuring the condition is only available when the EHI the requestor seeks can, in practice, be accessed, exchanged, or used by the requestor via TEFCA.

Structuring the Exception Within the Existing Regulatory Framework

In creating a new subpart and finalizing a separate exception, we have made it easier for actors and requestors to understand when an actor's fulfillment of EHI access, exchange, or use only via TEFCA would not constitute information blocking. By creating a new subpart, we are clearly delineating that the exception is available only to TEFCA participants. Also, by removing it from the Manner Exception, we avoid introducing confusion about when an actor must offer alternative manners and in what order they must do so. Further, in creating this new subpart, we leave room for identifying other reasonable and necessary activities related to TEFCA that do not constitute information blocking, should we propose them in future rulemakings.

EHI That Can Be Made Available Versus EHI That Must Be Made Available via TEFCA

Comments. Some commenters stated that because TEFCA only requires the exchange of the USCDI, the exception will be of limited utility. Another commenter asked for clarity that EHI can exceed the base set of EHI required by TEFCA. Other commenters appreciated that the condition would not be limited to a subset of EHI, so long as the EHI could be accessed, exchanged, or used by the requestor, as applicable.

Response. We appreciate the feedback. As finalized, the exception can be satisfied when any EHI requested by the requestor can be made available to the requestor via TEFCA for the requested access, exchange, or use of the EHI, including where the EHI requested is beyond what is represented by the data elements within any USCDI version. Nothing in this exception restricts how much or which EHI can be shared via TEFCA or limits the exception's application to the minimum data elements that TEFCA's terms require TEFCA entities to make available in response to TEFCA queries. If an actor is capable of sharing all the requested EHI via TEFCA, and, importantly, the requestor is capable of accessing, exchanging, or using all of the EHI via TEFCA, as applicable, then the exception could apply to the practice (if all other conditions are also satisfied). Similarly, if an actor is capable of providing access, exchange, or use of some, but not all, of the requested EHI via TEFCA, the exception can cover the practice for the EHI that the actor *is* capable of providing via TEFCA and the requestor is capable of accessing, exchanging, or using (as applicable). The actor could then provide the remaining EHI in a different manner, for example, by using any of the methods in the Manner Exception (§ 171.301), or resolve the request through other means or applicable information blocking exceptions.

Other Concerns and Observations From Commenters

Comments. A couple of commenters stated that, in some cases, one business unit may sign up for TEFCA, in which case the entire organization would also become part of TEFCA. The commenters stated that in such cases, a requestor may be unaware that they are considered a part of TEFCA, may not have the technical capability to connect their IT systems to the TEFCA network, and will want to receive EHI in another manner.

Response. We thank the commenters for the feedback. The § 171.403(b) *requestor capability* condition of the finalized TEFCA Manner Exception ensures that the exception is only available when the requestor is capable via TEFCA of accessing, exchanging, or using, as applicable, the requested EHI from the actor at the time the request is made. We cannot anticipate every corporate arrangement; however, if a requester's organization is a party to the Common Agreement or a Framework Agreement, it is the requester's responsibility to resolve its approach to EHI access, exchange, and use within the organization.

Agreed Upon by the Requestor

Comments. Several commenters noted that, under the Manner Exception, a requestor must agree to access,

exchange, or use of EHI if the actor offers to fulfill the request in any alternative manner. The commenters stated that, in the proposed *TEFCA manner* condition, requestors would not be required to agree to receive the EHI via TEFCA. They noted that this shifts the balance of power towards actors and away from requestors. Commenters expressed concerns that the requestor cannot counter with an alternative manner and are forced to accept via TEFCA. Other commenters appreciated that the condition would simplify responses for many actors who participate in TEFCA and allow requestors and actors to exchange EHI more efficiently.

Response. In the Manner Exception, one policy objective is to ensure the requestor receives the EHI in either the manner requested or in an alternative manner to which the requestor agrees. This policy assumes that the requestor would not agree to an alternative manner unless that manner allowed them the access, exchange, or use of EHI which they sought in the first place. In finalizing the TEFCA Manner Exception, this policy objective is fulfilled by two conditions. The requestor has agreed to be part of TEFCA and the *requester capability* condition, which states that the requestor is capable, via TEFCA, of accessing, exchanging, or using, as applicable, the EHI requested from the actor. Although the requestor does not have to agree to receive the EHI via TEFCA, the requestor did voluntarily join TEFCA, and assuming the requestor has the necessary capabilities, the requestor will still be able to access, exchange, and/or use the EHI, as applicable. In other words, even if the requestor does not agree to a specific instances of access, exchange, or use of EHI via TEFCA, the TEFCA Manner Exception is still available to the actor for providing such access via TEFCA, so long as an actor has satisfied all of the conditions of the exception at all relevant times. We believe this approach balances the policy interest of promoting interoperability and TEFCA participation with the interest in ensuring EHI moves in a manner that is usable by the requestor.

We also note that the comment and similar comments assume that TEFCA participation will not streamline information exchange. Those who join TEFCA are voluntarily seeking to get the benefits of scalable nationwide trust and infrastructure services for IHE-based and, as the transition to FHIR takes place, FHIR API exchange. Thus, those who join TEFCA would be motivated to fulfill as much of their information sharing obligations and practices as they are able to in order to reduce the overhead associated with achieving interoperability outside of TEFCA. In short, rather than hampering information sharing, we believe that encouraging exchange via TEFCA will make it easier for both actors and requestors to achieve access, exchange, and use of the EHI.

Finally, to clarify the distinction between the Manner Exception (§ 171.301) and its conditions (a) *manner requested* and (b) *alternative manner,* we have finalized a new subpart D, ''Exceptions That Involve Practices Related to Actors' Participation in The Trusted Exchange Framework and Common Agreement (TEFCA)'' and finalized the TEFCA Manner Exception within that subpart at § 171.403.

Concerns About TEFCA Policies

Comments. A commenter asked for clarification about how to distinguish exchange that occurs pursuant to a Framework Agreement versus an intra-QHIN agreement. The same commenter also asked how actors will be able to ascertain whether a request made for a certain purpose (*e.g.,* health care operations) outside the TEFCA network aligns with the same purpose that they (the actors) would be offering to respond to under TEFCA; and how to handle situations where a requestor does not support the capability to make or receive requests or perform other transmissions for certain Exchange Purposes that do not require a response (*e.g.,* Payment, Public Health, or health care operations). Another commenter asked ONC to clarify which purposes are permitted under TEFCA as applied to this exception. One commenter asked that ONC clarify that if the EHI being requested or the exchange purpose for which it was requested are not part of the current required parameters of TEFCA, the condition will still be available.

Response. QHIN-to-QHIN exchange would be covered by this exception because both parties, the QHINs, are ''part of TEFCA,'' having signed the Common Agreement to become a QHIN. Exchange *within* QHINs (in other words, exchange between Participants or Subparticipants who have joined the same QHIN) would also qualify for this exception. In addition, the purpose of the request is not relevant for the information blocking definition, nor is the status of the parties beyond their being ''part of TEFCA.'' So long as the actor can respond to the request via TEFCA, and the requestor participates in TEFCA and is capable of access, exchange, or use of the EHI, as applicable, then the condition can be satisfied, assuming all the other conditions of the exception are also met. In situations where a requestor does not support the capability to make or receive requests or perform other transmissions for certain Exchange Purposes that do not require a response, then the TEFCA Manner Exception would not be available because the requestor would not be able to access, exchange, or use the EHI if transmitted via TEFCA, and thus the second condition of the exception, *requestor capability* (§ 171.403(b)) would not be met.

TEFCA Directory

ONC requested comment on whether an actor should be required to search a directory prior to responding via TEFCA (88 FR 23873).

Comment. One commenter expressed concerns that the directory would be unreliable, or that actors may not be recognized due to naming issues. Another commenter asked if QHINs would be permitted to leverage their own provider directories.

Response. We thank the commenters for their feedback. At this time, for reasons such as those mentioned by the commenter as well as due to the logistical complexities of providing real-time access to an easily usable directory for purposes of identifying requestors of EHI, we have not finalized a requirement that an actor search the TEFCA directory as a condition of the exception. Actors should be able to determine whether requestors are part of TEFCA through customary business interactions, such as those that occur when parties engage in exchanging EHI. Actors may also choose to use their own resources, such as provider directories, to make affirmative determinations of whether a requestor is part of TEFCA. However, it ultimately remains the actor's responsibility in making a positive determination as to whether a requestor is part of TEFCA for the purposes of satisfying this exception.

General Comments

Comments. A few commenters recommended that ONC restrict the scope of the proposed exception such that it covers only those reasonable activities that are necessary to comply with and implement the Common Agreement, and not to extend it to other practices. Commenters noted this would still incentivize TEFCA participation without inadvertently inhibiting innovation and competition.

Response. While we appreciate the commenter's position and agree that

such an exception may incentivize TEFCA participation, the finalized TEFCA Manner Exception will provide certainty to actors that the practice of making EHI available for access, exchange, and use via TEFCA to other TEFCA participants, and consistent with the relevant outlined conditions, will not be information blocking. We may consider proposing additional TEFCA exceptions in future rulemakings.

Comments. One commenter expressed support for the exception, stating that it would reduce burden on physicians who connect to a QHIN by allowing physicians to rely on that connection as a substitute for fulfillment of tailored requests for EHI by redirecting the requestor to the QHIN.

Response. We want to clarify that, as proposed and as finalized, the TEFCA Manner Exception does not permit physicians to redirect all requests for access, exchange, or use of EHI to a QHIN. However, TEFCA participation and meeting the exception in applicable circumstances may allow physicians to redirect a significant portion of EHI requests. The exception outlines the specific circumstances under which an actor, who is part of TEFCA, may respond to a requestor, who is also part of TEFCA, via TEFCA services regardless of the manner requested, unless the requestor asked for the access via the standards adopted in 45 CFR 170.215, including versions of those standards approved pursuant to 45 CFR 170.405(b)(8). Further, the requestor must be capable of accessing, exchanging, or using the EHI, as applicable to the circumstances, via TEFCA. Therefore, there will be circumstances when both the actor and requestor may be part of TEFCA, but the exception would not apply because the requestor cannot, for technical reasons or due to TEFCA-related agreements, access, exchange, or use the EHI via TEFCA. We also emphasize, again, that individuals cannot be ''part of TEFCA;'' thus, if the requestor is an individual, the TEFCA Manner Exception will not be available to any actor.

Comment. A commenter suggested ONC simplify the information blocking regulations and create separate exceptions/conditions for providers different from those for developers and networks and explore provider-targeted exception options not tied to certified Health IT Module use or TEFCA participation.

Response. We appreciate the comment, but we did not propose exceptions specific to any one of the three categories of actors (health care provider, HIN/HIE, and health IT developer of certified health IT), and decline to adopt such an approach in this final rule. The exceptions address reasonable and necessary activities that are not considered information blocking and are designed to be used by any of the regulated actors where appropriate. Generally, they are not contingent on the use of certified health IT. Further, all of the exceptions set forth in subparts B and C of 45 CFR part 171 are available to any actor, when they are satisfied, regardless of whether the actor has chosen to become a part of the TEFCA ecosystem. Health care providers interested in learning more about any or all of the information blocking exceptions can find more information about the exceptions at *https://www.healthit.gov/topic/information-blocking.* The exceptions themselves can be found in their entirety in 42 CFR part 171 (available online at: *https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-D/part-171?toc=1*).[262]

Comments Beyond the Scope of the Proposal

Comments. A commenter asked for clarification regarding the participation of entities in TEFCA that are acting on behalf of other entities, like business associates, and the data sharing requirements for those entities.

Response. We appreciate the comment. The regulations and requirements governing TEFCA are out of scope for the proposal.

Comments. One commenter asked ONC to better explain the controls that are in place to ensure that QHIN requested data does not violate HIPAA. Another commenter asked ONC to address how patients will provide consent for the networked sharing of their data via TEFCA, and how patients will even be informed about what of their data has been shared by whom, to whom, and for what use. A few commenters asked ONC to incorporate privacy-protective practices into the Common Agreement.

Response. These comments are beyond the scope of the proposal. However, we offer the following information in response to these comments about TEFCA. TEFCA includes strong privacy protections within the Common Agreement, Qualified Health Information Network Technical Framework (QTF), and standard operating procedures. Most connected entities under TEFCA will be HIPAA covered entities or business associates of covered entities, and thus will already be required to comply with the HIPAA Privacy Rule. The Common Agreement requires each non-HIPAA entity that participates in TEFCA to protect individually identifiable information that it reasonably believes is TEFCA information in substantially the same manner as HIPAA covered entities protect PHI, including having to comply with most provisions of the HIPAA Privacy Rule as if they were subject to the HIPAA Privacy Rule. Further, in some ways, the TEFCA requirements related to the Individual Access Services (IAS) exchange purpose require that IAS providers meet an even higher bar of privacy than HIPAA, including providing individuals with the right to delete their data.

For additional information about TEFCA requirements related to privacy, we refer readers to the most recent versions of the Common Agreement, QTF, and standard operating procedures. ONC's official website, *HealthIT.gov*, also provides additional information about TEFCA.

Comment. A commenter suggested ONC align with the approach taken by CMS in its promoting interoperability programs to explicitly name TEFCA as an optional alternative for claiming credit under the HIE Objective.

Response. We appreciate the comment. We are uncertain how or in what manner the commenter recommends we align the TEFCA Manner Exception with the approach CMS implemented for TEFCA participation under the promoting interoperability programs. However, as mentioned above, this comment is beyond the scope of the proposal.

Comment. One commenter requested ONC to consider how it can address patient portals that cannot share a full record set with a patient, and interoperability concerns that arise from portal configurations.

Response. We appreciate the feedback. Although ONC does consider and regulate the interoperability capabilities of health IT as it relates to patient portals through the ''view, download, and transmit to 3rd party'' certification criterion (45 CFR 170.315(e)(1)) of the Program, this comment is beyond the scope of the proposal.

D. Information Blocking Requests for Information

1. Additional Exclusions From Offer Health IT—Request for Information

In the HTI–1 Proposed Rule (at 88 FR 23873), we sought comment on whether we should consider proposing in future rulemaking any additional exclusions from the *offer health information*

[262] URLs retrieved Oct 26, 2023.

technology or *offer health IT* definition proposed in § 171.102 of this proposal. We also welcomed information specific to how potential additional exclusions could be structured or balanced by other measures to mitigate risks of unintended consequences of such exclusions. We also indicated we would welcome comments on other steps ONC might consider taking to further encourage lawful donation or other subsidized provision of certified health IT to health care providers who may otherwise struggle to afford modern, interoperable health IT.

Comments. We received 14 comment submissions that included comments in response to this RFI.

Response. We thank the commenters for their feedback. As noted in the HTI–1 Proposed Rule, we may use this feedback to inform a future rulemaking.

2. Possible Additional TEFCA Reasonable and Necessary Activities—Request for Information

In the HTI–1 Proposed Rule (at 88 FR 23873 through 23874), we sought comment on whether any other particular practices that are not otherwise required by law, but are required of an individual person or entity by virtue of their status as a QHIN, Participant, or Subparticipant pursuant to the Common Agreement, pose a substantial concern or uncertainty regarding whether such practices *could* constitute information blocking as defined in 45 CFR 171.103. We sought comment on which particular practices the commenters believe are not covered by existing information blocking exceptions and that the commenters would advocate we assess for potential identification as reasonable and necessary activities that do not constitute information blocking as defined in 45 CFR 171.103. We also sought comment on whether and how any such identification of additional reasonable and necessary activities might pose concerns about unintended consequences for EHI access, exchange, or use by individuals or entities that are not QHINs, Participants, or Subparticipants.

Comments. We received 16 comment submissions that included comments in response to this RFI.

Response. We thank the commenters for their feedback. As noted in the HTI–1 Proposed Rule, we may use this feedback to inform future rulemaking.

3. Health IT Capabilities for Data Segmentation and User/Patient Access—Request for Information

In the HTI–1 Proposed Rule (at 88 FR 23874 through 23875), we discussed the importance of data segmentation capabilities and a variety of situations in which segmentation of data may be required or requested, including use cases where special handling or other restriction of access, exchange, or use of particular portion(s) of a patient's EHI is required by law or consistent with an individual patient's expressed preference regarding their own or others' access to their EHI. The HTI–1 Proposed Rule included a primary and several alternative proposals for a new certification criterion specifically focused on supporting patient preferences related to their right to request restrictions on certain uses and disclosures of their PHI under the HIPAA Privacy Rule (see 45 CFR 164.522). This proposal is addressed in section III.C.10 of this final rule (see section III.C.10 for further detail).

In addition to the specific right to request a restriction on disclosure consistent with 45 CFR 164.522, there are other use cases related to patient preferences—and specific nuances within use cases—which present challenges from a technical point of view.

We sought comment to inform steps we might consider taking to improve the availability and accessibility of solutions supporting health care providers' and other information blocking actors' efforts to honor patients' expressed preferences regarding their EHI (88 FR 23874). We also specifically sought (88 FR 23875) comment on additional topics related to the capabilities of health IT products to segment data, such as experiences with the availability and utility of certified health IT products' capabilities to segment data in use cases, including, but not limited to, the illustrative examples above.

Comments. We received 102 comment submissions that included comments in response to this RFI.

Response. We thank the commenters for their feedback. As noted in the HTI–1 Proposed Rule, we may use this feedback to inform a future rulemaking.

V. Incorporation by Reference

The Office of the Federal Register has established requirements for materials (*e.g.,* standards and implementation specifications) that agencies incorporate by reference in the Code of Federal Regulations (79 FR 66267; 1 CFR 51.5(b)). Specifically, § 51.5(b) requires agencies to discuss, in the preamble of a final rule, the ways that the materials they incorporate by reference are reasonably available to interested parties or how it worked to make those materials reasonably available to interested parties; and summarize, in the preamble of the final rule, the material they incorporate by reference.

To make the materials we intend to incorporate by reference reasonably available, we provide a uniform resource locator (URL) for the standards and implementation specifications. In many cases, these standards and implementation specifications are directly accessible through the URLs provided. In most of these instances, access to the standard or implementation specification can be gained through no-cost (monetary) participation, subscription, or membership with the applicable standards developing organization (SDO) or custodial organization. Alternatively, a copy of the standards may be viewed for free at the U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, 330 C Street SW, Washington, DC 20201. Please call (202) 690–7171 in advance to arrange inspection.

The National Technology Transfer and Advancement Act (NTTAA) of 1995 (15 U.S.C. 3701 *et seq.*) and the Office of Management and Budget (OMB) Circular A–119 require the use of, wherever practical, technical standards that are developed or adopted by voluntary consensus standards bodies to carry out policy objectives or activities, with certain exceptions. The NTTAA and OMB Circular A–119 provide exceptions to selecting only standards developed or adopted by voluntary consensus standards bodies, namely when doing so would be inconsistent with applicable law or otherwise impractical. As discussed in section III.B of this preamble, we have followed the NTTAA and OMB Circular A–119 in adopting standards and implementation specifications, including describing any exceptions in the adoption of standards and implementation specifications. Over the years of adopting standards and implementation specifications for certification, we have worked with SDOs, such as HL7, to make the standards we adopt and incorporate by reference in the **Federal Register**, available to interested parties. As described above, this includes making the standards and implementation specifications available through no-cost memberships and no-cost subscriptions.

As required by § 51.5(b), we provide summaries of the standards we have adopted and incorporate by reference in the Code of Federal Regulations. We also provide relevant information about these standards and implementation specifications throughout the preamble.

We have organized the following standards and implementation specifications that we have adopted through this rulemaking according to the sections of the CFR in which they would be codified and cross-referenced for associated certification criteria and requirements that we have adopted.

Content Exchange Standards and Implementation Specifications for Exchanging Electronic Health Information—45 CFR 170.205

- *Health Level 7 (HL7®) CDA® R2 Implementation Guide: C–CDA Templates for Clinical Notes STU Companion Guide, Release 4.1—US Realm, June 2023, Specification Version: 4.1.1.*

URL: *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=447.*

Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: The Consolidated Clinical Document Architecture (C–CDA) Companion Guide R4.1, provides essential implementer guidance to continuously expand interoperability for clinical information shared via structured clinical notes. The guidance supplements specifications established in the Health Level Seven (HL7) CDA® R2.1 IG: C–CDA Templates for Clinical Notes. This additional guidance is intended to make implementers aware of expectations and best practices for C–CDA document exchange. The objective is to increase consistency and expand interoperability across the community of data sharing partners who utilize C–CDA for information exchange.

- *HL7 FHIR® Implementation Guide: Electronic Case Reporting (eCR)—US Realm 2.1.0—STU 2 US (HL7 FHIR eCR IG), August 31, 2022.*

URL: *https://build.fhir.org/ig/HL7/case-reporting/.*

Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: With the adoption and maturing of Electronic Health Records (EHRs), there are opportunities to better support public health surveillance as well as to better support the delivery of relevant public health information to clinical care. Electronic Case Reporting (eCR) can provide more complete and timely case data, support disease/condition monitoring, and assist in outbreak management and control. It can also improve bidirectional communications through the delivery of public health information in the context of a patient's condition and local disease trends and by facilitating ad hoc communications, as well as reduce health care provider burden by automating the completion of legal reporting requirements. The purpose of this FHIR IG is to offer opportunities to further enable automated triggering and reporting of cases from EHRs, to ease implementation and integration, to support the acquisition of public health investigation supplemental data, and to connect public health information (*e.g.,* guidelines) with clinical workflows. Over time, FHIR may also support the distribution of reporting rules to clinical care to better align data authorities and make broader clinical data available to public health decision support services inside the clinical care environment.

- *HL7 CDA® R2 Implementation Guide: Public Health Case Report—the Electronic Initial Case Report (eICR) Release 2, STU Release 3.1—US Realm (HL7 CDA eICR IG), July 2022.*

URL: *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=436.*

Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: The purpose of this implementation guide (IG) is to specify a standard for electronic submission of electronic initial public health case reports using HL7 Version 3 Clinical Document Architecture (CDA), Release 2 format. This implementation guide specifies a standard that will allow health care providers to electronically communicate the specific data needed in initial public health case reports (required by state laws/regulations) to jurisdictional public health agencies in CDA format—an interoperable, industry-standard format.

- *HL7 CDA® R2 Implementation Guide: Reportability Response, Release 1, STU Release 1.1—US Realm (HL7 CDA RR IG), July 2022.*

URL: *https://www.hl7.org/implement/standards/product_brief.cfm?product_id=470.*

Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: The purpose of this implementation guide (IG) is to specify a standard for a response document for a public health electronic Initial Case Report (HL7 eICR all releases) using HL7 Version 3 Clinical Document Architecture (CDA), Release 2 format. Through the Reportability Response, public health seeks to support bidirectional communication with clinical care for reportable conditions in CDA format, which is an interoperable, industry-standard format.

- *Reportable Conditions Trigger Codes Value Set for Electronic Case Reporting. RCTC OID: 2.16.840.1.114222.4.11.7508, Release March 29, 2022.*

URL: *https://ecr.aimsplatform.org/ehr-implementers/triggering/.*

Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: The Reportable Condition Trigger Codes (RCTC) are a nation-wide set of standardized codes to be implemented within an electronic health record (EHR) that provide a preliminary identification of events that may be of interest to public health for electronic case reporting. The RCTC are the first step in a two-step process to determine reportability. The RCTC are single factor codes that represent any event that may be reportable to any public health agency in the United States. A second level of evaluation still must be done against jurisdiction-specific reporting regulations, to confirm whether the event is reportable and to which public health agency or agencies. The RCTC currently includes ICD 10 CM, SNOMED CT, LOINC, RxNorm, CVX, and CPT, representing condition-specific diagnoses, resulted lab tests names, lab results, lab orders for conditions reportable upon suspicion, and medications for select conditions.

Vocabulary Standards for Representing Electronic Health Information—45 CFR 170.207

- *HL7 Standard Code Set CVX—Vaccines Administered, dated June 15, 2022.*

URL: *https://www2a.cdc.gov/vaccines/iis/iisstandards/vaccines.asp?rpt=cvx.*

This is a direct access link.

Summary: The CDC's National Center of Immunization and Respiratory Diseases (NCIRD) developed and maintains the CVX (vaccine administered) code set. It includes both active and inactive vaccines available in the US. CVX codes for inactive vaccines allow transmission of historical immunization records. When a MVX (manufacturer) code is paired with a CVX (vaccine administered) code, the specific trade named vaccine may be indicated. These codes should be used for immunization messages using HL7 Version 2.5.1.

- *National Drug Code Directory (NDC)—Vaccine NDC Linker, dated July 19, 2022.*

URL: *https://www2.cdc.gov/vaccines/iis/iisstandards/ndc_tableaccess.asp.*

This is a direct access link.

Summary: The Drug Listing Act of 1972 requires registered drug establishments to provide the FDA with a current list of all drugs manufactured, prepared, propagated, compounded, or processed by it for commercial distribution. Drug products are identified and reported using a unique, three-segment number, called the National Drug Code (NDC), which serves as the universal product identifier for drugs. This standard is limited to the NDC vaccine codes identified by CDC.

- *CDC Race and Ethnicity Code Set version 1.2, (July 08, 2021).*

URL: *https://www.cdc.gov/phin/resources/vocabulary/index.html.*

The code set can be accessed through this link.

Summary: The CDC has prepared a code set for use in coding race and ethnicity data. This code set is based on current federal standards for classifying data on race and ethnicity, specifically the minimum race and ethnicity categories defined by the U.S. Office of Management and Budget (OMB) and a more detailed set of race and ethnicity categories maintained by the U.S. Bureau of the Census (BC). The main purpose of the code set is to facilitate use of federal standards for classifying data on race and ethnicity when these data are exchanged, stored, retrieved, or analyzed in electronic form. At the same time, the code set can be applied to paper-based record systems to the extent that these systems are used to collect, maintain, and report data on race and ethnicity in accordance with current federal standards.

- *Medicare Provider and Supplier Taxonomy Crosswalk, 2021.*

URL: *https://data.cms.gov/provider-characteristics/medicare-provider-supplier-enrollment/medicare-provider-and-supplier-taxonomy-crosswalk/data/2021.*

This is a direct access link.

Summary: The Medicare Provider and Supplier Taxonomy Crosswalk dataset lists the providers and suppliers eligible to enroll in Medicare programs with the proper healthcare provider taxonomy code. This data includes the Medicare specialty codes, if available, provider/supplier type description, taxonomy code, and the taxonomy description. The Healthcare Provider Taxonomy Code Set is a hierarchical code set that consists of codes, descriptions, and definitions. Healthcare Provider Taxonomy Codes are designed to categorize the type, classification, and/or specialization of health care providers. The Code Set is available from the Washington Publishing Company (*https://wpc-edi.com/*). The Code Set is maintained by the National Uniform Claim Committee (*https://www.nucc.org/*).

- *Public Health Data Standards Consortium Users Guide for Source of Payment Typology Code Set, December 2020, Version 9.2.*

URL: *https://nahdo.org/sites/default/files/2020-12/SourceofPaymentTypologyUsersGuideVersion9.2December2020.pdf.*

This is a direct access link.

Summary: The Source of Payment Typology was developed to create a standard for reporting payer type data that will enhance the payer data classification; it is also intended for use by those collecting data or analyzing healthcare claims information. Modeled loosely after the ICD typology for classifying medical conditions, the proposed typology identifies broad Payer categories with related subcategories that are more specific. This format provides analysts with flexibility to either use payer codes at a highly detailed level or to roll up codes to broader hierarchical categories for comparative analyses across payers and locations.

- *Logical Observation Identifiers Names and Codes (LOINC®) Database Version 2.72, a universal code system for identifying laboratory and clinical observations produced by the Regenstrief Institute, Inc., February 16, 2022.*

URL: *https://loinc.org/downloads/.*

Access requires registration, a user account, and license agreement. There is no monetary cost for registration, a user account, and license agreement.

Summary: Informed by tracking healthcare trends, evaluating concept requests, and listening to guidance from the community, this release contains new and edited concepts in Laboratory, Clinical, Survey, Document Type, and other domains. It also includes a newly streamlined release file structure for more efficient download and use.

- *The Unified Code for Units of Measure, Revision 2.1, November 21, 2017.*

URL: *https://ucum.org/ucum.html.*

This is a direct access link.

Summary: The Unified Code for Units of Measure is a code system intended to include all units of measures being contemporarily used in international science, engineering, and business. The purpose is to facilitate unambiguous electronic communication of quantities together with their units. The focus is on electronic communication, as opposed to communication between humans. A typical application of The Unified Code for Units of Measure are electronic data interchange (EDI) protocols, but there is nothing that prevents it from being used in other types of machine communication.

- *Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®) U.S. Edition, March 2022.*

URL: *https://www.nlm.nih.gov/healthit/snomedct/us_edition.html.*

Access requires a user account and license agreement. There is no monetary cost for a user account and license agreement.

Summary: In addition to the 279 new active concepts specific to the US Edition, the March 2022 SNOMED CT US Edition also includes the SNOMED CT COVID–19 Related Content published in the January 2022 SNOMED CT International Edition. This latest version of the US Edition also includes the SNOMED CT to ICD–10–CM reference set, with over 126,000 SNOMED CT source concepts mapped to ICD–10–CM targets.

- *RxNorm, a standardized nomenclature for clinical drugs produced by the United States National Library of Medicine, July 5, 2022, Full Update Release.*

URL: *https://www.nlm.nih.gov/research/umls/rxnorm/docs/rxnormfiles.html.*

Access requires a user account and license agreement. There is no monetary cost for a user account and license agreement.

Summary: RxNorm, a standardized nomenclature for clinical drugs, is produced by the National Library of Medicine. RxNorm's standard identifiers and names for clinical drugs are connected to the varying names of drugs present in many different controlled vocabularies within the Unified Medical Language System (UMLS) Metathesaurus, including those in commercially available drug information sources. These connections are intended to facilitate interoperability among the computerized systems that record or process data dealing with clinical drugs.

United States Core Data for Interoperability—45 CFR 170.213

- *United States Core Data for Interoperability (USCDI), October 2022 Errata, Version 3 (v3).*

URL: *https://www.healthit.gov/USCDI.*

This is a direct access link.

Summary: The United States Core Data for Interoperability (USCDI establishes a minimum set of data classes that are required to be interoperable nationwide and is

designed to be expanded in an iterative and predictable way over time. Data classes listed in the USCDI are represented in a technically agnostic manner to set a foundation for broader sharing of electronic health information. ONC has established a predictable, transparent, and collaborative expansion process for USCDI based on public evaluation of previous versions and submissions by the health IT community and the public, including input from a federal advisory committee.

Application Programming Interface Standards—45 CFR 170.215

- *HL7 FHIR US Core Implementation Guide Version 6.1.0—STU6, June 19, 2023.*

URL: *http://hl7.org/fhir/us/core/.*

This is a direct access link.

Summary: The US Core Implementation Guide is based on FHIR Version R4.0.1 and defines the minimum set of constraints on the FHIR resources to create the US Core Profiles. It also defines the minimum set of FHIR RESTful interactions for each of the US Core Profiles to access patient data. By establishing the ''floor'' of standards to promote interoperability and adoption through common implementation, it allows for further standards development evolution for specific uses cases.

- *HL7 FHIR® SMART App Launch Implementation Guide Release 2.0.0, November 26, 2021.*

URL: *http://hl7.org/fhir/smart-app-launch/.*

This is a direct access link.

Summary: This implementation guide describes a set of foundational patterns based on OAuth 2.0 for client applications to authorize, authenticate, and integrate with FHIR-based data systems.

VI. Collection of Information Requirements

Under the Paperwork Reduction Act of 1995 (PRA), codified as amended at 44 U.S.C. 3501 *et seq.,* agencies are required to provide a 30-day notice in the **Federal Register** and solicit public comment on a proposed collection of information before it is submitted to the Office of Management and Budget for review and approval. In order to fairly evaluate whether an information collection should be approved by the OMB, section 3506(c)(2)(A) of the PRA requires that we solicit comment on the following issues:

1. Whether the information collection is necessary and useful to carry out the proper functions of the agency.

2. The accuracy of the agency's estimate of the information collection burden.

3. The quality, utility, and clarity of the information to be collected; and

4. Recommendations to minimize the information collection burden on the affected public, including automated collection techniques.

Under the PRA, the time, effort, and financial resources necessary to meet the information collection requirements referenced in this section are to be considered. We solicited comment on these issues in the HTI–1 Proposed Rule (88 FR 23878 through 23880) for the matters discussed in detail below.

A. Independent Entity

As stated in the HTI–1 Proposed Rule (88 FR 23847), we proposed that response submissions related to the Insights Condition and Maintenance of Certification requirements would be submitted to an independent entity on behalf of ONC, and that we intend to award a grant, contract, or other agreement to an independent entity as part of the implementation of the Insights Condition and Maintenance of Certification requirements.

For estimating potential burden, we stated that we believe the independent entity would take approximately 5 minutes to review a response submission for completeness, and approximately 30 minutes to submit the completed response submission to ONC, based on how many products a developer of certified health IT may be required to submit responses for. We also stated that we plan to minimize burden for the independent entity by automating parts of the response review and submission process via an online tool.

TABLE 3—ESTIMATED ANNUALIZED BURDEN HOURS FOR INDEPENDENT ENTITY TO REVIEW AND SUBMIT DEVELOPER RESPONSES TO ONC PER INSIGHTS CONDITION REQUIREMENTS

Code of Federal regulations section	Number of independent entity	Average burden hours	Total
45 CFR 170.407(a)	1	24	24
45 CFR 170.407(b)	1	143	143
Total Burden Hours	.....	.....	167

Comments. We did not receive any comments specific to the response submissions related to the Insights Condition and Maintenance of Certification requirements that would be submitted to an independent entity on behalf of ONC.

Response. We continue to maintain our estimated annualized burden hours for an independent entity to take approximately 5 minutes to review a response submission for completeness, and approximately 30 minutes to submit the completed response submission to ONC. We refer readers to section VII (Regulatory Impact Analysis) of this final rule for the cost estimates related to the Insights Condition.

B. Health IT Developers

We stated in the HTI–1 Proposed Rule (88 FR 23846), developers of certified health IT would be required to submit responses associated with the Insights Condition and Maintenance of Certification requirements to an independent entity twice a year. For the purposes of estimating potential burden, we estimated 52 developers of certified health IT would be required to report on the Insights Condition. We estimated it would take approximately 21,136 to 44,900 hours on average for a developer of certified health IT to collect and report on the proposed measures within the Insights Condition and Maintenance of Certification requirements. For the purposes of estimating the total potential burden for developers of certified health IT, we estimated an average burden of 2,334,800 hours. We stated that this was crude upper bound estimate as there are multiple measures with varying complexity associated with the Insights Condition and Maintenance of Certification, and the number of developers of certified health IT required to report changes by each measure.

TABLE 4—ESTIMATED ANNUALIZED TOTAL BURDEN HOURS FOR HEALTH IT DEVELOPERS TO COMPLY WITH THE INSIGHTS CONDITION AND MAINTENANCE OF CERTIFICATION REQUIREMENTS

Code of Federal regulations section	Number of health IT developers	Average burden hours—lower bound	Average burden hours—upper bound
45 CFR 170.407(a)	52	17,445	38,750
Total Burden Hours		790,806	1,767,692

In the HTI–1 Proposed Rule (88 FR 23797), we stated for § 170.315(b)(11)(vii)(B), health IT developers would compile documentation regarding the intervention risk management practices listed in § 170.315(b)(11)(vii)(A), and upon request from ONC, make available such detailed documentation for any Predictive DSI, as defined in § 170.102, that the certified Health IT Module enables or interfaces with. We stated that we believe ONC has the authority to conduct Direct Review consistent with § 170.580(a)(2) for any known non-conformity or where it has a reasonable belief that a non-conformity exists enabling ONC to have oversight of these requirements. The PRA, however, exempts these information collections. Specifically, 44 U.S.C. 3518(c)(1)(B)(ii) excludes collection activities during the conduct of administrative actions or investigations involving the agency against specific individuals or entities.

Comments. We did not receive any comments specific to either collection of information from developers of health IT or our corresponding PRA determinations.

Response. For the first information collection, we have provided updated burden estimates above in Table 4 to reflect revisions we have finalized for the Insights Condition. Recognizing that there was some overlap for the Insights and Real World Testing Condition of Certification, we have finalized that health IT developers who were required to report for the Insights Condition could leverage relevant Insights measures for real world testing annual reporting to reduce costs. In addition, due to significant overlap we have finalized across many of the measures, we have reduced the estimated burden hours assuming there will be a 10% overlap of developing infrastructure across all measures. For a more detailed discussion and the cost estimates of these new regulatory requirements associated with the Insights Condition and Maintenance of Certification, we refer readers to section VII (Regulatory Impact Analysis) of this final rule.

For the second information collection, we continue to maintain that information collected pursuant to an administrative enforcement action is not subject to the PRA under 44 U.S.C. 3518(c)(1)(B)(ii), which excludes collection activities during the conduct of administrative actions or investigations involving the agency against specific individuals or entities.

C. ONC–ACBs

As stated in the HTI–1 Proposed Rule (88 FR 23782), we proposed in § 170.315(b)(11)(vii)(C) that a health IT developer that attests ''yes'' in § 170.315(b)(11)(v)(A) submit summary information of the intervention risk management practices listed in § 170.315(b)(11)(vii)(A)(*1*) through (*3*) to its ONC–ACB via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps. To support submission of documentation, and consistent with other Principles of Proper Conduct in § 170.523(f)(1), we proposed a new Principle of Proper Conduct for documentation related to § 170.315(b)(11)(vii)(C) in § 170.523(f)(1)(xxi). In the 2015 Edition Proposed Rule (80 FR 16894), we estimated fewer than ten annual respondents for all of the regulatory ''collection of information'' requirements that applied to the ONC–ACBs, including those previously approved by OMB. In the 2015 Edition Final Rule (80 FR 62733), we concluded that the regulatory ''collection of information'' requirements for the ONC–ACBs were not subject under the implementing regulations of the PRA at 5 CFR 1320.3(c).

Comments. We did not receive any comments specific to the new Principle of Proper Conduct for the submission of documentation in § 170.523(f)(1)(xxi).

Response. We have finalized the requirements in § 170.523(f)(1)(xxi), as proposed, which will require ONC–ACBs to ensure that developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) submit summary information of intervention risk management practices (for each Predictive DSI supplied by the health IT developer as part of its Health IT Module) via publicly accessible hyperlinks that allow any person to access the summary information directly without any preconditions or additional steps. We continue to maintain our past determinations in that we estimate less than ten annual respondents for all the regulatory ''collection of information'' requirements for ONC–ACBs under part 170 of title 45, including those previously approved by OMB and in this final rule, and that the regulatory ''collection of information'' requirements under the Program described in this section are not subject under the implementing regulations of the PRA at 5 CFR 1320.3(c). For the cost estimates of these new regulatory requirements, we refer readers to section VII (Regulatory Impact Analysis) of this final rule.

VII. Regulatory Impact Analysis

A. Statement of Need

This final rule is necessary to meet our statutory responsibilities under the Cures Act and to advance HHS policy goals to promote interoperability and mitigate burden for health IT developers and users. Policies that could result in monetary costs for health IT developers and users include: (1) updates to ONC Certification Criteria for Health IT; (2) the Insights Condition and Maintenance of Certification requirements; and (3) policies related to information blocking.

While much of this final rule's costs will fall on health IT developers who seek to certify health IT under the Program, we believe the implementation and use of ONC Certification Criteria for Health IT, compliance with the Insights Condition and Maintenance of Certification requirements (''Insights Condition''), and the provisions related to information blocking will ultimately result in significant benefits for health care providers and patients. We outline some of these benefits below. We emphasize in this regulatory impact analysis (RIA) that we believe this final rule will remove barriers to interoperability and EHI exchange, which will greatly benefit health care providers and patients.

We note in this RIA that there were instances in which we had difficulty quantifying certain benefits due to a lack of applicable studies, data, or both. However, in such instances, we highlight the significant non-quantified benefits of our policies to advance an interoperable health system that empowers individuals to use their EHI to the fullest extent and enables health care providers and communities to deliver smarter, safer, and more efficient care.

B. Alternatives Considered

If there are alternatives to our policies, we have described them within each of the sections within this RIA. In some cases, we have been unable to identify alternatives that would appropriately implement our responsibilities under the Cures Act and support interoperability. We believe our policies take the necessary steps to fulfill the mandates specified in the Public Health Service Act (PHSA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act and the Cures Act, in the least burdensome way. We welcomed comments on our assessment and any alternatives we should consider.

C. Overall Impact

We have examined the impacts of this rule as required by Executive Order 12866 on Regulatory Planning and Review (September 30, 1993), Executive Order 13563 on Improving Regulation and Regulatory Review (January 18, 2011), Executive Order 14094 entitled ''Modernizing Regulatory Review'' (April 6, 2023), the Regulatory Flexibility Act (RFA) (September 19, 1980, Pub. L. 96–354), section 1102(b) of the Social Security Act, section 202 of the Unfunded Mandates Reform Act of 1995 (March 22, 1995; Pub. L. 104–4), Executive Order 13132 on Federalism (August 4, 1999), and the Congressional Review Act (5 U.S.C. 804(2)).

Executive Orders 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). The Executive Order 14094 entitled ''Modernizing Regulatory Review'' (hereinafter, the Modernizing E.O.) amends section 3(f)(1) of Executive Order 12866 (Regulatory Planning and Review). The amended section 3(f) of Executive Order 12866 defines a ''significant regulatory action'' as an action that is likely to result in a rule: (1) having an annual effect on the economy of $200 million or more in any 1 year (adjusted every 3 years by the Administrator of OIRA for changes in gross domestic product), or adversely affect in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or state, local, territorial, or tribal governments or communities; (2) creating a serious inconsistency or otherwise interfering with an action taken or planned by another agency; (3) materially altering the budgetary impacts of entitlement grants, user fees, or loan programs or the rights and obligations of recipients thereof; or (4) raise legal or policy issues for which centralized review would meaningfully further the President's priorities or the principles set forth in this Executive order, as specifically authorized in a timely manner by the Administrator of OIRA in each case.

A regulatory impact analysis (RIA) must be prepared for major rules with significant regulatory actions and/or with significant effects as per section 3(f)(1) ($200 million or more in any 1 year).

Based on our estimates, OMB's Office of Information and Regulatory Affairs has determined this rulemaking is significant per section 3(f)(1) as measured by the $200 million or more in any 1 year, and hence also a major rule under Subtitle E of the Small Business Regulatory Enforcement Fairness Act of 1996 (also known as the Congressional Review Act) (Pub. L. 104–121, Mar. 29, 1996).

a. Costs and Benefits

We have estimated the potential monetary costs and benefits of this final rule for health IT developers, health care providers, patients, and the Federal Government (*i.e.,* ONC), and have broken those costs and benefits out by section. In accordance with Executive Order 12866, we have included the RIA summary table as Table 37.

Our cost calculations quantify health IT developers' time and effort to implement these policies through new development and administrative activities. We recognize that the costs developers incur as a result of these policies may be passed on to certified health IT end-users. These end-users include but are not limited to the nearly 5,000 non-federal hospitals who provide acute, inpatient care and over one million clinicians who provide outpatient care to all Americans. Official statistics show that nearly all U.S. non-federal acute care hospitals (*https://www.healthit.gov/data/quickstats/national-trends-hospital-and-physician-adoption-electronic-health-records*) and the vast majority of outpatient physicians use certified health IT (*https://www.healthit.gov/data/quickstats/office-based-physician-electronic-health-record-adoption*). These policies affect the technology that all these health care providers use.

The benefits, both quantifiable and not quantifiable, articulated in this impact analysis have the potential to remove barriers to interoperability and EHI exchange for all these health care providers. Though these policies first require effort by developers of certified health IT to reflect them in their software, they must then be implemented by end-users to achieve the stated benefits—to improve healthcare delivery and the overall efficacy of the technology to document, transmit, and integrate EHI across multiple data systems.

To this end, we acknowledge that these estimated costs may not be borne solely by the developers of certified health IT and could be passed on to end-users through health IT developers' licensing, maintenance, and other operating fees and costs. We assume health IT developers may pass on up to the estimated costs of these policies, but not amounts above those estimated totals.

However, we have limited data on the fees and costs charged by health IT developers and how those fees and costs are distributed across various customer organizations. Given the ongoing nature of updates made by ONC to the Certification Program, EHR developers may have already built in the costs associated with making these updates in their existing contracts. To the extent the costs associated with the updates have not been taken into account, these costs may be passed on to end-users in different ways by developers of certified health IT and across different health care provider organization types. Large integrated healthcare systems may face different fees and other pricing than different sized or structured health care provider organizations. The incredible diversity of the healthcare system also limits our ability to accurately model how these costs could be passed on, even if there were data available to estimate how these policies might alter the pricing models and fee rates of the nearly 400 health IT developers we estimate will be impacted.

What we can say with more certainty is the overall impact of these policies on the healthcare system as a whole. These policies affect the certified health IT used by the providers who give care to a vast majority of Americans. Nearly all

emergency room visits, hospital stays, and regular check-ups are documented and managed using certified health IT. These policies affect the interoperability of EHI for these care events and patients' electronic access to their health information. Certified health IT is now a nearly ubiquitous part of U.S. healthcare, and the costs and benefits estimated here encompass the widespread use of these technologies and their impact on all facets of care.

Overall, it is highly speculative to quantify benefits associated with the new technical requirements and standards for certification criteria we have adopted in this final rule. Emerging technologies may be used in ways not originally predicted. For example, ONC helped support the development of SMART on FHIR, which defines a process for an application to securely request access to data, and then receive and use that data. ONC could not have predicted the scale this technical approach has already achieved. Not only is it used to support major EHR products, but is also leveraged, for example, by Apple to connect its Health® App to hundreds of healthcare systems and for apps to launch on the Microsoft Azure® product. It is also speculative to quantify benefits for specific groups because benefits associated with many of ONC's policies, which advance interoperability, don't necessarily accrue to parties making the investments in developing and implementing the technologies. Benefits related to interoperability are spread across the healthcare ecosystem and can be considered a societal benefit. We have sought to describe benefits for each of the specific policies, and we welcomed comments on how to quantify these benefits across a variety of interested parties.

We note that we have rounded all estimates to the nearest dollar and that all estimates are expressed in 2022 dollars as it is the most recent data available to address all cost and benefit estimates consistently. The wages used to derive the cost estimates are from the May 2022 National Occupational Employment and Wage Estimates reported by the U.S. Bureau of Labor Statistics.[263] We also note that estimates presented in the following ''Employee Assumptions and Hourly Wage,'' ''Quantifying the Estimated Number of Health IT Developers and Products,'' and ''Number of End Users that Might Be Impacted by ONC's Proposed Regulations'' sections are used throughout this RIA.

For policies where research supported direct estimates of impact, we estimated the benefits. For policies where no such research was identified to be available, we developed estimates based on a reasonable proxy.

We note that interoperability can positively impact patient safety, efficacy, care coordination, and improve healthcare processes and other health-related outcomes.[264] However, achieving interoperability is a function of a number of factors including the capability of the technology used by health care providers. Therefore, to assess the benefits of our policies, we must first consider how to assess their respective effects on interoperability holding other factors constant.

Employee Assumptions and Hourly Wage

We have made employee assumptions about the level of expertise needed to complete the requirements in this section. Unless indicated otherwise, for wage calculations for federal employees and ONC–ACBs, we have correlated the employee's expertise with the corresponding grade and step of an employee classified under the General Schedule (GS) Federal Salary Classification, relying on the associated employee hourly rates for the Washington, DC, locality pay area as published by the Office of Personnel Management for 2022.[265] We have assumed that other indirect costs (including benefits) are equal to 100% of pre-tax wages. Therefore, we have doubled the employee's hourly wage to account for other indirect costs. We have concluded that a 100% expenditure on benefits and overhead is an appropriate estimate based on research conducted by HHS.[266] Unless otherwise noted, we have consistently used the May 2022 National Occupational Employment and Wage Estimates reported by the U.S. Bureau of Labor Statistics (BLS) to calculate private sector employee wage estimates (*e.g.,* health IT developers, health care providers, HINs, attorneys, etc.), as we believe BLS provides the most accurate and comprehensive wage data for private sector positions.[267] Just as with the General Schedule Federal Salary Classification calculations, we have assumed that other indirect costs (including benefits) are equal to 100% of pre-tax wages. We welcomed comments on our methodology for estimating labor costs.

Quantifying the Estimated Number of Health IT Developers and Products

In this section, we describe the methodology used to assess the potential impact of new certification requirements on the availability of certified products in the health IT market. This analysis is based on the number of health IT developers that certified Health IT Modules for the 2015 Edition and the estimated number of developers that will participate in the future and the number of products these developers will certify.

These estimations are based on observed and expected conformance to 2015 Edition Cures Update requirements, market consolidation, industry trends and business decisions by participating developers, and other voluntary and involuntary withdrawals from the Program. In Table 5 below, we quantify the number of participating developers and certified products for the 2011 Edition, 2014 Edition, and 2015 Edition. We found that the number of health IT developers certifying products between the 2011 Edition and 2014 Edition decreased by 22.1% and the number of certified products available decreased by 23.2%. Furthermore, we found that between the 2014 Edition and 2015 Edition the number of participating developers and certified products decreased by 38.3% and 33.9%.

[263] May 2021 National Occupational Employment and Wage Estimates, United States. U.S. Bureau of Labor Statistics. *https://www.bls.gov/oes/current/oes_nat.htm.*

[264] Nir Menachemi, Saurabh Rahurkar, Christopher A Harle, Joshua R Vest, The benefits of health information exchange: an updated systematic review, *Journal of the American Medical Informatics Association,* Volume 25, Issue 9, September 2018, Pages 1259–1265, *https://doi.org/10.1093/jamia/ocy035.*

[265] Office of Personnel and Management. 2022 General Schedule (GS) Locality Pay Tables *https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/2022/general-schedule/.*

[266] *See* U.S. Department of Health and Human Services, Office of the Assistant Secretary for Planning and Evaluation (ASPE), *Guidelines for Regulatory Impact Analysis,* at 28–30 (2016), available at *https://aspe.hhs.gov/reports/guidelines-regulatory-impact-analysis.*

[267] May 2021 National Occupational Employment and Wage Estimates, United States. U.S. Bureau of Labor Statistics. *https://www.bls.gov/oes/current/oes_nat.htm.*

TABLE 5—NUMBER OF DEVELOPERS AND PRODUCTS FOR THE 2011 EDITION, 2014 EDITION, AND 2015 EDITION

	2011 Edition	2014 Edition	Change (%)	2015 Edition	Change (%)
Participating Health IT Developers	1,017	792	−22.1	489	−38.3
Certified Products Available	1,408	1,081	−23.2	714	−33.9

Note: Counts for 2015 Edition reflect all certificates through 2021. These counts include certificates that are active and withdrawn.

We recognize that certification for 2015 Edition and 2015 Edition Cures Update is ongoing and the number of health IT developers certifying products to the 2015 Edition and 2015 Edition Cures Update is subject to change. The figures for 2015 Edition in Table 5 reflect certifications through 2021 to provide a fixed point for analysis. We have found it prudent to use certification data that represent entire calendar years, and not to use certification stats mid-year. Therefore, 2015 Edition counts do not account for all certificates as of the publication of this rulemaking.

These figures give us insight into how participation in the Program and certification for individual certification editions has changed over time—the effect of both market and regulatory forces. Given historical trends and the asymmetric costs faced by developers of certified technology with large and small client bases, we must consider the effect of certification requirements going into effect and adopted in this rulemaking on future participation in the Program to make our best estimates of the cost and benefits of this rulemaking.

Our estimates of health IT developers and certified products specifically factor in a reduction in Program participation due to non-conformance with the 2015 Edition Cures Update criterion, ''standardized API for patient and population services (''standardized API criterion''). The criterion replaces the 2015 Edition criterion, ''application access—data category request'' (''data category request criterion''). The data category request criterion required no content and exchange standard, although ONC communicated its intent to support a standard for future rulemaking and did encourage the use of the FHIR standard to meet criterion requirements. The new standardized API criterion does require FHIR as a content and exchange standard. Products that certified the data category request criterion must certify the standardized API criterion by December 31, 2022.

In the RIA for the ONC Cures Act Final Rule, we estimated that certified API products that did not support FHIR and must do so to meet regulatory requirements may face up to $1.9 million in development and other labor and maintenance costs to develop this technology for the first time (85 FR 25921). In 2018 [268] and 2021 [269] analyses, we found that support for FHIR was not common among 2015 Edition certified API products, although health IT market leaders predominantly supported the standard and used it as the content and exchange standard for their certified API technology. As of the end of 2021, our analysis of certification data found that approximately 60% of certified API developers did not support FHIR as part of their certified API technology. Considering this variation in support for the standard under the 2015 Edition and the costs faced by developers of certified health IT to meet this requirement, we expect some attrition from the Program.

Our model assumes that 1 in 4 certified API developers that do not currently support FHIR will not certify the standardized API criterion and withdraw their certificates. This is based on available market data and the historical trend of developers with small client bases to exit the Program as program requirements and their costs increase. Our estimates may change as health IT developers meet 2015 Edition Cures Update requirements and developers certify the standardized API criterion.

TABLE 6—ESTIMATED NUMBER OF DEVELOPERS AND PRODUCTS

Scenario	Estimated number of health IT developers	Estimated number of products
All Products—End of 2021	414	569
All Products—Modeled Attrition	368	502

Note: End of 2021 counts reflect active products only.

At the end of 2021, 414 health IT developers certified 569 products with active certificates for the 2015 Edition or 2015 Edition Cures Update. This is a 15% decrease in the number of health IT developers and a 20% decrease in 2015 Edition certified products, overall. Using our model of certification for the standard API criterion, we estimate an additional 11% decrease in the number of health IT developers and a 12% decrease in the number of certified products. For this RIA, we will use 368 as the number of health IT developers and 502 as the number of certified health IT products impacted by this rulemaking.

Number of End Users That Might Be Impacted by ONC's Finalized Regulations

For the purpose of this analysis, the population of end users impacted are the number of health care providers that possess certified health IT. Due to data limitations, our analysis is based on the number of hospitals and clinicians who participate in Medicare and who may be required to use certified health IT to participate in various CMS programs, inclusive of those providers who received incentive payments to adopt certified health IT as part of the Medicare EHR Incentive Program (now known as the Promoting Interoperability Program).

[268] *https://www.healthit.gov/buzz-blog/interoperability/heat-wave-the-u-s-is-poised-to-catch-fhir-in-2019.*

[269] *https://www.healthit.gov/buzz-blog/health-it/the-heat-is-on-us-caught-fhir-in-2019.*

One limitation of this approach is that we are unable to account for the impact of our provisions on users of health IT that were ineligible or did not participate in the CMS EHR Incentive Programs or current Medicare performance programs (*e.g.,* Promoting Interoperability and Advanced Payment Model (APM) programs). For example, in 2017, 78 percent of home health agencies and 66 percent of skilled nursing facilities reported adopting an EHR (*https://www.healthit.gov/data/data-briefs/electronic-health-record-adoption-and-interoperability-among-us-skilled-nursing*). Nearly half of these facilities reported engaging aspects of health information exchange. However, we are unable to quantify, specifically the use of certified health IT products, among these provider types.

Despite these limitations, these Medicare program participants represent an adequate sample on which to base our estimates. An analysis of the CMS Provider of Services file for Hospitals (*https://data.cms.gov/provider-characteristics/hospitals-and-other-facilities/provider-of-services-file-hospital-non-hospital-facilities*) and CMS National Downloadable File of Doctors and Clinicians (*https://data.cms.gov/provider-data/dataset/mj5m-pzi6*) provides a current accounting of Medicare-participating hospitals and practice locations. In total, we estimated about 4,800 non-federal acute care hospitals from the Provider of Services file and 1.25 million clinicians (including doctors and advanced nurse practitioners) across over 350,000 practice locations. If we assume that 96% of these hospitals and 80% of these practice locations use certified health IT, as survey data estimate, approximately 4,600 hospitals and 283,000 practice locations may face some passed-on costs from these requirements.

We understand there will likely not be a proportional impact of these costs across all health care providers. We can assume a hospital will face different costs than a physician practice, and no two hospitals will face the same costs, as those costs may vary based upon various characteristics, including but not limited to: staff size, patient volume, and ownership. The same is true for individual clinical practices, for which costs may vary across the same characteristics as hospitals. However, given our limited data, our approach to model pass-through costs onto health care providers assumes that hospitals face the same average costs and that they face a higher average cost per site than an individual clinical practice. Furthermore, we assume that clinical practices face the same average costs and lower average costs per site than the average hospital.

Based upon our prior modeling work for the ONC Cures Act Final Rule (*https://www.federalregister.gov/documents/2020/05/01/2020-07419/21st-century-cures-act-interoperability-information-blocking-and-the-onc-health-it-certification*), we assume that one-third of estimated costs will be passed on to hospitals and the remaining amount on to clinician practices. Table 7 shows an assumed distribution of the costs across technology users. The cost to any one hospital or practice is small compared to the cost as a whole. The average hospital user of certified health IT could be expected to face up to $65,217 in average additional costs associated with implementing technology that adopt these policies. The average clinician practice site could be expected to face up to $2,170 in average additional costs associated with implementing technology that adopt these policies. These are considered pass-through costs incurred by the health IT developer to adopt these policies and not additional costs exogenous to health IT developer efforts to adopt and engineer these policies into their certified health IT.

TABLE 7—MODEL OF COST DISTRIBUTION BASED ON ESTIMATED NUMBER OF HOSPITALS AND CLINICAL PRACTICES WITH CERTIFIED HEALTH IT

Health care provider	Est. count	Est. $ per provider	Total $ cost (m)
Hospitals	4,600	65,217	300
Clinical Practices	283,000	2,170	614
All	287,600	3,178	914

These costs are not expected to be borne at once. Requirements from this finalized rulemaking may be implemented over several years, so in some cases an individual hospital or clinician's share of pass-through costs from their health IT developer may be distributed over one or more years. One issue to reiterate is that some of these costs may have already been incorporated within existing contracts and thus it is possible that the actual additional costs experienced by hospitals and clinicians may be lower than what is estimated. We do not have insights into proprietary contracts between EHR developers and their clients, and thus cannot speculate the extent to which the estimated additional costs will be passed on to their clients.

It's unknown if the estimated benefits will have the same distribution. A single clinician may not benefit the same as a single hospital, nor will one hospital benefit the same as another. However, given the same constraints to model costs across different provider types, we must assume a similar distribution for benefits as we propose for costs.

General Comments on the RIA

Comments. Commenters were generally concerned with unmeasured costs on entities beyond developers of certified health IT, including public health authorities, health care providers, and patients, noting that the proposed regulations have effects beyond developers of certified health IT.

Response. We appreciate these comments and understand concerns about the broader overall downstream impact of the proposed rulemaking on entities beyond developers of certified health IT, which are specifically regulated by ONC authorities. The impact analysis measures the estimated costs for developers of certified health IT to meet the proposed new Certification Program requirements—for example, to develop or modify the technical functionality of their certified health IT or adopt a new standard or standard version. These are the expected direct costs of the proposals on developers of certified health IT. However, we recognize that developers of certified health IT are largely private businesses who operate in a competitive marketplace and that they may not bear all costs to meet these requirements. We include in the ''Costs and Benefits'' section of the Regulatory Impact Analysis the estimated impact on certified health IT end users. In this case, health care providers, such as

hospitals and clinicians. We believe these estimates provide a general, but not necessarily comprehensive, understanding of the possible pass-through costs borne by users of certified health IT.

Comments. Several commenters provided suggestions to broaden the scope and depth of the regulatory impact analysis, with specific recommendations to include patient-level measures.

Response. We appreciate commenters' thoughtful suggestions to build upon the proposed regulatory impact analysis, however, we're confident that the impact analysis provides the correct measurement of quantifiable costs and benefits. Though patient-level impacts are inherent to technology use, given the interconnectedness of healthcare, we believe that patient impacts are more directly tied to the implementation of the technology and not to its development and sale. It is hard to predict the effect on patient outcomes of one unique software technology from another, given that developers may choose to differentiate their product offerings to provide choices and competitive options to their customers. Furthermore, how the technology end-user, here defined as the health care provider, chooses to use the technology can affect outcomes for patient care, exogenous to the requirements that must be met by the developers of certified health IT, as part of Certification Program participation. Disentangling or singling out differential impacts of how technology is used and how it was designed or developed to be used is difficult to do and out of scope for this impact analysis.

Comments. Several commenters expressed concerns about the total costs measured and limited quantified benefits for this proposed rulemaking and the broader impact of these costs on end-users, who must adopt, learn, and use new versions of certified health IT.

Response. We understand commenters' concerns about the estimated cost amounts for the proposed rulemaking and acknowledge the limited quantifiable benefits for some of these proposals. The ONC Health IT Certification Program, although voluntary, attracts participation from hundreds of developers who certify hundreds of health IT products. The impact analysis assesses the expected costs and benefits across all these developers and products. The high rates of certified health IT use further show the expansive market for health IT. In the ''Costs and Benefits'' section of the Regulatory Impact Analysis, we estimate the expected costs on certified health IT end-users, here defined as the health care provider. When costs are distributed across these end users, we see the expected average costs passed on to individual health care providers. We recognize the hardships faced by health care providers to finance technology upgrades and pay for new software versions that incorporate the final rule's updates. We believe the benefits from interoperability improvements, transparency, patient access, and increased data sharing outweigh those costs.

''The ONC Certification Criteria for Health IT'' and Discontinuing Year Themed ''Editions''

As discussed in section III.A of this preamble, we proposed to rename § 170.315 as the ''ONC Certification Criteria for Health IT'' and replace all references throughout 45 CFR part 170 to the ''2015 Edition'' with this new description (this would impact §§ 170.102, 170.405, 170.406, 170.523, 170.524, and 170.550).

Costs

This policy is not intended to place additional burden on developers of certified health IT and does not require new development or implementation. We expect the costs associated with attesting to these criteria to be de minimis because we do not expect any additional effort on the part of health IT developers.

Benefits

Maintaining a single set of ''ONC Certification Criteria for Health IT'' will create more stability for the health IT community and Program partners and make it easier for developers of certified health IT to maintain their product certificates over time. For example, when new rules are released, unchanged certification criteria will remain exactly as they are, rather than being placed in a new CFR section and requiring health IT developers to seek an updated certificate attributed to the new CFR section.

Comments. We received no comments on this impact analysis.

Response. We have finalized the impact analysis as proposed.

United States Core Data for Interoperability Version 3 (USCDI v3)

As discussed in section III.C.1 of this preamble, we have finalized to update the USCDI standard in § 170.213 by adding USCDI v3 and by establishing an expiration date for USCDI v1 (July 2020 Errata) on January 1, 2026, for purposes of the Program. We have finalized to add USCDI v3 in § 170.213(b) and incorporate it by reference in § 170.299. We have finalized to codify the existing reference to USCDI v1 (July 2020 Errata) in § 170.213(a). We have finalized that as of January 1, 2026, any Health IT Modules seeking certification for criteria referencing § 170.213 would need to be capable of exchanging the data classes and data elements that comprise USCDI v3. Additionally, once the USCDI standard in § 170.213 is updated to include USCDI v3, we have finalized that in order for previously certified Health IT Modules to maintain certification, health IT developers would be required to update their certified Health IT Modules to be capable of exchanging the data classes and data elements that comprise USCDI v3 for all certification criteria referencing § 170.213 by December 31, 2025. USCDI, via cross-reference to § 170.213, is currently referenced in the following criteria, each of which would refer to USCDI v1 and USCDI v3 until December 31, 2025 and only to USCDI v3 thereafter:

- ''Care coordination—transitions of care—create'' (§ 170.315(b)(1)(iii)(A)(*1*)).
- ''Care coordination—clinical information reconciliation and incorporation—reconciliation'' (§ 170.315(b)(2)(iii)(D)(*1*) through (*3*));
- ''Patient engagement—view, download, and transmit to 3rd party—view'' (§ 170.315(e)(1)(i)(A)(*1*)).
- ''Design and performance—consolidated CDA creation performance'' (§ 170.315(g)(6)(i)(A)).
- ''Design and performance—application access—all data request—functional requirements'' (§ 170.315(g)(9)(i)(A)(*1*)); and
- ''Design and performance—standardized API for patient and population services—data response'' (§ 170.315(g)(10)(i)(A) and (B)).

We note that § 170.315(f)(5) also currently references § 170.213. However, we have finalized to rely on specific implementation guides for this certification criterion, rather than referencing § 170.213. Health IT Modules certified to § 170.315(f)(5) are no longer required to support USCDI, as finalized by this rule.

Costs

The USCDI v3 adds five new data classes and 46 new data elements that were not in USCDI v1. This will require updates to the Consolidated Clinical Document Architecture (C–CDA) standard, the FHIR US Core Implementation Guide, and updates to the criteria listed above. We have estimated the cost to health IT developers to add support for the additional data classes and data

elements in USCDI v3 in C–CDA, and to make the necessary updates to the affected certification criteria. These estimates are detailed in Table 8 below and are based on the following assumptions:

1. Health IT developers will experience the assumed average costs of labor and data model use. Table 8 shows the estimated labor costs per product for a health IT developer to develop support for the additional data elements and data classes in USCDI v3 for each affected certification criteria. We recognize that health IT developer costs will vary; however, our estimates in this section assume all health IT developers will incur, on average, the costs noted in Table 8.

2. We estimate that 346 products certified by 269 developers will be affected. These estimates are a subset of the total estimated health IT developers and certified products we estimated above.

We estimate that, in total, 368 health IT developers will certify 502 health IT products impacted by this policy. However, not all these developers and products certify USCDI applicable criteria and need to meet the USCDI update requirements. As of the end of 2021, 73% of developers and 69% of products certified to one of the USCDI applicable criteria, listed above. We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by the USCDI updates. In Table 9, we also applied separate modifiers for individual criteria, calculated from an analysis of certificates through 2021. This allows us to assess USCDI update costs more accurately for individual criterion.

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91. As noted previously, we have assumed that other indirect costs (including benefits) are equal to 100 percent of pre-tax wages, so the hourly wage including other indirect costs is $127.82.

TABLE 8—COSTS TO HEALTH IT DEVELOPERS TO DEVELOP SUPPORT FOR THE ADDITIONAL USCDI DATA ELEMENTS IN AFFECTED CERTIFICATION CRITERIA

Tasks	Details	Lower bound hours	Upper bound hours	Remarks
Update C–CDA creation	New development to support USCDI v2 and v3 updates and changes to data classes and constituent data elements for C–CDA and C–CDA 2.1 Companion Guide.	1,800	3,600	(1) Lower bound assumes health IT product was voluntarily updated through the ONC Standards Version Advancement Process (SVAP) and USCDIv2 data elements are incorporated in the certified product. (2) Upper bound assumes certified product conforms only to USCDIv1 and needs to be updated to fully conform with USCDIv3.
§ 170.315(b)(1)(iii)(A)(*1*) Care coordination—Transitions of care—Create.	New development to support USCDI v2 and v3 updates and changes to data classes and constituent data elements for C–CDA and C–CDA 2.1 Companion Guide.	200	600	Necessary updates to health IT to support the new data classes and data elements to meet the criteria requirements.
§ 170.315(b)(2)(iii)(D)(*1*) through (*3*) Care coordination—Clinical information reconciliation and incorporation—Reconciliation.	New development to support USCDI v2 and v3 updates and changes to data classes and constituent data elements for C–CDA and C–CDA 2.1 Companion Guide.	200	600	Necessary updates to health IT to support the new data classes and data elements to meet the criteria requirements.
§ 170.315(e)(1)(i)(A)(*1*) Patient engagement—View, download, and transmit to 3rd party—View.	New development to support USCDI v2 and v3 updates and changes to data classes and constituent data elements for C–CDA and C–CDA 2.1 Companion Guide.	200	600	Necessary updates to health IT to support the new data classes and data elements to meet the criteria requirements.
§ 170.315(g)(6)(i) Design and performance—Consolidated CDA creation performance.	New development to support USCDI v2 and v3 updates and changes to data classes and constituent data elements for C–CDA and C–CDA 2.1 Companion Guide.	200	600	Necessary updates to health IT to support the new data classes and data elements to meet the criteria requirements.
§ 170.315(g)(9)(i)(A)(*1*) Design and performance—Application access—all data request—Functional requirements.	New development to support USCDI v2 and v3 updates and changes to data classes and constituent data elements for C–CDA and C–CDA 2.1 Companion Guide.	200	600	Necessary updates to health IT to support the new data classes and data elements to meet the criteria requirements.
§ 170.315(g)(10)(i)(A) and (B) Design and performance—Standardized API for patient and population services—Data response.	New development to support USCDI v2 and v3 updates and changes to data classes and constituent data elements for C–CDA and C–CDA 2.1 Companion Guide.	200	600	Necessary updates to health IT to support the new data classes and data elements to meet the requirements.

TABLE 9—TOTAL COST TO DEVELOP SUPPORT FOR THE ADDITIONAL USCDI DATA ELEMENTS IN AFFECTED CERTIFICATION CRITERIA

[2022 Dollars]

Tasks	Estimated number of products	Estimated cost	
		Lower bound	Upper bound
Update C–CDA creation	346	$79,718,400	$159,436,800
Updates to § 170.315(b)(1)	281	7,193,600	21,580,800
Updates to § 170.315(b)(2)	261	6,681,600	20,044,800
Updates to § 170.315(e)(1)	246	6,297,600	18,892,800
Updates to § 170.315(g)(6)	341	8,729,600	26,188,800
Updates to § 170.315(g)(9)	276	7,065,600	21,196,800
Updates to § 170.15(g)(10)	276	7,065,600	21,196,800

TABLE 9—TOTAL COST TO DEVELOP SUPPORT FOR THE ADDITIONAL USCDI DATA ELEMENTS IN AFFECTED CERTIFICATION CRITERIA—Continued

[2022 Dollars]

Tasks	Estimated number of products	Estimated cost	
		Lower bound	Upper bound
Total Cost	346	122,752,000	288,537,600

Notes: The number of estimated products that certify applicable criteria vary. We estimated separate modifiers for each certification criterion to estimate the number of products impacted by the USCDI updates. Estimates reflect the percent of all products that certify a criterion through 2021, except. Modifiers: (b)(1): 56%; (b)(2): 52%; (e)(1): 49%; (g)(6): 68%; (g)(9): 55%. This estimate is subject to change.

The cost to a health IT developer to develop support for the additional USCDI data classes and elements vary by the number of applicable criteria certified for a Health IT Module. On average, the cost to update C–CDA creation to support the additional USCDI data elements range from $230,400 to $460,800 per product. The cost to make updates to individual criteria to support the new data classes and elements range from $25,600 to $76,800 per product. Therefore, assuming 346 products overall and a labor rate of $128 per hour, we estimate that the total cost to all health IT developers will, on average, range from $123 million to $289 million. This will be a one-time cost to developers per product that is certified to the specified certification criteria and will not be perpetual.

Benefits

We believe this policy will benefit health care providers, patients, and the industry collectively. The USCDI comprises a core set of structured and unstructured data needed to support patient care and facilitate patient access to health information using health IT; establishes a consistent baseline of harmonized data elements that can be broadly reused across use cases, including those outside of patient care and patient access; and will expand over time via a predictable, transparent, and collaborative process, weighing both anticipated benefits and industry-wide impacts. In Standards Bulletin 2022–2,[270] we noted that based on these principles and the established prioritization criteria, USCDI v3 contains data elements whose collection and exchange promote equity, reduce disparities, and support public health data interoperability as discussed in Standards Bulletin 2021–3,[271] where we highlighted that the collection, access, use, and reporting of SDOH as well as sexual orientation and gender identity data can help identify and address differences in health equity and improve health outcomes at an individual and population level. The additional data elements in USCDI v3 expand the baseline set of data available for health information exchange and thus provide more comprehensive health data for both providers and patients. We expect the resulting improvements to interoperable exchange of health information to significantly benefit providers and patients and improve the quality of healthcare provided. In addition, we believe the increased availability of the additional data elements in USCDI v3 as interoperable structured data will facilitate improvements in the efficiency, accuracy, and timeliness of public health reporting, quality measurement, health care operations, and clinical research. However, we are not aware of an approach for quantifying these benefits and welcomed comments on potential approaches to quantifying these benefits.

Comments. We received no comments regarding the impact analysis for required adoption of USCDI v3 by applicable developers of certified health IT.

Response. The final impact analysis is consistent with the proposed rulemaking. Cost estimates were updated to reflect wages of software developers as of 2022.

Electronic Case Reporting

In section III.C.4 of this preamble, we discuss the finalized updates to the 2015 Edition certification criterion for ''transmission to public health agencies—electronic case reporting'' that would require developers of certified health IT to adopt specific electronic standards to support functional requirements that were previously adopted as part of the § 170.315(f)(5) certification criterion. We have finalized as proposed that Health IT Modules certified to this criterion must enable a user to: (i) create an electronic initial case report (eICR) according to at least the Health Level Seven (HL7) Clinical Document Architecture (CDA) eICR implementation guide (IG) or the eICR profiles defined in the HL7 Fast Health Interoperability Resources (FHIR) eCR IG and (ii) consume and process a reportability response (RR) according to at least the HL7 CDA RR IG or the RR profiles defined in the HL7 FHIR eCR IG. For the standards-based requirements in § 170.315(f)(5)(i) through (ii), we have finalized as proposed that Health IT Modules support all ''mandatory'' and ''must support'' data elements as applicable in the respective implementation guides (IGs). We have also finalized as proposed that Health IT Modules support the use of a version of the Reportable Conditions Trigger Code (RCTC) value set in § 170.315(f)(5)(1)(B) for determining potential case reportability.

Costs

This section describes the estimated costs of meeting the requirements in the updated ''transmission to public health agencies—electronic case reporting'' criterion. The cost estimates are based on the following assumptions:

- *Health IT developers will experience the assumed average costs of labor and data model use.* Tables 10–11 show the estimated labor costs per product for a health IT developer to meet the requirements in the eCR certification criterion. We recognize that health IT developer costs will vary; however, our estimates in this section assume all health IT developers will, on average, incur the costs noted in the tables below.
- *The number of products that will update to the new eCR criterion is estimated based on the total number of currently certified products plus the number of new products we expect to certify to the eCR criterion.* Both estimates are adjusted for attrition. As of 2021, 54 developers certified 63 products to the eCR certification criterion or 13% of developers and 11% of products. Beginning in 2022, CMS

[270] *https://www.healthit.gov/sites/default/files/page/2022-07/Standards_Bulletin_2022-2.pdf.*

[271] *https://www.healthit.gov/sites/default/files/page/2021-07/Standards_Bulletin_2021-3.pdf.*

required eligible hospitals and critical access hospitals in the Medicare Promoting Interoperability Program and eligible clinicians reporting on the Promoting Interoperability performance category in MIPS to report on use of eCR as part of the Public Health and Clinical Data Exchange Objective. The Electronic Case Reporting measure was optional in prior program years. Due to this new program requirement, we expect more Health IT Modules to certify the criterion in the coming year(s). As a proxy for possible future certification of eCR, we used the number of products that are currently certified to § 170.315(f)(1) (transmission to immunization registries) to estimate future certification of the eCR criterion. As of 2021, 31% of developers and 28% of products certified to the immunization criterion, but not the eCR certification criterion. We used these rates to estimate future certification of the eCR criterion. We estimate that 368 developers will certify 502 products impacted by this rulemaking. We estimate updates to the eCR certification criterion will impact 141 products certified by 114 developers for the first time (''New'') and 55 products already certified by 48 developers (''Current'') for an estimated total of 196 products certified by 162 developers.

• *Wages are determined using BLS estimates.* According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91.[272] We assume that other indirect costs (including benefits) are equal to 100 percent of pre-tax wages, so the hourly wage, including other indirect costs, is $127.82.

TABLE 10—ESTIMATED LABOR HOURS TO MEET eCR CERTIFICATION REQUIREMENTS—NEW PRODUCTS

Activity	Details	Estimated labor hours		Remarks
		Lower bound	Upper bound	
Task 1: Case Report Creation.	(1) Enable a user to create a case report for electronic transmission according to (i) eICR profiles of HL7 FHIR eCR IG, or (ii) HL7 CDA eICR IG; (2) Support RCTC value set.	1,000	1,500	(1) Lower bound assumes health IT product has begun to implement at least one of the two IGs. (2) Upper bound assumes health IT product does not support either IG or has not begun to implement.
Task 2: Case Report Response Receipt.	Health IT Module must be able to consume and process a reportability response according to (1) RR profiles of HL7 FHIR eCR IG, or (2) HL7 CDA RR IG.	1,000	1,500	(1) Lower bound assumes health IT product has begun to implement at least one of the two IGs. (2) Upper bound assumes health IT product does not support either IG or has not begun to implement.
Task 3: Support for Reporting.	Health IT Module must be able to report to a system capable of receiving case reports electronically.	0	160	(1) Lower bound assumes that health IT already has the technical pre-requisites for reporting but is not yet connected to platform or method to enable reporting. (2) Upper bound assumes health IT does not have technical pre-requisites for reporting (*e.g.,* no support for electronic connection and no support for available exchange methods).

TABLE 11—ESTIMATED LABOR HOURS TO MEET eCR CERTIFICATION REQUIREMENTS—CURRENTLY CERTIFIED PRODUCTS

Activity	Details	Estimated labor hours		Remarks
		Lower bound	Upper bound	
Task 1: Case Report Creation.	(1) Enable a user to create a case report for electronic transmission according to (i) eICR profiles of HL7 FHIR eCR IG, or (ii) HL7 CDA eICR IG; (2) Support RCTC value set.	0	1,000	(1) Lower bound assumes health IT product has already implemented at least one of the two IGs. (2) Upper bound assumes health IT product has begun to implement at least one of the two IGs.
Task 2: Case Report Response Receipt.	Health IT Module must be able to consume and process a reportability response according to (1) RR profiles of HL7 FHIR eCR IG, or (2) HL7 CDA RR IG.	0	1,000	(1) Lower bound assumes health IT product has already implemented at least one of the two IGs. (2) Upper bound assumes health IT product has begun to implement at least one of the two IGs.
Task 3: Support for Reporting.	Health IT Module must be able to report to a system capable of receiving case reports electronically.	0	160	(1) Lower bound assumes health IT already supports at least one reporting option, such as to the AIMS platform, state-based registries or health information exchanges. (2) Upper bound assumes health IT does not have technical pre-requisites for reporting (e.g., no support for electronic connection and no support for available exchange methods).

Total Costs, *TC* can be represented by the following equation:

$$TC = p_c\left[\sum_{k=1}^{3} h_k w + h_r w\right] + p_n\left[\sum_{k=1}^{3} h_k w + h_r w\right]$$

[272] *https://www.bls.gov/oes/current/oes151252.htm.*

Number of currently certified products, p_c = 55
Number of new certified products, p_n = 141
Fully loaded wage, w = 127.82
Labor hours for IG implementation, h_k, for each profile or IG, k
Labor hours for reporting, h_r

TABLE 12—EXAMPLE CALCULATION FOR THE LOWER BOUND ESTIMATED COST TO NEW PRODUCTS TO PERFORM TASK 1 IN TABLE 10 TO MEET eCR CERTIFICATION REQUIREMENTS

Activity	Estimated labor hours	Developer salary	Projected products
	Lower bound		
Task 1	1,000 hours	$127.82 per hour	141 products
Example Calculation: 1,000 hours * $127.82 * 141 products = $18,022,620.			

TABLE 13—COSTS TO MEET eCR CERTIFICATION REQUIREMENTS—NEW PRODUCTS

Activity	Estimated labor hours	
	Lower bound	Upper bound
Task 1 (141 products)	$18,022,620	$27,033,930
Task 2 (141 products)	18,022,620	27,033,930
Task 3 (141 products)	0	2,883,619
Total Cost	36,045,240	56,951,479

TABLE 14—COSTS TO MEET eCR CERTIFICATION REQUIREMENTS—CURRENTLY CERTIFIED PRODUCTS

Activity	Estimated cost	
	Lower bound	Upper bound
Task 1 (55 products)	$0	$7,030,100
Task 2 (55 products)	0	7,030,100
Task 4 (55 products)	0	1,124,816
Total Cost	0	15,185,016

TABLE 15—COSTS TO MEET eCR CERTIFICATION REQUIREMENTS—ALL PRODUCTS

Activity	Estimated cost	
	Lower bound	Upper bound
Task 1 (196 products)	$18,022,620	$34,064,030
Task 2 (196 products)	18,022,620	34,064,030
Task 3 (196 products)	0	4,008,435
Total Cost	36,045,240	72,136,495

Based on the stated assumptions and costs outlined in Tables 13–15, the total estimated cost for certified health IT products to meet the finalized eCR certification criterion requirements will range from $36 million to $72.1 million. Assuming 162 health IT developers, there will be an average cost per developer ranging from $222,501 to $445,287, with an average cost per product ranging from $255,640 to $403,911 for new products and $0 to $276,091 for currently certified products.

Benefits

The primary benefit of adopting standards-based requirements for the eCR certification criterion is to improve consistency and promote interoperability over time. eCR is one of the pillars of ONC's and CMS' broader efforts to support effective healthcare data interoperability, which ensures that electronic health information is shared appropriately between healthcare organizations and public health agencies (PHAs) in the right format, through the right channel at the right time.[273] Adopting a standards-based approach to eCR facilitates the exchange of health information between healthcare and public health by requiring the use of a common format for the creation of case reports and processing of a reportability response.

Potential benefits of a centralized approach to eCR have been assessed in an Association of State and Territorial Health Officials (ASTHO)-sponsored economic analysis of the efficiencies gained at PHAs by using centralized eCR services through the Association of Public Health Laboratories (APHL) Informatics Messaging Services (AIMS) platform, rather than using localized eCR solutions or manual, paper-based methods.[274] A key component of this service is the inclusion of the CDC

[273] *https://www.cdc.gov/datainteroperability/index.html.*

[274] *https://www.aphl.org/programs/informatics/Pages/aims_platform.aspx.*

supported Council of State and Territorial Epidemiologists' (CSTE) developed decision support tool, Reportable Condition Knowledge Management System (RCKMS), which helps determine whether initial case reports are reportable in specific public health jurisdictions and eliminates confusion regarding where reports should be sent.[275] [276] According to the analysis, centralized eCR components could provide, ''$2.5 million in increased efficiency per jurisdiction over 15 years'' compared to manual reporting and ''$310,000 of net benefits over 15 years'' compared to localized eCR solutions.[277]

Benefits of eCR to the healthcare sector and public health that will be promoted through standards adoption:

- Automatic, complete, accurate data reported in real-time (faster and more complete than manual entry) facilitates evidence-based decision-making for public health.
- Directly benefits public health response efforts by supporting situational awareness, case management, contract tracing, and efforts to coordinate isolation.
- Helps improve public health efficiency for evaluation and follow-up by providing PHAs with higher quality patient and clinical data in a timely manner.
- Reduces reporting burden for health care providers without disrupting clinical workflow, which can result in time and cost savings for the healthcare sector.
- Fulfills legal reporting requirements as well as CMS PI Program requirements for eCR, meaning benefits to public health would not come at an additional cost to health care providers who are already required to report.
- Streamlines reporting to multiple jurisdictions.

Benefits of certification criterion update:

- Adoption of standards for eCR will improve consistency and interoperability over time.
- Consistency in the reporting of specific data elements will increase the efficiency of exchange (*e.g.,* by facilitating automated reporting, enabling RCKMS and PHA processing of eICRs and bi-directional communication between providers and public health).
- RCTC value set establishes a baseline for use in the Program and enables developers of certified health IT to support newer or updated versions of RCTC value sets as soon as new releases are available.

Comments. We received no comments regarding the impact analysis for updates to the electronic care reporting criterion.

Response. The final impact analysis is consistent with the proposed rulemaking. Cost estimates were updated to reflect wages of software developers as of 2022.

Decision Support Interventions and Predictive Models

In section III.C.5 of this preamble, we have finalized the proposed new certification criterion for ''decisions support interventions'' in § 170.315(b)(11) with modifications, including more clearly separating technical functionality and ongoing maintenance for transparency purposes. The intent of this certification criterion is to ensure the availability of sufficient information on decision support interventions based on predictive models, including machine learning and artificial intelligence, through a more comprehensive list of source attributes and through the conduct and documentation of risk management activities. That information is intended to enable the selection and use of fair (*i.e.,* unbiased), appropriate, valid, and effective interventions. The certification criterion also would provide additional transparency into evidence-based decision support interventions by requiring that products allow decision support to be enabled based on specific data classes.

Alternatives Considered

We considered several alternative regulatory approaches, but believe this approach implies the lowest burden of available options while having a high likelihood of impacting decision-making. Because we seek to address a market failure related to inadequate and asymmetric information, we proposed an informational intervention. The approach is market-oriented and aimed at ensuring that model purchasers and users have sufficient information to select and use models responsibly. We believe that several alternative approaches, such as performance or design standards would imply substantially higher regulatory burden and are inappropriate given the ongoing research and development in this area and uncertainty inherent in predictive model development.

Rather than mandatory reporting, we considered the potential for a voluntary database to which model developers might report information on the quality of their models. However, we are concerned that such a database would achieve relatively low participation because of disincentives for some developers to make the performance of their models' public. We believe that the current approach in which we have required reporting of a set of core source attributes that we strongly believe should be available for all models (*e.g.,* intended use) and reporting of other attributes (*e.g.,* external validation results) as required if available but otherwise providing the option to clearly label as missing, is a more effective balance between prescriptive requirements and voluntary participation. Given the national availability of many models, Federal regulation is beneficial to set a common set of expectations across the national market.

Costs

This section describes the estimated costs of the ''Decision Support Intervention'' certification criterion and associated maintenance of certification requirements. The cost estimates are based on the following assumptions:

- *Health IT developers will experience the assumed average costs of labor and data model use.* Table 16 shows the estimated labor costs per product for a health IT developer to develop support for the predictive decision support certification criterion. We recognize that health IT developer costs will vary; however, our estimates in this section assume all health IT developers will, on average, incur the costs noted in Table 16.
- *The number of health IT developers and products certified will closely align with certification of the 2015 Edition clinical decision support (CDS) criterion.* We estimate that 301 products certified by 243 developers will be affected by our policy. These estimates are a subset of the total estimated health IT developers and certified products we estimated above. We estimate that, in total, 368 health IT developers will certify 502 health IT products impacted by this rulemaking. However, we estimate that not all these developers and products will certify the new Decision Support Intervention criterion. As of the end of 2021, 66% of developers and 60% of products certified to the *CDS* criterion. We assume that all products certified to the CDS criterion will certify the new

[275] CSTE Surveillance/Informatics: Reportable Conditions Knowledge Management Systems. CSTE website. *http://www.cste.org/group/RCKMS.*

[276] *https://ecr.aimsplatform.org/cms/resources/blocks/digital-bridge-ecr-evaluation-report-12-32019.pdf.*

[277] Cooney MA, Iademarco MF, Huang M, MacKenzie WR, Davidson AJ. The public health community platform, electronic case reporting, and the digital bridge. Journal of Public Health Management and Practice. 2018 Mar 1;24(2):185–9.

Decision Support Intervention criterion. We, therefore, use certification of the CDS criterion as a proxy for the percent of developers and products that will certify the Decision Support Intervention criterion in the future. We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products that will certify this criterion and be impacted by the costs of this new criterion.

• *Wages are determined using BLS estimates.* According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91.[278] We assume that other indirect costs (including benefits) are equal to 100 percent of pre-tax wages, so the hourly wage, including other indirect costs, is $127.82.

We believe developers will expend substantial initial effort to develop the technical capabilities to support the criterion and that their effort will be varied depending on the extent, scope, and scale necessary on their part to develop initial documentation related to source attributes and intervention risk management as required as part of their maintenance of certification to this certification criterion. In this final rule, we require that developers maintain and keep current information source attribute information for certain decision support interventions. We also have finalized requirements for an annual review of risk management information and documentation. We believe that both requirements imply sustained annual effort, which we have estimated in Table 16. However, we have constrained the scope of responsibility for developers of certified health IT under this final rule.

TABLE 16—ESTIMATED LABOR HOURS TO DEVELOP AND MAINTAIN UPDATED DECISION SUPPORT FUNCTIONALITY

Activity	Lower bound hours	Upper bound hours	Remarks
Task 1: Update decision support tools to enable interventions based on additional data classes and enable selection of Predictive DSI.	1,000	1,600	(1) Lower bound assumes health IT already has developed decision support modules that only need to be updated for new data classes. (2) Upper bound assumes further data-structure related work is necessary to facilitate CDS based no additional classes.
Task 2: Enable end-users to provide feedback on evidence-based DSI.	200	1,000	(1) Lower bound assumes that developers have already developed feedback capabilities and will need to make limited updates to the reporting of that information. (2) Upper bound assumes that developer's current capability to support feedback on decision support needs to be significantly enhanced to support enabling end-users to provide effective feedback and to create reports from that feedback.
Task 3: Provide users the ability to record, change and access source attribute information.	1,000	2,000	(1) Lower bound assumes that existing tools used to create similar forms or documents can be adapted to this purpose. (2) Upper bound assumes a higher burden due to more novel development.
Task 4: Provide complete and up-to-date source attribute information for Predictive DSI supplied by the developer.	0 annually	800 annually	We expect a wide range of effort based on the extent to which developers make DSI available in the future, and whether they author Predictive DSI s available. For those that author Predictive DSI in the future and, we believe that evaluating and reporting source attributes for those Predictive DSI will imply substantial costs.
Task 5: Additional effort to provide information for source attributes related to Predictive DSI available as of December 31, 2024.	0	1,600	We expect a wide range of effort based on the extent to which EHR developers currently author Predictive DSI s. For those that do author predictive decision supported interventions and do not currently evaluate the models on the attributes included, we believe doing so will imply substantial costs.
Task 6: Engage in risk management and annually update risk management information.	0 annually	285 annually	We expect a wide range of effort based on the extent to which EHR developers currently author or execute Predictive DSI s. The total hours estimated to conduct real world testing per developer were 1,140 annually and that accounted for numerous criteria included as eligible for real world testing. We believe that conducting intervention risk management for (b)(11), including the provision of risk management documentation, would require a fraction of that time equivalent to one quarter of the time for real world testing.
Task 7: Additional initial engagement in risk management and updating risk management information available as of December 31, 2024.	0	570	The total hours estimated to conduct real world testing per developer were 1,140 annually and that accounted for numerous criteria included as eligible for real world testing. We believe that conducting initial intervention risk management for, including the provision of risk management documentation, would require time equivalent to about one quarter of the time for real world testing.

Table 17 provides the overall costs projecting that 301 products will be certified to the criterion.

[278] *https://www.bls.gov/oes/current/oes151252.htm.*

TABLE 17—TOTAL COST TO DEVELOPERS TO DEVELOP AND MAINTAIN UPDATED DECISION SUPPORT FUNCTIONALITY

	Projected products	Estimated Total Cost (10 year) (assuming software developer pay of $58.17 per hour software developers (*bls.gov*))	
		Lower bound	Upper bound
Task 1	301	$38,473,820	$61,558,112
Task 2	301	7,694,764	38,473,820
Task 3	301	38,473,820	76,947,640
Task 4	301	0	307,790,560
Task 5	301	0	61,558,112
Task 6	301	0	109,650,387
Task 7	301	0	21,930,077
Total	.....	84,642,404	677,908,708

Benefits

Predictive DSIs are common, with some individual interventions being applied to tens or hundreds of millions of individuals despite, in some cases, crucial insufficiencies in the performance of those models.[279] However, there are a wide range of potential applications of Predictive DSI, and we believe that the healthcare delivery field is far from fully adopting these interventions in the circumstances where they would be beneficial. Because Predictive DSIs are currently, and potentially can be, applied to a wide range of contexts, comprehensively estimating quantitative benefits from improved interventions and underlying models is challenging, and for some types of benefits infeasible. However, we have generated some quantitative benefits related to the scope of potential cost savings and have identified additional benefits, characterized qualitatively, to the adopted certification criterion and its associated maintenance of certification requirements.

We believe that the most directly quantifiable benefits of the adopted changes to predictive decision support relate to increased use of more accurate and effective Predictive DSIs.[280] We believe that increased transparency into the performance of models and risk management practices related to their development will result in (1) wider uptake of Predictive DSIs overall due to greater certainty about the intervention's performance, and (2) selection of fairer, more appropriate, more accurate, more effective and safer models through greater information on the available choices. However, we acknowledge that there is substantial uncertainty in the degree to which the policy will result in wider uptake and use of more effective interventions.

Given the sheer number of algorithms and applicable conditions and uses, we have selected two relevant scenarios—sepsis onset and ambulatory care sensitive admission—which have a fair amount of supporting research, to show the potential benefits of our policy. First, in patient populations in whom the risk of sepsis is moderate to high, risk-assessments based on patient factors and characteristics (*i.e.,* data elements) are (or should be) made for implementing rapid risk-based patient care. The potential impact of using Predictive DSIs to more effectively conduct these risk-assessments can illustrate the benefits. Admissions for sepsis cost $24 billion per year [281] and early detection of sepsis can lead to interventions that dramatically reduce those costs. However, advanced Predictive DSIs for the identification of sepsis are not widely used and instead older models, such as Sequential Organ Failure Assessment (SOFA), are dominant.[282]

Existing evidence indicates that more advanced predictive models can provide substantial performance improvements over simpler, widely used models.[283] The potential benefits of more advanced models are large. A prospectively evaluated sepsis Predictive DSI decreased in-hospital mortality related to sepsis by 39.5%, decreased length of stay by 32.3% and decreased readmission by 22.7% in one clinical trial.[284] However, there is also substantial uncertainty about whether models will offer that benefit when implemented on a broad scale. Performance of the same model evaluated in that clinical trial was substantially lower in a separate evaluation,[285] and that difference may be attributable to difference in performance in varied deployments and locations.

Transparency has the potential to shed light on the variation in performance across models and to drive uptake of higher performing models. A systematic review of predictive models designed to detect early onset of sepsis found that published evaluations demonstrated sensitivities ranging from 64% to 98%.[286] One sepsis model that was recently widely adopted was found in subsequent validation to have relatively poor performance with a sensitivity of 33%. This again highlights

[279] Ziad Obermeyer, et al., *Dissecting racial bias in an algorithm used to manage the health of populations,* 366 Science (2019).

Andrew Wong, et al., *External validation of a widely implemented proprietary sepsis prediction model in hospitalized patients,* 181 JAMA Internal Medicine (2021).

The Johns Hopkins ACG® System, available at *https://www.johnshopkinssolutions.com/wp-content/uploads/2016/08/ACG-System-Brochure.pdf.*

[280] *https://www.healthit.gov/buzz-blog/health-innovation/back-to-the-future-what-predictive-decision-support-can-learn-from-deloreans-and-the-big-short.*

[281] Epidemiology and Costs of Sepsis in the United States—An Analysis Based on Timing of Diagnosis and Severity Level*—PMC (*nih.gov*).

[282] J-L Vincent, et al., The SOFA (Sepsis-related Organ Failure Assessment) score to describe organ dysfunction/failure (Springer-Verlag 1996).

[283] As one example of a study demonstrating clear accuracy improvements over widely used, simpler models see Ryan J Delahanty, et al., *Development and evaluation of a machine learning model for the early identification of patients at risk for sepsis,* 73 Annals of Emergency Medicine (2019).

[284] Burdick, Hoyt, et al. ''Effect of a sepsis prediction algorithm on patient mortality, length of stay and readmission: a prospective multicentre clinical outcomes evaluation of real-world patient data from US hospitals.'' BMJ health & care informatics 27.1 (2020).

[285] Topiwala, Raj, et al. ''Retrospective observational study of the clinical performance characteristics of a machine learning approach to early sepsis identification.'' *Critical Care Explorations* 1.9 (2019).

[286] Hassan, Nehal, et al. ''Preventing sepsis; how can artificial intelligence inform the clinical decision-making process? A systematic review.'' *International Journal of Medical Informatics* 150 (2021): 104457.

Makam, Anil N., Oanh K. Nguyen, and Andrew D. Auerbach. ''Diagnostic accuracy and effectiveness of automated electronic sepsis alert systems: a systematic review.'' *Journal of hospital medicine* 10.6 (2015): 396–402.

the potential value of greater information to evaluate these models.[287]

Given the heterogeneity in the literature, it is challenging to estimate the extent to which the availability of information that will be facilitated by our policy will impact the average quality of predictive models used or how that average quality will evolve over time. Because models often perform less effectively in real-world implementation than in test environments, we believe the likely impact will be smaller than that implied by the literature but believe an impact on the average sensitivity of models used of 5 percentage points is reasonable. We note that in the cited systematic review, the median sensitivity of included models was 81% so that our assumption is that with the rule in place median sensitivity of available models will increase by 5 percentage points to 86%. Based on cost savings indicated in the available literature, we estimate that early detection of onset will result in cost savings of 50% for the incrementally more commonly detected patient event.

Beyond increases in the accuracy and effectiveness of models used, it is also challenging to estimate the extent to which the adopted certification criterion will result in increased use of more accurate decision support interventions. Findings on other transparency related public policies, such as nutrition labels, indicate that use of labels can have substantial impacts on consumers choices.[288] While these findings indicate a likely increase in use of interventions from transparency related policies, we believe it is difficult to transfer these findings to the specific case of Predictive DSIs. We are assuming that the policy will relate to application of improved models (with an average increased sensitivity of 5%) by 2% a year beginning in the year that requirements commenced.

Another example we wish to highlight along with sepsis is the use of models to identify patients at risk for ambulatory care sensitive conditions (ACSCs). Such conditions result in costs of $33.7 billion (bn) per year.[289] As in the sepsis example, there are several existing predictive models, and they exhibit a wide range accuracy.[290] We therefore believe it is reasonable to apply the estimates used in the prior example related to sepsis onset to estimate potential benefits related to ambulatory care-sensitive admissions. Given substantial differences in the sensitivity of models intended to identify patients at risk of ambulatory care-sensitive admissions, we believe this assumption is reasonable.[291]

We estimate all benefits on a 10-year time horizon. Because developers of certified health IT with Health IT Modules certified to the existing certification criterion in § 170.315(a)(9) are not required to certify to the adopted criterion in § 170.315(b)(11) until 2024, we note that benefits would not commence until the third year. We believe that period of time allows sufficient time for the full impact of the policy to take effect, including developer certification to the criterion, publication of risk management information, and hospital resorting to improved predictive models. We expect that the use of predictive models in healthcare will continue to evolve well beyond that time horizon; however, given the dynamic and uncertain nature of this area, we do not believe it would be appropriate to provide estimates beyond that period.

We examined the sensitivity of our estimated benefits based on uncertainty in the underlying rates. We varied two rates: the average increase in the sensitivity of models used and the increased rate at which more accurate models were used. Specifically, we recalculated benefits with an assumed sensitivity increase of 2.5%, 5% or 10% (with 5% representing our primary estimate) and an assumed increase in application of models of 1%, 2% and 3% (with 2% representing our primary estimate). In these analyses, we estimated that the 10-year undiscounted incremental impacts ranged from $259,650,000 to $3,115,800,000. We also estimated the annualized benefits of the incremental impacts using alternative modeling assumptions and present them in Table 19.

TABLE 18—SELECT BENEFITS TO PATIENTS AND PAYERS FROM UPDATED DECISION SUPPORT FUNCTIONALITY

Year impacts are incurred	Cost of sepsis admission (bn)	Proportion of admissions for which more sensitive model used	Increased sensitivity of models used	Assumed costs saved for impacted admissions	Incremental impacts (undiscounted) *	Incremental impacts (7% discount)	Incremental impacts (3% discount)	
1						$0.00	$0.00	
2						0.00	0.00	
3	$24	0.02	0.05	0.5	$12,000,000	9,795,575	10,981,670	
4	24	0.04	0.05	0.5	24,000,000	18,309,485	21,323,689	
5	24	0.06	0.05	0.5	36,000,000	25,667,502	31,053,916	
6	24	0.08	0.05	0.5	48,000,000	31,984,427	40,199,244	
7	24	0.1	0.05	0.5	60,000,000	37,364,985	48,785,491	
8	24	0.12	0.05	0.5	72,000,000	41,904,656	56,837,465	
9	24	0.14	0.05	0.5	84,000,000	45,690,434	64,379,006	
10	24	0.16	0.05	0.5	96,000,000	48,801,532	71,433,016	
Total					432,000,000.00	259,518,595	344,993,527	PV
						36,949,610	40,443,766	Ann

[287] Wong, Andrew, et al. ''External validation of a widely implemented proprietary sepsis prediction model in hospitalized patients.'' *JAMA Internal Medicine* 181.8 (2021): 1065–1070.

[288] For examples, see Joanne F Guthrie, et al., *Who uses nutrition labeling, and what effects does label use have on diet quality?* 27 Journal of Nutrition education (1995); Marian L Neuhouser, et al., *Use of food nutrition labels is associated with lower fat intake,* 99 Journal of the American dietetic Association (1999).

[289] *https://www.hcup-us.ahrq.gov/reports/statbriefs/sb259-Potentially-Preventable-Hospitalizations-2017.jsp.*

[290] Emma Wallace, et al., *Risk prediction models to predict emergency hospital admission in community-dwelling adults: a systematic review,* 52 Medical Care (2014).

Seung Eun Yi, et al., *Predicting hospitalisations related to ambulatory care sensitive conditions with machine learning for population health planning: derivation and validation cohort study,* 12 BMJ Open (2022).

[291] Garcia-Arce, Andres, Florentino Rico, and José L. Zayas-Castro. ''Comparison of machine learning algorithms for the prediction of preventable hospital readmissions.'' *The Journal for Healthcare Quality (JHQ)* 40.3 (2018): 129–138.

Year impacts are incurred	Cost of ambulatory sensitive admission (bn)	Proportion of admissions for which more sensitive model used	Increased sensitivity of models used	Assumed costs saved for impacted admissions	Incremental impacts (undiscounted) *	Incremental impacts (7% discount)	Incremental impacts (3% discount)	
1								
2								
3	$33.7	0.02	0.05	0.5	$16,850,000	$13,754,619	$15,420,136	
4	33.7	0.04	0.05	0.5	33,700,000	25,709,569	29,942,014	
5	33.7	0.06	0.05	0.5	50,550,000	36,041,451	43,604,874	
6	33.7	0.08	0.05	0.5	67,400,000	44,911,466	56,446,439	
7	33.7	0.1	0.05	0.5	84,250,000	52,466,666	68,502,960	
8	33.7	0.12	0.05	0.5	101,100,000	58,841,120	79,809,274	
9	33.7	0.14	0.05	0.5	117,950,000	64,156,985	90,398,854	
10	33.7	0.16	0.05	0.5	134,800,000	68,525,485	100,303,860	
Total					606,600,000	364,407,361	484,428,410	PV
						51,883,410	56,789,788	Ann

TABLE 19—SELECT BENEFITS FROM UPDATED DECISION SUPPORT FUNCTIONALITY UNDER ALTERNATIVE ASSUMPTIONS, $ MILLIONS, ANNUALIZED, 3% DISCOUNT RATE

Impact on annual model application (%)	Impact on model sensitivity		
	2.50%	5%	10%
1	$24.3	$48.6	$97.2
2	48.6	97.2	194.5
3	72.9	145.9	291.7

We have highlighted one condition and one event that will benefit from the more widespread use of more accurate predictive models under this final rule. There are numerous other conditions and events in which increased sensitivity could offer substantial cost savings. However, given uncertainty in the estimates around the included estimates, and important differences across various conditions and the extent to which Predictive DSIs might impact care, we are not confident that the assumptions generated here are transferable to other contexts.

In addition to benefits associated with more sensitive models, we believe that there are numerous other potential benefits related to the more widespread use of more accurate predictive decision support. However, many of the benefits associated with greater accuracy, specific models, such as reduced inappropriate treatment or reduced burdens on providers, are difficult to quantify and have to date been targeted by fewer predictive models. For salient examples, we note that false-positives for screening for with $4 billion per year and that more specific interventions could reduce the rates of false-positives.[292] We further note that provider burnout and fatigue are important and costly issues, we believe these benefits may be large.[293] However, since we are aware of fewer estimates around the potential impact of Predictive DSIs to address these issues, we have not attempted to quantify the potential benefits associated with their use.

Beyond the benefits associated with greater use of accurate models, we believe there will be several important benefits associated with the adopted transparency requirements. We believe that increased transparency into the intended use of models will increase the appropriate use of models. There is concern that models will be applied to populations, contexts, and decisions for which they are not well-suited to provide accurate information.[294] A transparent display of the intended use and what is out of scope could reduce the occurrence of treatment decisions resulting in harm. However, we are not aware of efforts to quantify harm from misapplied models today.

We believe increased transparency into models and practices will result in the selection and use of fairer models. Biased models, for instance, exhibit higher sensitivity or specificity for some groups than others and are likely to deprioritize treatment for certain groups. They are also likely to recommend inappropriate treatment for certain groups resulting in limited benefit and potential harm to those certain groups relative to those for whom models the perform well. Reliance on biased models, particularly those used in the context of preventive care or early identification of a disease, could result in greater costs for groups in which the model performs poorly compared to developing a fairer model or not using the model altogether. Greater transparency into the fairness of models will enable users to select fairer models and reward producers of fairer models. This will lead to the selection of models that further, opposed to hinder, the equitable delivery of healthcare to groups that have been marginalized. We requested comment on the feasibility of quantifying benefits associated with increased model fairness, which may be identifiable through the increased benefits to groups that have been marginalized.

We believe that increased transparency will lead to an effective market for predictive models that adequately incentivizes and rewards high-quality models. Currently, model developers have an information advantage relative to consumers, and consumers of models act under considerable uncertainty regarding the quality of the product they are acquiring. This market dynamic can lead to harmful choices by consumers and inadequate reward for high quality developers, potentially leading to a

[292] Ong, Mei-Sing, and Kenneth D. Mandl. ''National expenditure for false-positive mammograms and breast cancer overdiagnoses estimated at $4 billion a year.'' *Health affairs* 34.4 (2015): 576–583.

[293] Gregory, Megan E., Elise Russo, and Hardeep Singh. ''Electronic health record alert-related workload as a predictor of burnout in primary care providers.'' *Applied clinical informatics* 8.03 (2017): 686–697.

[294] Richard Ribón Fletcher, et al., *Addressing fairness, bias, and appropriate use of artificial intelligence and machine learning in global health,* 3 Frontiers in Artificial Intelligence (2021).

feedback loop through adverse selection that encourages market exit by high quality, high-cost model developers. However, adequately characterizing the benefits of a higher information market to the overall quality of models developed and sold is not feasible.

Comments. We received no comments on this analysis.

Response. The final impact analysis was updated to include the expected annual costs for applicable developers of certified health IT to meet annual documentation requirements. Cost estimates were also updated to reflect wages of software developers as of 2022.

Synchronized Clocks Standard

In section III.C.6 of this preamble, we discuss the proposed removal of the current named specification for clock synchronization, which is Network Time Protocol (NTP v4 of RFC 5905), in 45 CFR 170.210(g). However, we proposed to maintain an expectation that Health IT Modules certified to applicable certification criteria continue to utilize any network time protocol (NTP) standard that can ensure a system clock has been synchronized and meets the time accuracy requirements as defined in the applicable certification criteria in § 170.315(d)(2), (3), (10), and (e)(1).

Costs

This policy is not intended to place additional burden on health IT developers as it does not require new development or implementation. Rather, a health IT developer's costs will be *de minimis* because we are providing flexibility to allow health IT developers to use any NTP standard that exists. We welcomed comments on these expectations.

Benefits

We believe leveraging existing NTP standards and not requiring a specific standard allows for more flexibility. We have heard from health IT developers that the current required functionality is in place but not fully used. This policy allows for additional flexibility to meet the time accuracy requirements as defined in applicable certification criteria. For example, under this policy, Microsoft-based certified health IT using Operating System to synchronize network time, may use Microsoft's version of Network Time Protocol (MS NTP) as an alternative to Network Time Protocol Version 4 (NTP v4) of RFC 5905 as specified in § 170.210(g), and must meet the time accuracy requirement as defined in the certification criteria. We welcomed comments regarding potential approaches for quantifying these benefits.

Comments. We received no comments on this section of the analysis.

Response. We have finalized the impact analysis as proposed for this section.

Standardized API for Patient and Population Services

As discussed in section III.C.7 of this preamble, we have finalized as proposed, to update the certification criterion, ''standardized API for patient and population services,'' to align with updated standards and new requirements. We have finalized as proposed, to adopt the SMART App Launch Implementation Guide Release 2.0.0 in § 170.215(c)(2), which would replace SMART Application Launch Framework Implementation Guide Release 1.0.0 in § 170.215(a)(3) (finalized in this rule in § 170.215(c)(1)).

We also have finalized as proposed, to revise the requirement in § 170.315(g)(10)(vi) to specify that Health IT Modules presented for certification that allow short-lived access tokens to expire, in lieu of immediate access token revocation, must be able to revoke an authorized application's access at a patient's direction within one hour of the request.

Additionally, we have finalized to amend the API Condition and Maintenance of Certification requirements by adding the requirement that Certified API Developers with patient-facing APIs must publish their service base URLs for all customers, regardless of whether the certified Health IT Modules are centrally managed by the Certified API Developer or locally deployed by an API Information Source. We have finalized that these service base URLs must conform to a specific data format.

Finally, we have also adopted the FHIR US Core Implementation Guide STU version 6.1.0 in § 170.215(b)(1)(ii). Health IT systems that adopt this version of the US Core IG can provide the latest consensus-based capabilities for providing access to USCDI v3 data classes and elements using a FHIR API.

Costs

We have estimated the cost to health IT developers to make these updates. These estimates are detailed in Table 20 below and are based on the following assumptions:

1. Health IT developers will experience the assumed average costs of labor and data model use. Table 20 shows the estimated labor costs per product for a health IT developer to implement these updates to the criterion. We recognize that health IT developer costs will vary; however, our estimates in this section assume all health IT developers will on average, incur the costs noted in Table 20.

2.We estimate that 276 products certified by 228 developers will be affected by our policies. These estimates are a subset of the total estimated health IT developers and certified products we estimated above. We estimate that in total, 368 health IT developers will certify 502 health IT products impacted by this rulemaking. However, not all these developers and products will certify the *Standardized API* criterion and need to meet these adopted requirements. As of the end of 2021, 62% of developers and 55% of products certified the ''application access—data category request'' criterion. By December 31, 2022, all products that certify this criterion must certify the new standardized API criterion. We, therefore, use current certification of the data category request criterion as a proxy for the percent of developers and products certified to the standardized API criterion in the future. We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by these updates to the standardized API criterion.

3. Wages are determined using BLS estimates. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91. As noted previously, we have assumed that other indirect costs (including benefits) are equal to 100 percent of pre-tax wages, so the hourly wage including other indirect costs is $128.

TABLE 20—ESTIMATED LABOR HOURS TO UPDATE STANDARDIZED API FOR PATIENT AND POPULATION SERVICES

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: Implementation to the FHIR US Core IG 6.1.0 (per product).	Implement FHIR US Core IG v6.1.0 to update API to conform to US Core v6.1.0, which adopts the USCDIv3 data classes and elements.	500	1,000	(1) Lower bound assumes health IT product voluntarily updated to USCDIv3 through SVAP. (2) Upper bound assumes health IT product only supports USCDIv1 and needs to update API to support resources aligned with data elements in USCDIv3.
Task 2: Service-base URL Publication (per developer).	(1) Publish service-base URL in FHIR Endpoint resource format (2) Publish API Information Source organization information in Organization resource format (3) Make both available as FHIR bundle.	250	1,000	(1) Lower bound assumes API Technology Supplier met the ONC Cures Act Final Rule service-base URL maintenance of certification requirement and published endpoint and organization data in these standard formats. (2) Upper bound assumes API Technology Supplier met the Cures Final Rule service-base URL maintenance of certification requirement but did not publish in the standard format.
Task 3: Develop support of 60-minute access revocation (per product).	Develop support for patients to revoke access to authorized app and for revocation to be fulfilled by server within 60 minutes of request.	50	100	(1) Lower bound assumes developer needs to modify current revocation process and not rebuild is necessary. (2) Upper bound assumes revocation process exists, as required by ONC Cures Act Final Rule, but needs to be reprogrammed to accommodate new revocation step.
Task 4: Update security via SMART App Launch Framework to IG 2.0 (per product).	Update API from SMART App Launch Framework IG 1.0 to IG 2.0.	500	1,000	(1) Lower bound assumes update to SMART App Launch Framework IG 2.0 underway. (2) Upper bound assumes update to Framework IG 2.0 not underway.

TABLE 21—EXAMPLE CALCULATION FOR THE LOWER BOUND ESTIMATED COST TO PRODUCTS TO PERFORM TASK 1 IN TABLE 20 TO UPDATE API

[2022 Dollars]

Activity	Estimated labor hours	Developer salary (per hour)	Projected products
	Lower bound		
Task 1 ..... Example calculation: 500 * $128 * 276 products = $17,664,000.	500	$128	276

TABLE 22—TOTAL COST TO UPDATE STANDARDIZED API FOR PATIENT AND POPULATION SERVICES

[2022 Dollars]

Activity	Estimated cost	
	Lower bound	Upper bound
Task 1 (276 products)	$17,664,000	$35,328,000
Task 2 (228 developers)	7,296,000	29,184,000
Task 3 (276 products)	1,766,400	3,532,800
Task 4 (276 products)	17,664,000	35,328,000
Total (276 products and 228 developers)	44,390,400	103,372,800

The cost to a health IT developer to update the standardized API criterion for their certified Health IT Modules will range from $166,000 to $397,000 per product, on average. Therefore, assuming 276 products overall and a labor rate of $128 per hour, we estimate that the total cost to all health IT developers will on average, range from $44 million to $103 million. This will be a one-time cost to developers per product that is certified to the specified certification criterion and will not be perpetual.

Benefits

We believe these policies will benefit health care providers, patients, and the industry. The adoption of the FHIR US Core IG v6.1.0 will, with the additional data elements in USCDI v3, expand the baseline set of data available and

provide more comprehensive health data for both providers and patients. Updates to the SMART App Launch Framework IG 2.0 will align the certified API functionality with current adopted standards-based methods to connect patients' health information to the app of their choice. Furthermore, updated requirements to the service-base URL publication API maintenance of certification requirement will provide a standard format for all published FHIR endpoints to be securely discovered and consumed by authorized applications. The standard publication format will reduce the burden on patients, app developers, and other third parties to find and connect to the appropriate FHIR endpoint to initiate data access. This will directly benefit the speed and efficiency of making these connections and reduce the level of effort on third parties to access and use these standards-based APIs.

We expect the resulting improvements to interoperable exchange of health information to significantly benefit providers and patients and improve the quality of healthcare provided. In the ONC Cures Act Final Rule (85 FR 25925), we estimated the total annual benefit of APIs on average, to range from $0.34 billion to $1.43 billion. These updates to the criterion ensure the benefits of APIs are maintained and the annual benefit due to improved health outcomes and patients having access to their online medical record is realized.

As described previously, there are additional potential future benefits to the expanded availability of an interoperable API for patient and population services that are not quantifiable at this time. For some use cases, there is a clear indication of future technical direction, but currently there is insufficient implementation to clearly quantify the scope. For example, CMS has identified an intent to leverage APIs for population services in order to modernize quality measurement and quality reporting under value-based payment programs.[295] In 2016, a report found that quality measurement reporting bears an estimate $15.4 billion cost on clinicians for chart abstraction, data validation, and measure reporting.[296] The potential future use of FHIR-based APIs for quality measurement could provide greater ability to implement real time data for quality purposes and drastically reduce the costs of manual quality reporting workflows. We sought comment on potential means to estimate these benefits and future cost savings.

Comments. We received no comments related to this impact analysis of updates to the standardized API criterion.

Response. The final impact analysis is consistent with the proposed rulemaking. Cost estimates were updated to reflect wages of software developers as of 2022.

Patient Demographics and Observations Certification Criterion

As discussed in section III.C.8 of this preamble, we have finalized as proposed to rename the ''demographics'' certification criterion (§ 170.315(a)(5)) to ''*patient demographics and observations.*'' We have finalized as proposed to add the data elements ''Sex Parameter for Clinical Use'' in § 170.315(a)(5)(i)(F), ''Name to Use'' in § 170.315(a)(5)(i)(G), and ''Pronouns'' in § 170.315(a)(5)(i)(H) to the ''Patient demographics and observations'' certification criterion (§ 170.315(a)(5)). Additionally, we have finalized as proposed to replace the terminology standards specified for ''Sex'' in § 170.315(a)(5)(i)(C), ''Sexual Orientation'' in § 170.315(a)(5)(i)(D), and ''Gender Identity'' in § 170.315(a)(5)(i)(E). As such, ONC has finalized as proposed to remove the fixed list of terms for ''Sex'' in § 170.315(a)(5)(i)(C), ''Sexual Orientation'' in § 170.315(a)(5)(i)(D), and ''Gender Identity'' in § 170.315(a)(5)(i)(E) which are represented by SNOMED CT and HL7® Value Sets for AdministrativeGender and NullFlavor in § 170.207(o)(1) and (2)), and replace it with the SNOMED CT code sets specified in § 170.207(n)(2) and (o)(3).

The proposed modifications to the ''patient demographics and observations'' criterion will provide greater clarity and standardization to how a patient's sexual orientation and gender identity are recorded electronically in the electronic health record. The USCDI v3 standard includes new data elements for Sexual Orientation and Gender Identity. These data elements are required to be included as part of a patient's electronic health information and included in any record shared with the patient, the patient's caregiver, or health care provider.

Costs

The adopted modifications to the ''patient demographics and observations'' criterion include 6 tasks: (1) Modify Sex, (2) Modify Sexual Orientation, (3) Modify Gender Identity, (4) Add Sex Parameter for Clinical Use, (5) Add Pronouns, and (6) Add Name to Use. These tasks have their own level of effort, and these estimates are detailed in Table 23 below and are based on the following assumptions:

1. Health IT developers will use the same labor costs and data models. Table 23 shows the estimated labor costs per product to modify the ''patient demographics and observations'' criterion. We recognize that health IT developer costs will vary; however, our estimates in this section assume all health IT developers will incur the costs noted in Table 23.

2. We estimate that 321 products certified by 261 developers will be affected by our policy. These estimates are a subset of the total estimated health IT developers and certified products we estimated above.

The estimate of 321 products certified by 261 developers is derived as follows. We estimate that, in total, 368 health IT developers would certify 502 health IT products impacted by this rulemaking. However, not all these developers and products certify the ''patient demographics and observations'' criterion and need to meet the adopted requirements. As of the end of 2021, 71% of developers and 64% of products certified to the criterion. We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by the modifications to the criterion.

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91. As noted previously, we have assumed that other indirect costs (including benefits) are equal to 100 percent of pre-tax wages, so the hourly wage including other indirect costs is $128.

[295] CMS Digital Quality Roadmap, March 2022: *https://ecqi.healthit.gov/sites/default/files/CMSdQMStrategicRoadmap_032822.pdf.*

[296] Health Aff (Millwood), March 2016. *US Physician Practices Spend More Than $15.4 Billion Annually To Report Quality Measures. https://pubmed.ncbi.nlm.nih.gov/26953292/.*

TABLE 23—ESTIMATED LABOR HOURS TO MODIFY § 170.315(a)(5) DEMOGRAPHICS CRITERION

Task	Details	Lower bound hours	Upper bound hours
Task 1: Modify Sex [§ 170.315(a)(5)(i)(C)]	Value set for Sex removed and now references SNOMED CT.	0	40
Task 2: Modify Sexual Orientation [§ 170.315(a)(5)(i)(D)].	Value set for Sexual Orientation removed and now references SNOMED CT.	0	40
Task 3: Modify Gender Identity [§ 170.315(a)(5)(i)(E)]	Value set for Gender Identity removed and now references SNOMED CT.	0	40
Task 4: Add Sex Parameter for Clinical Use [§ 170.315(a)(5)(i)(F)].	Add ''Sex Parameter for Clinical Use'' using LOINC	240	580
Task 5: Add Pronouns [§ 170.315(a)(5)(i)(H)]	Add ''Pronouns'' using LOINC	240	580
Task 6: Add Name to Use [§ 170.315(a)(5)(i)(G)]	Add ''Name to Use'' as a kind of name field	240	580

TABLE 24—EXAMPLE CALCULATION FOR THE LOWER BOUND ESTIMATED COST TO PRODUCTS TO PERFORM TASK 1 IN TABLE 23 TO MODIFY DEMOGRAPHICS

[2022 dollars]

Activity	Estimated labor hours	Developer salary (per hour)	Projected products
	Lower bound		
Task 1 Example calculation: 200 * $116 * 321 products = $7,447,200.	200	$128	321

TABLE 25—TOTAL COST TO MODIFY DEMOGRAPHICS

[2022 dollars]

Activity	Estimated cost	
	Lower bound	Upper bound
Task 1 (321 products)	$0	$1,643,520
Task 2 (321 products)	0	1,643,520
Task 3 (321 products)	0	1,643,520
Task 4 (321 products)	9,861,120	23,831,040
Task 5 (321 products)	9,861,120	23,831,040
Task 6 (321 products)	9,861,120	23,831,040
Total (321 products and 261 developers)	29,583,360	76,423,680

The cost to a health IT developer to make the modifications to the ''patient demographics and observations'' criterion for their certified Health IT Modules will range from $92,160 to $238,080 per product, on average. Therefore, assuming 321 products overall and a labor rate of $128 per hour, we estimate that the total cost to all health IT developers will, on average, range from $30 million to $76 million. This will be a one-time cost to developers per product that is certified to the specified certification criterion.

Benefits

Improved recording of sexual orientation and gender identity in the medical record has multiple benefits. This has clinical benefits for patients in the immediate term as information related to gender identity and sexual orientation is critical for informing treatment. Additionally, advances in treatment may result from researchers having more reliable and accurate sexual orientation and gender identity data available. Not only will this benefit clinical care teams who are treating patients within a particular clinical setting, this will improve the interoperability of this data when shared electronically with the patient or the patient's authorized representative through the technology of their choosing or when shared electronically with a third party elected by the patient, such as an application developer, health care provider, or other entity.

The benefits of these modifications are not quantifiable at this time, but we expect the resulting improvements to interoperable exchange of health information to significantly benefit providers and patients and improve the quality of healthcare provided. Furthermore, having a patient's information recorded uniformly and available across their medical records would improve the patient's access to their information and ensure the information is available uniformly across technologies.

Comments. We received no comments specific to this update to the ''demographics'' criterion.

Response. The final impact analysis is consistent with the proposed rulemaking. Cost estimates were updated to reflect wages of software developers as of 2022.

Updates to Transitions of Care Certification Criterion in § 170.315(b)(1)

As discussed in section III.C.9 of this preamble, we proposed to modify the ''transitions of care'' certification criterion in § 170.315(b)(1). We proposed to replace the fixed value set for the USCDI data element Sex and instead enable health IT developers to represent sex with the standard adopted in § 170.207(n)(1) for the time-period up to and including December 31, 2025; or § 170.207(n)(2).

Costs

1. Health IT developers will use the same labor costs and data models. Table 26 shows the estimated labor costs per product to modify the transitions of care criterion. We recognize that health IT developer costs will vary; however, our estimates in this section assume all health IT developers will incur the costs noted in Table 26.

2. We estimate that 281 products certified by 236 developers will be affected by our policy. These estimates are a subset of the total estimated health IT developers and certified products we estimated above.

The estimate of 281 products certified by 236 developers is derived as follows. We estimate that, in total, 368 health IT developers will certify 502 health IT products impacted by this rulemaking. However, not all these developers and products certify the transitions of care criterion and need to meet the adopted requirements. As of the end of 2021, 64% of developers and 56% of products certified to the transitions of care criterion. We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by the modifications to the criterion.

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91. As noted previously, we have assumed that overhead costs (including benefits) are equal to 100 percent of pre-tax wages, so the hourly wage including overhead costs is $128.

TABLE 26—ESTIMATED LABOR HOURS TO MODIFY § 170.315(b)(1) TRANSITIONS OF CARE CRITERION

Task	Details	Lower bound hours	Upper bound hours
Task 1: Modify Sex [§ 170.315(a)(5)(i)(C)]	Value set for Sex removed and now references SNOMED CT	0	40

TABLE 27—TOTAL COST TO MODIFY TRANSITIONS OF CARE

[2022 dollars]

Activity	Estimated cost	
	Lower bound	Upper bound
Modify Sex (281 products)	$0	$1,438,720

The cost to a health IT developer to make the modifications to the transitions of care criterion for their certified Health IT Modules will range from $0 to $5,120 per product, on average. Therefore, assuming 281 products overall and a labor rate of $128 per hour, we estimate that the total cost to all health IT developers will, on average, range from $0 to $1.5 million. This will be a one-time cost to developers per product that is certified to the specified certification criterion.

Benefits

There are multiple benefits associated with having more granular information available related to improved recording of sexual orientation and gender identity. This has clinical benefits for patients in the immediate term as information related to gender identity and sexual orientation is critical for informing treatment. Additionally, advances in treatment may result from researchers having more reliable and accurate sexual orientation and gender identity data available. Not only will this benefit clinical care teams who are treating patients within a particular clinical setting, this will improve the interoperability of this data when shared electronically with the patient or the patient's caregiver through the technology of their choosing or when shared electronically with a third party elected by the patient, such as an application developer, health care provider, or other entity.

The benefits of these modifications are not quantifiable at this time, but we expect the resulting improvements to interoperable exchange of health information to significantly benefit providers and patients and improve the quality of healthcare provided. Furthermore, having a patient's information recorded uniformly and available across their medical records will improve the patient's access to their information and ensure the information is available uniformly across technologies.

Comments. We received no comments related to the impact analysis of updates to the Transitions of care criterion.

Response. The final impact analysis is consistent with the proposed rulemaking. Cost estimates were updated to reflect wages of software developers as of 2022.

Patient Right To Request a Restriction on Use or Disclosure

As discussed in section III.C.10 of this preamble, we have finalized as proposed to modify the existing criterion in § 170.315(e)(1) to add a paragraph (iii) stating patients (and their authorized representatives) must be able to use an internet-based method to request a restriction to be applied for any data expressed in the standards in § 170.213. This policy is standards agnostic for the implementation of functional requirements supporting workflows for a patient to exercise their right to request restrictions on certain uses and disclosures of their EHI and for a HIPAA covered entity, such as a clinician that transmits any health information in electronic form in connection with a HHS adopted standard transactions, to honor such request.

Costs

The update to § 170.315(e)(1) includes a new technical functionality that provides patients (and their authorized representatives) the ability to use an internet-based method to request a restriction to be applied for any data expressed in the standards in § 170.213. This task has its own level of effort, and this estimate is detailed in Table 28 below and is based on the following assumptions:

1. Health IT developers will use the same labor costs and data models. Table 29 shows the estimated labor costs per product to modify § 170.315(e)(1). We recognize that health IT developer costs will vary; however, our estimates in this section assume all health IT developers will incur the costs noted in Table 29.

2. We estimate that 246 products certified by 210 developers will be affected by our proposal. These estimates are a subset of the total

estimated health IT developers and certified products we estimated above.

The estimate of 246 products certified by 210 developers is derived as follows. We estimate that, in total, 368 health IT developers will certify 502 health IT products impacted by this rulemaking. However, not all these developers and products certify § 170.315(e)(1) and need to meet the proposed requirements. As of the end of 2021, 57% of developers and 49% of products certified § 170.315(e)(1). We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by the proposed modifications to the criterion.

3. According to the Month 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91. As noted previously, we have assumed that overhead costs (including benefits) are equal to 100 percent of pre-tax wages, so the hourly wage including overhead costs is $128.

TABLE 28—ESTIMATED LABOR HOURS TO MODIFY 170.315(e)(1)

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: Add internet-based method for patients (and their authorized representatives) to request a restriction.	New technical functionality to be added to criterion § 170.315(e)(1). This is a standards agnostic method. Developer may choose internet-based method of choice (e.g., free-text box, check boxes for applicable data classes, etc.).	240	580	

TABLE 29—TOTAL COST TO MODIFY 170.315(e)(1)

[2022 dollars]

Activity	Estimated cost	
	Lower bound	Upper bound
Task 1 (246 products)	$7,557,120	$18,263,040

The cost to a health IT developer to modify § 170.315(e)(1) for their Health IT Modules would range from $30,720 to $74,240 per product, on average. Therefore, assuming 246 products overall and a labor rate of $128 per hour, we estimate that the total cost to all health IT developers would, on average, range from $7.5 million to $18 million. This would be a one-time cost to developers per product that is certified to the specified certification criterion and would not be perpetual.

Benefits

In the ONC Cures Act Final Rule, we noted that the updated criteria in § 170.315(b)(7) and (b)(8) (''security tags—summary of care—send'' and ''security tags—summary of care—receive'') would benefit providers, patients, and ONC because it would support more complete records, contribute to patient safety, and enhance care coordination. We stated that implementing security tags enables providers to share patient records more effectively with sensitive information, thereby protecting patient privacy while still delivering actionable clinical content. We emphasized that health care providers already have processes and workflows to address their existing compliance obligations, which could be made more efficient and cost effective using health IT. We were, however, unable to quantify these benefits at the time because we did not have adequate information to support quantitative estimates (85 FR 25927).

Since we issued the ONC Cures Act Final Rule, the number of developers certified to the voluntary criteria in § 170.315(b)(7) and (b)(8) has increased, but it remains a small percentage of the total products certified. While we believe there will be similar benefits to patients and other covered entities from our policies in this rule to support privacy workflows, we similarly are limited in our ability to estimate such impact at this time.

Comments. We received no comments specific to this impact analysis of patient requested restrictions.

Response. The final impact analysis was updated to reflect the final policy to include the ability for patients to request restrictions for their information in the ''view, download, and transmit'' criterion.

Insights Condition and Maintenance of Certification Requirements

The ''Insights Condition'' calls for developers of certified health IT to report for each applicable product on measures which focus on interoperability. For the initial requirements of the Insights Condition, ONC proposed nine measures that relate to individual access to electronic health information, clinical care information exchange, public health information exchange, and standards adoption and conformance.

Alternatives

Section 4002(c) of the Cures Act requires the creation of an Electronic Health Record (EHR) Reporting Program. We have chosen to implement the developer reporting through ONC's Health IT Certification Program to integrate this legislative mandate with other reporting requirements for developers of certified health IT as a Condition and Maintenance of Certification requirement. This approach is aligned with how we have interpreted other similar provisions of the Cures Act, and it is intended to maximize participation among developers of certified health IT while aligning participation with other requirements of the Program. Other alternatives to implementing this provision of the Cures Act could be to conduct a survey of developers of certified health IT to report on measures; however, such an effort would reflect only those developers who participated in the survey, thus limiting the generalizability of the results. A survey approach would also complicate ONC's ability to standardize developer results reporting and thus the quality and the rigor of the data would be affected. Thus, in order to be consistent with ONC's implementation of other Cures Act Condition and Maintenance of Certification requirements, to maximize the generalizability and accuracy of the data gathered through this effort, and to align it with other activities, we have chosen

to implement the Condition and Maintenance of Certification through ONC's Health IT Certification Program.

Costs

In calculating the cost of reporting each measure *m* we applied the following expression:

Cm = #Hours × Wage × # of Developers

The data for each of the elements (*e.g.,* #hours, wages, #developers) were extracted from various sources and there are assumptions associated with each element, which are described in this section.

The *#Hours* represents the labor hours it takes to produce measure *m.* The developers of certified health IT were asked the average number of hours they would need to develop and report a measure. Based on their reporting, we created a lower bound that represents 25% less than the reported number and an upper bound that represents 35% more than the reported number. We adjusted the number of hours required for developing each measure according to the difficulty level as ranked by developers of certified health IT.[297] We attributed more hours to skillful labor categories (from administrators to programmers and managers) than what was provided by developers as we believe these will be more accurate estimates.

The *Wage* represents hourly wage of a particular occupation needed to produce a measure. The wage estimates were extracted from the 2022 Bureau of Labor Statistics data and multiplied by two to account for administrative and other indirect costs, representing the median hourly wage of a software developer ($128) and a management analyst ($101) (the numbers incorporate other indirect costs of labor).[298] We assumed that the time used only by these occupations was sufficient for completing the task. The number of health IT developers is a function of the finalized small developer threshold and certified criteria requirements, which are described in more detail in section III.F.3 of this preamble under *Associated Thresholds for Health IT Developers.* We used data from the 2019 CMS Promoting Interoperability (PI) program and the Certified Health IT Product List to estimate the number of developers that would be reporting measures to the program. Per the finalized small developer threshold, developers whose certified health IT products were used by at least 50 hospitals, or 500 clinicians would have to report measures to the Program. In addition to having these minimum number of users across their certified health IT products, per the policy, we limited developers to those with products that certify to at least one of the following criteria associated with the adopted measures (see Table 30):

- Transitions of care § 170.315(b)(1)
- Clinical information reconciliation and incorporation § 170.315(b)(2)
- Transmission to immunization registry § 170.315(f)(1)
- View, download, and transmit to 3rd party § 170.315(e)(1)
- Standardized API for patient and population services § 170.315(g)(10)

For each measure, the estimated the number of developers of certified health IT depended on whether developers' products certified to criteria associated with a particular measure (as shown in Table 31) and whether they meet the threshold requirement for a small developer.

TABLE 30—ESTIMATED NUMBER OF HOURS AND DEVELOPERS ASSOCIATED FOR EACH MEASURE

[per developer]

Measure	Related criterion	Estimated number of applicable developers of certified health IT (no threshold)	Estimated number of applicable developers of certified health IT (threshold applied)	Management analyst estimated hours (per developer)		Software developer estimated hours (per developer)	
				Lower bound	Upper bound	Lower bound	Upper bound
Individuals' Access to EHI	§ 170.315(e)(1); § 170.315(g)(10)	157	53	320	800	1,100	2,220
Immunization Submission to IIS	§ 170.315(f)(1)	115	37	480	1,200	2,800	5,600
Immunization History and Forecasts	§ 170.315(f)(1)	115	37	470	1,200	1,380	2,760
C–CDAs Reconciliation and Incorporation.	§ 170.315(b)(1); § 170.315(b)(2)	171	56	400	1,400	3,200	8,700
Apps Supported	§ 170.315(g)(10)	176	59	320	800	1,850	3,700
Use of FHIR in in Apps	§ 170.315(g)(10)	176	59	400	1,000	2,300	4,600
Use of FHIR Bulk Data Access	§ 170.315(g)(10)	176	59	400	1,000	2,300	4,600

Data Source: ONC analysis of 2019 CMS Promoting Interoperability Program Data & CHPL.

We decided the small developer thresholds based upon analyses we conducted of the 2019 CMS PI Program and Certified Health IT Product List. We examined the various alternatives for setting user thresholds based on the percentage of users and developers that would be represented and reporting measures, respectively in the Program (*see* Table 31 below). The thresholds we decided upon maximize coverage and while not unduly disadvantaging smaller developers. The thresholds were determined based upon analysis of 2019 CMS PI program data and the CHPL data. The data from the CMS PI program included 4,209 non-federal acute hospitals and 691,381 clinicians who attested to the program. After limiting hospitals and clinicians to those using existing 2015 Edition certification criteria, the 2015 Edition Cures Update criteria, or a combination of the two; and to those products of developers who had certified to at least one of the criteria associated with the measures adopted in the Program (see Table 30), we ended up with 3,863 hospitals and 689,801 clinicians. For example, based upon a threshold of 50 hospitals, we would be able to include approximately 99% of all hospital users and the top 18 developers (based upon market share) while excluding the bottom 33 developers (based upon market share). This 99% value is based upon the percentage of users who are not exclusively using products from developers who meet the small developer threshold. Thus, in the case of a 50-hospital threshold, only 1.4% of hospital users are exclusively using

[297] Blavin F., et al. 2020. Urban Institute. Electronic Health Record (EHR) Reporting Program: Developer-Reported Measures. Available at *https://www.urban.org/sites/default/files/publication/105427/electronic-health-record-ehr-reporting-program-developer-reported-measures.pdf.* Accessed March 16, 2023.

[298] See BLS at *https://www.bls.gov/oes/current/oes_nat.htm.* Accessed September 15, 2023.

products from small developers, and thus about 99% of the inpatient market is covered.

TABLE 31—THRESHOLDS OPTIONS AT THE DEVELOPER LEVEL

	Estimated number of users *only* using small developers	Estimated % of users *only* using small developers	Estimated number of small developers	Estimated number of remaining developers
Hospitals:				
Option (a) 100 Threshold	142	3.7	39	12
Option (b) 50 Threshold	56	1.4	33	18
Clinicians:				
Option (a) 2,000 Threshold	21,075	3.1	176	31
Option (b) 1,000 Threshold	11,251	1.6	160	47
Option (b) 500 Threshold	7,828	1.1	146	61

In calculating the aggregate cost of developing all measures, we applied the concept of economies of scope, where the total cost of production is not incrementally increasing in the number of measures, but it is rather attenuating. Specifically, the aggregate cost in this application is governed by the following expression: The total cost (TC) of producing measures 1 and 2 is the sum of producing the two measures separately minus the cost of producing them together.

To calculate the cost of producing measures together, developers of certified health IT were asked during discussions to provide an estimate on the extent to which there would be an overlap in developing infrastructure between the measures published by the Urban Institute and level of difficulty by measure.[299] While some measures we have finalized differ from those the Urban Institute published, there is significant overlap across many of the measures, which would retain the validity of these estimates. The weighted average for selected measures suggested that there would be considerable overlap on the immunization measures (see Table 32). We note that for the incorporation measure, there is overlap between the proposed measure and the CMS PI Program Measure. We welcomed comments that provide us information on the level of perceived overlap so that we can adjust the estimates accordingly for the costs associated with that measure.

TABLE 32—PERCENT OVERLAP IN DEVELOPING THE FOLLOWING COMBINATION OF MEASURES

	Percent
Immunization Submission to IIS and Immunization History and Forecasts	50

Additionally, we assessed that there will be a 10% overlap of developing infrastructure across all measures. We applied these rates accordingly when calculating the total cost of developing measures for the Insights Condition.

Following this approach, the aggregate cost estimates over a 10-year period to develop and report on these measures are presented by different alternatives associated with thresholds in Table 33. The first row shows the total cost assuming developers have at least 50 hospital or 500 clinician users, which generates the cost between $98 and $218 million. In addition to estimating the costs associated with the 50 hospitals or 500 clinician user thresholds, we also present the cost for two alternatives where the number of users for hospitals is 100 and for clinician ranges from 1000 to 2000. The total cost would be reduced by about a half compared to the previous specification because smaller number of developers would qualify for the Insights Condition.

TABLE 33—AGGREGATE COST ESTIMATES FOR THE INSIGHTS CONDITION BY THRESHOLD ALTERNATIVES

Options	Lower bound	Upper bound
50 Hospitals and 500 Clinicians Threshold (Proposed Approach)	$98,373,673	$218,671,106
100 Hospitals and 1000 Clinicians Threshold (Alternative 1)	69,268,381	153,852,086
100 Hospitals and 2000 Clinicians Threshold (Alternative 2)	47,638,637	105,007,568
No Threshold Applied	297,027,045	660,807,830

In Table 30, we present the estimated number of labor hours to develop and report by measure for each individual developer. This table served as the basis for the cost estimates, prior to adjusting as described above.

In Table 34, we present cost estimates for each individual measure by developer and across all developers. The measures vary in cost because we made adjustments based on synergies discussed above (*e.g.,* similar measures, common infrastructure) and the level of

[299] Blavin F., et al. 2020. Urban Institute. Electronic Health Record (EHR) Reporting Program: Developer-Reported Measures. Available at *https://www.urban.org/sites/default/files/publication/105427/electronic-health-record-ehr-reporting-program-developer-reported-measures.pdf.* Accessed March 16, 2023.

expected burden to develop each measure.

TABLE 34—ESTIMATED COSTS BY MEASURE PER DEVELOPER OF CERTIFIED HEALTH IT AND ACROSS ALL ELIGIBLE DEVELOPERS OF CERTIFIED HEALTH IT

[No threshold]

Measure	Number eligible developers	Estimated costs (per developer)		Total estimated costs (all eligible developers)	
		Lower bound	Upper bound	Lower bound	Upper bound
Individuals' Access to EHI	157	$169,924	$353,846	$26,678,005	$55,553,791
Immunization Submission to IIS	115	360,023	739,508	41,425,606	85,043,311
Immunization History and Forecasts	115	109,227	228,908	12,561,105	26,324,363
C–CDAs Reconciliation and Incorporation	171	402,305	1,116,610	68,794,070	190,940,267
Applications Supported	176	238,088	488,773	41,903,326	86,024,030
Use of FHIR in Apps	176	300,186	616,256	52,832,657	108,461,034
Use of FHIR Bulk Data Access	176	300,186	616,256	52,832,567	108,461,034
All Measures: Total Cost		1,880,136	4,160,155	297,027,425	660,807,830

TABLE 35—ESTIMATED COSTS BY MEASURE PER DEVELOPER OF CERTIFIED HEALTH IT AND ACROSS ALL ELIGIBLE DEVELOPERS OF CERTIFIED HEALTH IT

[Threshold applied]

Measure	Number eligible developers	Estimated costs (per developer)		Total estimated costs (all eligible developers)	
		Lower bound	Upper bound	Lower bound	Upper bound
Individuals' Access to EHI	53	$169,924	$353,846	$9,005,951	$18,753,827
Immunization Submission to IIS	37	260,223	739,508	13,328,238	27,361,761
Immunization History and Forecasts	37	109,227	228,908	4,041,399	8,469,578
C–CDAs Reconciliation and Incorporation	56	402,305	1,116,610	22,529,052	62,530,146
Apps Supported	59	238,088	488,773	14,047,138	28,837,601
Use of FHIR in Apps	59	300,186	616,256	17,710,948	36,359,097
Use of FHIR Bulk Data Access	59	300,186	616,256	17,710,948	36,359,097
All Measures: Total Cost		1,880,136	4,160,1550	98,373,673	218,671,106

For the Insights Condition of Certification, we have indicated that developers of certified health IT who were required to report for Insights could leverage relevant Insights measures for real world testing annual reporting. We recognize some overlap in the two Conditions of Certification and that Insights measures would be appropriate to meet real world testing requirements for applicable certification criteria. An analysis of the CHPL shows that among developers required to report for Insights, 25% to 50% of their real world testing reporting requirements could be satisfied leveraging Insights metrics. Considering this we estimate that 25% to 50% of an average developer's annual real world testing costs could be saved by using Insights reporting as part of their real world testing plans.

We estimated cost savings for developers required to report for Insights. Cost savings were modeled using the real world testing cost estimates we have finalized in the ONC Cures Final Rule. We estimated in that final rule that a developer, on average, would face annual costs of $109,557 (2017 dollars) to meet real world testing reporting requirements. In 2022 dollars, we estimate this is $130,811 in annual costs. In Table 36 we show the impact of these cost savings on the total 10-year cost of developers to meet Insights requirements. We estimate this flexibility in meeting both Insights and real world testing reporting requirements will yield $13.6 million to $27.4 million in cost savings in total. We estimate these costs savings will reduce the overall total cost of developers reporting for Insights. The total cost of Insights is estimated to be $84.7 million to $191.2 million.

TABLE 36—ESTIMATED COST SAVINGS FROM REPORTING FOR BOTH REAL WORLD TESTING AND INSIGHTS

Options	Lower bound	Upper bound
50 Hospitals and 500 Clinicians Threshold (No Cost Savings applied)	$98,373,673	$218,671,106
50 Hospitals and 500 Clinicians Threshold (Cost Savings applied)	84,735,783	191,233,443

Benefits

The ONC Cures Act Final Rule seeks to advance interoperability and support the access, exchange, and use of electronic health information. There is currently limited transparency and information regarding interoperability; this not only stymies informed decision-making by ONC but also others in the industry, including health care providers, and entities that enable

exchange, including various types of health information networks and health app developers. ONC's measurement of interoperability is currently reliant primarily on self-reported survey data from end users of health information technology. While this information does provide some insights on interoperability from end-user perspectives, the insights derived are limited. The adopted measures will provide system-generated metrics on interoperability that will complement self-reported, user perspective data sources, such as surveys. Through the Insights Condition section of this final rule, we have identified where surveys have been limited in providing a clear picture of certain aspects of interoperability that these measures will elucidate. In addition, they will reach a greater number of health care providers than surveys, giving a more complete and representative national perspective. Greater transparency and information on interoperability of health IT products has the potential to benefit several interested parties, including ONC and other entities that enable exchange, including health app developers and health information networks. The adopted measures are also designed to identify areas that are working well and problems that we can monitor over time. This will help identify the need for technical and policy solutions as well as spur innovation that builds on successes and addresses gaps. While we currently do not have a means to quantify these benefits, we welcomed any feedback on methods to better quantify the impact these measures can have for healthcare and health IT.

The measures in this final rule for the Insights Condition will help improve and inform ONC programmatic and regulatory decision-making. ONC's programs and policies are designed to make direct and positive impacts on health IT use, care delivery, and patient health. ONC does this primarily through supporting standards development and the Program. The adopted measures will help ONC and others better understand the use, progress, and value of health IT standards. This has practical implications for improving the work ONC leads that increases the use of standards. For example, ONC has limited empirical information to provide guidance on the usage of standards associated with the Interoperability Standards Advisory. With the addition of the adopted measures, ONC can provide guidance to industry that is grounded in data from health IT developers rather than anecdotes. This has the potential to move industry to adopt standards more quickly, which has downstream impacts on improved interoperability. In addition, the adopted measures will increase transparency regarding the capability and usage of certified products. Through these measures, ONC and other interested parties will be able to identify areas that are problematic and in need of further investigation, such as cross-cutting policy and technical issues. They will also provide needed data to develop solutions to these complex problems.

The adopted measures from the Insights Condition will focus on four key priority areas: individual access to electronic health information, clinical care information exchange, standards adoption and conformance, and public health information exchange. Under the individuals' access to electronic health information measurement area, the measure will inform on the ONC Cures Act Final Rule goal of increasing access of electronic health information to individuals, particularly through the use of third-party apps. Increased patient engagement has been associated with improved health outcomes, and improved ease of access to their own medical records can improve patient engagement.[300] Thus, a better understanding of how patients are using apps through certified health IT will help inform ONC and other interested parties on the progress to reaching this goal. In addition, this measure will help inform app developers and developers of certified health IT, who are supporting apps on what individual's needs are to access their EHI. It will also inform health care provider organizations regarding action they may need to consider in supporting EHI and the need for outreach to patients and caregivers.

The clinical care information exchange measure will help ONC and other interested parties better understand the volume of information exchanged using C–CDA documents and how the information exchange is subsequently used via incorporation and reconciliation. Understanding the rates of C–CDA document incorporation is valuable for interested parties supporting C–CDA document exchange (*e.g.,* is it incorporated and used). This measure can also support further development in the incorporation of C–CDA documents.

Currently, ONC has limited data on the use of certified API technology in the app market. The ONC Cures Act Final Rule established the rules for the use of certified API technology in such a way to increase access to health information for both patients and health care providers. By understanding which apps are using FHIR-based APIs and the volume of transfer of FHIR resources, ONC and standards development organizations (SDOs) will be able to prioritize their work toward high-use data elements as well as explore why some data elements may not have as much use as anticipated. This will not only benefit ONC and SDOs, but in the long-term this will benefit patient care as exchange at the data element level is likely to be less cumbersome than document-based exchange. In addition, these measures are expected to increase transparency in the health IT app market which should lead to improved efficiencies, more competition, and better use of data. Greater transparency will inform decision-making among app developers, patients, health care providers, and other key parties (*e.g.,* CARIN Alliance). Through better insights into the intersections of health IT and the app market, gaps as well as areas of strength can be identified that may spur further innovations in the market.

The ONC Cures Act Final Rule also introduced certification criteria and policies for the exchange of bulk patient health information. The goal of these functionalities is to make patient data requests easier and less expensive as well as allow health care providers a greater choice of health IT applications. Understanding how these functionalities are being used will allow ONC and others to assess the progress toward those goals and identify where there may be areas in need of refinement. It will provide interested parties, such as Accountable Care Organizations (ACO), researchers, and others with interest in secondary use of certified health IT data with insights as to whether such data is easily moved out of health IT products to support a variety of use cases to advance patient care.

Finally, because of the COVID–19 epidemic, there has been increased attention on the capabilities of health care providers to share public health information with public health agencies (PHA).[301] There has been a focus on the electronic exchange of immunization data to an immunization information system (IIS) via certified health IT. The

[300] Health Affairs. (2013). Health Policy Brief: Patient Engagement. Accessed March 16, 2023, at: *http://healthaffairs.org/healthpolicybriefs/brief_pdfs/healthpolicybrief_86.pdf.*

[301] Dixon BE, Caine VA, Halverson PK. Deficient Response to COVID–19 Makes the Case for Evolving the Public Health System. American Journal of Preventive Medicine. 2020;59(6):887–891. *https://doi.org/10.1016/j.amepre.2020.07.024.*

adopted measures will identify trends and patterns in IIS' ability to receive immunization data to enable innovative solutions and improve the utility of IIS' and IIS data. Thus, this data would be beneficial to IIS registries to help make improvements to their systems and policies to better support exchange of immunization data. In addition, these measures can help support the numerous HHS efforts aimed at improving the flow of information between health care providers and PHAs, such as ONC's STAR HIE Program and the CDC's ongoing Data Modernization Initiative.

Comments. We did not receive specific comments related to the Insights impact analysis. Commenters did, however, raise general concerns about the overall cost of the rulemaking, including costs estimated for Insights.

Response. We updated the Insights impact analysis based upon updates to the condition of certification, as adopted in this final rule. The impact analysis reflects reduced costs, as well as cost savings, to implement this finalized Condition of Certification.

Information Blocking Enhancements

We proposed in section IV of this preamble several enhancements with respect to the information blocking provisions in the ONC Cures Act Final Rule. These include defining in regulation text what it means, and what it does not mean, to ''offer'' health IT. The enhancements also include updating the Infeasibility (45 CFR 171.204) and Manner (45 CFR 171.301, formerly known as the ''Content and Manner'') Exceptions for clarity and to add more ways for actors' practices to satisfy these exceptions and thus not be considered ''information blocking'' for purposes of 45 CFR part 171.

Costs

We expect ONC to incur an annual cost for issuing educational resources related to the proposed information blocking enhancements. We estimate that ONC would issue educational resources each quarter, or at least four times per year. We assume that the resources would be provided by ONC staff with the expertise of a GS–15, Step 1 federal employee(s). The hourly wage with benefits for a GS–15, Step 1 employee located in Washington, DC is approximately $142.[302] We estimate it would take ONC staff between 100 and 200 hours to develop resources each quarter, or 400 to 800 hours annually. Therefore, we estimate the annual cost to ONC would, on average, range from $56,800 to $113,600.

Benefits

Currently, ONC has limited data and research available to reasonably estimate the benefits of how often an actor may avail itself of one of the permitted exceptions or the costs for an actor to meet a condition to an exception.

We anticipate that the adopted information blocking enhancements will enable actors to determine more easily and with greater certainty whether their practices (acts or omissions) that may or do interfere with access, exchange, or use of EHI (as defined in 45 CFR 171.102) meet the conditions to be considered a ''reasonable and necessary'' activity under an information blocking exception. As such, we expect these policies will further ease the burden and costs of complying with the information blocking regulations, while providing increased predictability. This predictability will permit regulated entities to plan and invest resources in developing and using interoperable technologies and services to improve healthcare efficiency and value more effectively. Additionally, we anticipate as a result of the revised definitions and exceptions, there will be reduced interference with the access, exchange, and use of electronic health information because of the added clarity the policies will provide the market regarding certain practices. Thus, we anticipate an increase in the overall benefits derived from reducing the prevalence of information blocking. We welcomed comment on these conclusions and the supporting rationale.

Total Annual Cost Estimate

We estimate that the total annual cost for this final rule for the first year after it is finalized (including one-time costs), based on the cost estimates outlined above and throughout this RIA, would result in $437 million. The total undiscounted perpetual cost over a 10-year period for this final rule (starting in year two), based on the cost estimates outlined above, would result in $477 million. We estimate the total costs to health IT developers to be $914 million while the government (ONC) costs to be between $56,800 to $113,600.

Total Annual Benefit Estimate

We estimate the total annual benefit for this final rule, based on the benefit estimates outlined above, would be on average $1.0 billion.

Total Annual Net Benefit

We estimate the total undiscounted perpetual annual net benefit for this final rule (starting in year three), based on the estimates outlined above, would result in a net benefit of $124 million.

b. Accounting Statement and Table

When a rule is considered significant under Section 3(f)(1) under Executive Order 12866 and E.O. 14094, we are required to develop an accounting statement indicating the classification of the expenditures associated with the provisions of the final rule. Monetary annual effects are presented as discounted flows using 3% and 7% factors in Table 38 below. We are not able to explicitly define the universe of all costs but have provided an average of likely costs of this final rule as well as a high and low range of likely costs.

TABLE 37—E.O. 12866 SUMMARY TABLE

[2022 Dollars]

	Primary (3%)	Primary (7%)
Present Value of Quantified Costs	$853,114,341	$784,445,719
Present Value of Quantified Benefits	829,421,937	623,925,956
Present Value of Net Benefits	23,692,404	160,519,763
Annualized Quantified Costs	100,011,026	111,687,422
Annualized Quantified Benefits	103,155,077	101,704,924
Annualized Net Quantified Benefits	3,144,051	9,982,498

[302] Office of Personnel and Management. *https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/pdf/2022/DCB.pdf.* Accessed March 16, 2023.

TABLE 38—E.O. 12866 SUMMARY TABLE NON-DISCOUNTED FLOWS

[2022 Dollars]

	Year 1	Year 2	Year 3	Year 4	Year 5
Costs	$437,500,845	$264,945,762	$50,769,243	$31,235,512	$21,692,039
Benefits	.....	.....	28,850,000	57,700,000	86,550,000
	Year 6	Year 7	Year 8	Year 9	Year 10
Costs	21,692,039	21,692,039	21,692,039	21,692,039	21,692,039
Benefits	115,400,000	144,250,000	173,100,000	201,950,000	230,800,000

D. Regulatory Flexibility Act

The Regulatory Flexibility Act (RFA) requires agencies to analyze options for regulatory relief of small entities, if a rule has a significant impact on a substantial number of small entities.

The Small Business Administration (SBA) establishes the size of small businesses for Federal Government programs based on average annual receipts or the average employment of a firm.[303] The entities that are likely to be directly affected by the requirements in this final rule requirements are health IT developers. We note that the finalized updates and clarifications to the reasonable and necessary activities that do not constitute information blocking will provide flexibilities and relief for health IT developers of certified health IT, health information networks, health information exchanges, and health care providers in relation to the information blocking provision of the Cures Act. We welcomed comments on the impact of our information blocking-related proposals on small entities.

Comments. We received no comments on our approach.

Response. We have finalized as proposed.

While health IT developers that pursue certification of their health IT under the Program represent a small segment of the overall information technology industry, we believe that many health IT developers impacted by the requirements adopted in this final rule most likely fall under the North American Industry Classification System (NAICS) code 541511 ''Custom Computer Programming Services.'' [304] OMB advised that the Federal statistical establishment data published for reference years beginning on or after January 1, 2022, should be published using the 2022 NAICS United States codes.[305] The SBA size standard associated with this NAICS code is set at $34 million annual receipts or less. There is enough data generally available to establish that between 75% and 90% of entities that are categorized under the NAICS code 541511 are under the SBA size standard. We also note that with the exception of aggregate business information available through the U.S. Census Bureau and the SBA related to NAICS code 541511, it appears that many health IT developers that pursue certification of their health IT under the Program are privately held or owned and do not regularly, if at all, make their specific annual receipts publicly available. As a result, it is difficult to locate empirical data related to many of these health IT developers to correlate to the SBA size standard. However, although not perfectly correlated to the size standard for NAICS code 541511, we do have information indicating that over 60% of health IT developers that have had Complete EHRs and/or Health IT Modules certified to the 2011 Edition have less than 51 employees.

We estimate that the finalized requirements in this final rule will have effects on health IT developers, some of which may be small entities, that have certified health IT or are likely to pursue certification of their health IT under the Program. We believe, however, that we have adopted the minimum number of requirements necessary to accomplish our primary policy goal of enhancing interoperability. Further, as discussed in this RIA above, there are very few appropriate regulatory or non-regulatory alternatives that could be developed to lessen the compliance burden associated with this final rule because at least a few of the policies are derived directly from legislative mandates in the Cures Act.

We do not believe that the finalized requirements of this final rule will create a significant impact on a substantial number of small entities and we received no comments on whether there are small entities that we have not identified that may be affected in a significant way. The Predictive DSI policy within the criterion adopted in the criterion at § 170.315(b)(11) and the Insights condition of certification represent the highest potential costs for health IT developers in our estimates. The finalized Decision Support Interventions policy establishes different requirements for developers of certified health IT that supply Predictive DSIs than those developers that do not supply Predictive DSIs. Many developers who do not supply a Predictive DSI as part of their Health IT Module are among those developers with smaller revenues and fewer clients. These developers will be able to certify to the criterion at § 170.315(b)(11) while expending limited additional development resources on products they have certified currently. Specifically, these developers will likely have little to no costs related to providing complete and up-to-date source attribute information for Predictive DSI supplied by the developer or engaging in risk management and annually update risk management information. Furthermore, the Insights Condition of Certification excludes small entities from reporting on the finalized measures. Small entities will face no additional costs for meeting the finalized measures, as described in the final policy and RIA for the Insights Condition.

The Secretary certifies that this final rule will not have a significant impact on a substantial number of small entities.

Comments. We received no comments.

Response. We have finalized as proposed.

E. Executive Order 13132—Federalism

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a final rule) that imposes substantial direct requirement costs on state and local governments, preempts state law, or otherwise has federalism implications.

[303] The SBA references that annual receipts mean ''total income'' (or in the case of a sole proprietorship, ''gross income'') plus ''cost of goods sold'' as these terms are defined and reported on Internal Revenue Service tax return forms.

[304] *https://www.sba.gov/sites/sbagov/files/2023-06/Table%20of%20Size%20Standardslowbar; Effective%20March%2017%2C%202023%20%282%29.pdf.*

[305] *https://www.sba.gov/article/2022/feb/01/guidance-using-naics-2022-procurement.*

Nothing in this final rule imposes substantial direct compliance costs on state and local governments, preempts state law, or otherwise has federalism implications. We are not aware of any state laws or regulations that are contradicted or impeded by any of the policies in this final rule.

Comments. We received no comments.

Response. We have finalized as proposed.

F. Unfunded Mandates Reform Act of 1995

Section 202 of the Unfunded Mandates Reform Act of 1995 requires that agencies assess anticipated costs and benefits before issuing any rule that imposes unfunded mandates on state, local, and tribal governments or the private sector requiring spending in any one year of $100 million in 1995 dollars, updated annually for inflation. The current inflation-adjusted statutory threshold is approximately $177 million in 2023. While the estimated potential cost effects of this final rule reach the statutory threshold, we do not believe this final rule imposes unfunded mandates on state, local, and tribal governments, or the private sector.

Comments. We received no comments.

Response. We have finalized as proposed.

OMB reviewed this final rule.

List of Subjects

45 CFR Part 170

Computer technology, Electronic health record, Electronic information system, Electronic transactions, Health, Healthcare, Health information technology, Health insurance, Health records, Hospitals, Incorporation by reference, Laboratories, Medicaid, Medicare, Privacy, Reporting and record keeping requirements, Public health, Security.

45 CFR Part 171

Computer technology, Electronic health record, Electronic information system, Electronic transactions, Health, Healthcare, Health care provider, Health information exchange, Health information technology, Health information network, Health insurance, Health records, Hospitals, Privacy, Reporting and recordkeeping requirements, Public health, Security.

For the reasons set forth in the preamble, 45 CFR subtitle A, subchapter D, is amended as follows:

PART 170—HEALTH INFORMATION TECHNOLOGY STANDARDS, IMPLEMENTATION SPECIFICATIONS, AND CERTIFICATION CRITERIA AND CERTIFICATION PROGRAMS FOR HEALTH INFORMATION TECHNOLOGY

■ 1. The authority citation for part 170 continues to read as follows:

Authority: 42 U.S.C. 300jj–11; 42 U.S.C 300jj–14; 5 U.S.C. 553.

■ 2. Amend § 170.102 by:
■ a. Removing definitions for ''2015 Edition Base EHR'' and ''2015 Edition health IT certification criteria''; and
■ b. Adding definitions for ''Base EHR'', ''ONC certification criteria for health IT'', ''Predictive Decision Support Intervention'', ''Provide'', and ''Revised certification criterion (or criteria)'' in alphabetical order.

The additions read as follows:

§ 170.102 Definitions.

Base EHR means an electronic record of health-related information on an individual that:

(1) Includes patient demographic and clinical health information, such as medical history and problem lists;

(2) Has the capacity:

(i) To provide clinical decision support;

(ii) To support physician order entry;

(iii) To capture and query information relevant to healthcare quality;

(iv) To exchange electronic health information with, and integrate such information from other sources; and

(3) Has been certified to the certification criteria adopted by the Secretary in—

(i) Section 170.315(a)(1), (2), or (3); (a)(5) and (14), (b)(1), (c)(1), and (g)(7), (9), (10); and (h)(1) or (2);

(ii) Section 170.315(a)(9) or (b)(11) for the period up to and including December 31, 2024; and

(iii) Section 170.315(b)(11) on and after January 1, 2025.

* * * * *

ONC certification criteria for health IT means the certification criteria in § 170.315.

* * * * *

Predictive Decision Support Intervention or Predictive DSI means technology that supports decision-making based on algorithms or models that derive relationships from training data and then produces an output that results in prediction, classification, recommendation, evaluation, or analysis.

* * * * *

Provide means the action or actions taken by a developer of certified Health IT Modules to make the certified health IT available to its customers.

* * * * *

Revised certification criterion (or criteria) means a certification criterion that meets at least one of the following:

(1) Has added or changed the capabilities described in the existing criterion in this part;

(2) Has an added or changed standard or implementation specification referenced in the existing criterion in this part; or

(3) Is specified through notice and comment rulemaking as an iterative or replacement version of an existing criterion in this part.

* * * * *

■ 3. Amend § 170.205 by:
■ a. Revising paragraph (a)(5); and
■ b. Adding paragraphs (a)(6) and (t).

The revision and additions read as follows:

§ 170.205 Content exchange standards and implementation specifications for exchanging electronic health information.

(a) * * *

(5) *Standard.* HL7 CDA® R2 Implementation Guide: C–CDA Templates for Clinical Notes R2.1 Companion Guide, Release 2 (incorporated by reference, see § 170.299). The adoption of this standard expires on January 1, 2026.

(6) *Standard.* HL7® CDA® R2 Implementation Guide: C–CDA Templates for Clinical Notes STU Companion Guide, Release 4.1—US Realm (incorporated by reference, see § 170.299).

* * * * *

(t) *Public health—electronic case reporting*—(1) *Standard.* HL7® FHIR® Implementation Guide: Electronic Case Reporting (eCR)—US Realm 2.1.0—STU 2 US (HL7 FHIR eCR IG) (incorporated by reference, see § 170.299).

(2) *Standard.* HL7 CDA® R2 Implementation Guide: Public Health Case Report—the Electronic Initial Case Report (eICR) Release 2, STU Release 3.1—US Realm (HL7 CDA eICR IG) (incorporated by reference, see § 170.299).

(3) *Standard.* HL7® CDA® R2 Implementation Guide: Reportability Response, Release 1, STU Release 1.1—US Realm (HL7 CDA RR IG) (incorporated by reference, see § 170.299).

(4) *Standard.* Reportable Conditions Trigger Codes Value Set for Electronic Case Reporting. (incorporated by reference, see § 170.299).

■ 4. Amend § 170.207 by:
■ a. Adding paragraph (a)(1);
■ b. Removing and reserving paragraph (a)(3);

■ c. Adding paragraph (c)(1);
■ d. Removing and reserving paragraph (c)(2);
■ e. Adding paragraphs (d)(1) and (4);
■ f. Adding paragraphs (e)(1) and (2), (f)(3)and (m)(2);
■ g. Revising paragraph (n)(1);
■ h. Adding paragraphs (n)(2) and (3);
■ i. Revising paragraphs (o)and (p); and
■ j. Adding paragraphs (r)(2) and (s)(2).

The additions and revisions read as follows:

§ 170.207 Vocabulary standards for representing electronic health information.

(a) * * *

(1) *Standard.* SNOMED CT®, U.S. Edition, March 2022 Release (incorporated by reference, see § 170.299).

* * * * *

(c) * * *

(1) *Standard.* Logical Observation Identifiers Names and Codes (LOINC®) Database Version 2.72, a universal code system for identifying health measurements, observations, and documents produced by the Regenstrief Institute, Inc., February 16, 2022 (incorporated by reference, see § 170.299).

* * * * *

(d) * * *

(1) *Standard.* RxNorm, a standardized nomenclature for clinical drugs produced by the United States National Library of Medicine, July 5, 2022 (incorporated by reference, see § 170.299).

* * * * *

(4) *Standard.* The code set specified at 45 CFR 162.1002(b)(2) as referenced in 45 CFR 162.1002(c)(1) for the time period on or after October 1, 2015.

(e) * * *

(1) *Standard.* HL7® Standard Code Set CVX—Vaccines Administered, dated through June 15, 2022 (incorporated by reference, see § 170.299).

(2) *Standard.* National Drug Code Directory (NDC)—Vaccine NDC Linker, dated July 19, 2022 (incorporated by reference, see § 170.299).

* * * * *

(f) * * *

(3) *Standard.* CDC Race and Ethnicity Code Set Version 1.2 (July 08, 2021) (incorporated by reference, see § 170.299).

* * * * *

(m) * * *

(2) *Standard.* The Unified Code for Units of Measure, Version 2.1, November 21, 2017 (incorporated by reference, see § 170.299).

(n) * * *

(1) *Standard.* Birth sex must be coded in accordance with HL7® Version 3 Standard, Value Sets for AdministrativeGender and NullFlavor (incorporated by reference, see § 170.299), up until the adoption of this standard expires January 1, 2026, attributed as follows:

(i) Male. M;

(ii) Female. F;

(iii) Unknown. NullFlavor UNK.

(2) *Standard.* Sex must be coded in accordance with, at a minimum, the version of SNOMED CT ® U.S. Edition codes specified in paragraph (a)(1) of this section.

(3) *Standard.* Sex Parameter for Clinical Use must be coded in accordance with, at a minimum, the version of LOINC® codes specified in paragraph (c)(1) of this section.

(o) *Sexual orientation and gender information*—(1) *Standard.* Sexual orientation must be coded in accordance with, at a minimum, the version of SNOMED–CT® U.S. Edition codes specified in paragraph (a)(4) of this section for paragraphs (o)(1)(i) through (iii) of this section and HL7 Version 3 Standard, Value Sets for AdministrativeGender and NullFlavor (incorporated by reference, see § 170.299), up until the adoption of this standard expires on January 1, 2026, for paragraphs (o)(1)(iv) through (vi) of this section, attributed as follows:

(i) *Lesbian, gay or homosexual.* 38628009

(ii) *Straight or heterosexual.* 20430005

(iii) *Bisexual.* 42035005

(iv) *Something else, please describe.* NullFlavor OTH

(v) *Don't know.* NullFlavor UNK

(vi) *Choose not to disclose.* NullFlavor ASKU

(2) *Standard.* Gender identity must be coded in accordance with, at a minimum, the version of SNOMED–CT® codes specified in paragraph (a)(4) of this section for paragraphs (o)(2)(i) through (v) of this section and HL7® Version 3 Standard, Value Sets for AdministrativeGender and NullFlavor (incorporated by reference in § 170.299), up until the adoption of this standard expires January 1, 2026, for paragraphs (o)(2)(vi) and (vii) of this section, attributed as follows:

(i) *Male.* 446151000124109

(ii) *Female.* 446141000124107

(iii) *Female-to-Male (FTM)/ Transgender Male/Trans Man.* 407377005

(iv) *Male-to-Female (MTF)/ Transgender Female/Trans Woman.* 407376001

(v) *Genderqueer, neither exclusively male nor female.* 446131000124102

(vi) *Additional gender category or other, please specify.* NullFlavor OTH

(vii) *Choose not to disclose.* NullFlavor ASKU

(3) *Standard.* Sexual Orientation and Gender Identity must be coded in accordance with, at a minimum, the version of SNOMED CT® codes specified in paragraph (a)(1) of this section.

(4) *Standard.* Pronouns must be coded in accordance with, at a minimum, the version of LOINC® codes specified in paragraph (c)(1) of this section.

(p) *Social, psychological, and behavioral data*—(1) *Financial resource strain.* Financial resource strain must be coded in accordance with, at a minimum, the version of LOINC® codes specified in paragraph (c)(1) of this section and attributed with the LOINC® code 76513–1 and LOINC® answer list ID LL3266–5.

(2) *Education.* Education must be coded in accordance with, at a minimum, the version of LOINC® codes specified in paragraph (c)(1) of this section and attributed with LOINC® code 63504–5 and LOINC® answer list ID LL1069–5.

(3) *Stress.* Stress must be coded in accordance with, at a minimum, the version of LOINC® codes specified in paragraph (c)(1) of this section and attributed with the LOINC® code 76542–0 and LOINC® answer list LL3267–3.

(4) *Depression.* Depression must be coded in accordance with, at a minimum, the version of LOINC® codes specified in paragraph (c)(1) of this section and attributed with LOINC® codes 55757–9, 44250–9 (with LOINC® answer list ID LL361–7), 44255–8 (with LOINC® answer list ID LL361–7), and 55758–7 (with the answer coded with the associated applicable unit of measure in the standard specified in paragraph (m)(2) of this section).

(5) *Physical activity.* Physical activity must be coded in accordance with, at a minimum, the version of LOINC® codes specified in paragraph (c)(1) of this section and attributed with LOINC® codes 68515–6 and 68516–4. The answers must be coded with the associated applicable unit of measure in the standard specified in paragraph (m)(2) of this section.

(6) *Alcohol use.* Alcohol use must be coded in accordance with, at a minimum, the version of LOINC® codes specified in paragraph (c)(1) of this section and attributed with LOINC® codes 72109–2, 68518–0 (with LOINC® answer list ID LL2179–1), 68519–8 (with LOINC® answer list ID LL2180–9), 68520–6 (with LOINC® answer list ID LL2181–7), and 75626–2 (with the answer coded with the associated applicable unit of measure in the standard specified in paragraph (m)(2) of this section).

(7) *Social connection and isolation.* Social connection and isolation must be coded in accordance with, at a minimum, the version of LOINC® codes specified in paragraph (c)(1) of this section and attributed with the LOINC® codes 76506–5, 63503–7 (with LOINC® answer list ID LL1068–7), 76508–1 (with the associated applicable unit of measure in the standard specified in paragraph (m)(2) of this section), 76509–9 (with the associated applicable unit of measure in the standard specified in paragraph (m)(2) of this section), 76510–7 (with the associated applicable unit of measure in the standard specified in paragraph (m)(2) of this section), 76511–5 (with LOINC answer list ID LL963–0), and 76512–3 (with the associated applicable unit of measure in the standard specified in paragraph (m)(2) of this section).

(8) *Exposure to violence (intimate partner violence).* Exposure to violence: Intimate partner violence must be coded in accordance with, at a minimum, the version of LOINC® codes specified in paragraph (c)(1) of this section and attributed with the LOINC® code 76499–3, 76500–8 (with LOINC® answer list ID LL963–0), 76501–6 (with LOINC® answer list ID LL963–0), 76502–4 (with LOINC® answer list ID LL963–0), 76503–2 (with LOINC® answer list ID LL963–0), and 76504–0 (with the associated applicable unit of measure in the standard specified in paragraph (m)(2) of this section).

* * * * *

(r) * * *

(2) *Standard.* Medicare Provider and Supplier Taxonomy Crosswalk, 2021 (incorporated by reference, see § 170.299).

(s) * * *

(2) *Standard.* Public Health Data Standards Consortium Users Guide for Source of Payment Typology, Version 9.2 (incorporated by reference, see § 170.299).

■ 5. Amend § 170.210 by revising paragraph (g) to read as follows:

§ 170.210 Standards for health information technology to protect electronic health information created, maintained, and exchanged.

* * * * *

(g) *Synchronized clocks.* The date and time recorded utilize a system clock that has been synchronized using any Network Time Protocol (NTP) standard.

* * * * *

■ 6. Revise § 170.213 to read as follows:

§ 170.213 United States Core Data for Interoperability.

The Secretary adopts the following versions of the United States Core Data for Interoperability standard:

(a) *Standard.* United States Core Data for Interoperability (USCDI), July 2020 Errata, Version 1 (v1) (incorporated by reference, see § 170.299). The adoption of this standard expires on January 1, 2026.

(b) *Standard.* United States Core Data for Interoperability Version 3 (USCDI v3) (incorporated by reference, see § 170.299).

■ 7. Revise § 170.215 to read as follows:

§ 170.215 Application Programming Interface Standards.

The Secretary adopts the following standards and associated implementation specifications as the available standards for application programming interfaces (API):

(a) *API base standard.* The following are applicable for purposes of standards-based APIs.

(1) *Standard.* HL7® Fast Healthcare Interoperability Resources (FHIR®) Release 4.0.1 (incorporated by reference, see § 170.299).

(2) [Reserved]

(b) *API constraints and profiles.* The following are applicable for purposes of constraining and profiling data standards.

(1) *United States Core Data Implementation Guides*—(i) *Implementation specification.* HL7® FHIR® US Core Implementation Guide STU 3.1.1 (incorporated by reference in § 170.299). The adoption of this standard expires on January 1, 2026.

(ii) *Implementation Specification.* HL7® FHIR® US Core Implementation Guide STU 6.1.0 (incorporated by reference, see § 170.299).

(2) [Reserved]

(c) *Application access and launch.* The following are applicable for purposes of enabling client applications to access and integrate with data systems.

(1) *Implementation specification.* HL7® SMART Application Launch Framework Implementation Guide Release 1.0.0, including mandatory support for the ''SMART Core Capabilities'' (incorporated by reference, see § 170.299). The adoption of this standard expires on January 1, 2026.

(2) *Implementation specification.* HL7® SMART App Launch Implementation Guide Release 2.0.0, including mandatory support for the ''Capability Sets'' of ''Patient Access for Standalone Apps'' and ''Clinician Access for EHR Launch''; all ''Capabilities'' as defined in ''8.1.2 Capabilities,'' excepting the ''permission-online'' capability; ''Token Introspection'' as defined in ''7 Token Introspection'' (incorporated by reference, see § 170.299).

(d) *Bulk export and data transfer standards.* The following are applicable for purposes of enabling access to large volumes of information on a group of individuals.

(1) *Implementation specification.* FHIR® Bulk Data Access (Flat FHIR®) (v1.0.0: STU 1), including mandatory support for the ''group-export'' ''OperationDefinition'' (incorporated by reference, see § 170.299).

(2) [Reserved]

(e) *API authentication, security, and privacy.* The following are applicable for purposes of authorizing and authenticating client applications.

(1) *Standard.* OpenID Connect Core 1.0, incorporating errata set 1 (incorporated by reference, see § 170.299).

(2) [Reserved]

■ 8. Amend § 170.299 by:

■ a. Revising paragraph (a) and the introductory text of paragraph (d);

■ b. Adding paragraphs (d)(17) through (19);

■ c. Revising the introductory text of paragraph (e) and adding paragraph (e)(6)

■ d. Removing paragraph (j) and redesignating paragraphs (f) through (i) as paragraphs (g) through (j), respectively;

■ e. Adding new paragraph (f);

■ f. Revising the introductory text of newly redesignated paragraph (g) and adding paragraphs (g)(35) through (40);

■ g. Revising the introductory text of paragraph (m) and adding paragraph (m)(6);

■ h. Revising the introductory text of paragraph (o) and adding paragraph (o)(2);

■ i. Revising the introductory text of paragraph (p) and adding paragraphs (p)(5) and (6);

■ j. Revising the introductory text of paragraph (r) and adding paragraphs (r)(8) and (9).

The revisions and additions read as follows:

§ 170.299 Incorporation by reference.

(a) Certain material is incorporated by reference into this part with the approval of the Director of the Federal Register under 5 U.S.C. 552(b) and 1 CFR part 51. All approved incorporation by reference (IBR) material is available for inspection at the U.S. Department of Health and Human Services (HHS) and at the National Archives and Records Administration (NARA). Contact HHS at: U.S. Department of Health and

Human Services, Office of the National Coordinator for Health Information Technology, 330 C Street SW, Washington, DC 20201; call ahead to arrange for inspection at 202–690–7151. For information on the availability of this material at NARA, visit *www.archives.gov/federal-register/cfr/ibr-locations* or email *fr.inspection@nara.gov.* The material may be obtained from the sources in the following paragraphs of this section.

* * * * *

(d) Centers for Disease Control and Prevention, 2500 Century Parkway, Mailstop E–78, Atlanta, GA 30333; phone: (800) 232–4636); website: *www.cdc.gov/cdc-info/index.html*

* * * * *

(17) HL7® Standard Code Set CVX—Vaccines Administered, dated June 15, 2022; IBR approved for § 170.207(e).

(18) National Drug Code Directory (NDC)—Vaccine NDC Linker, dated July 19, 2022; IBR approved for § 170.207(e).

(19) CDC Race and Ethnicity Code Set version 1.2 (July 08, 2021); IBR approved for § 170.207(f).

(e) Centers for Medicare & Medicaid Services, Office of Clinical Standards and Quality, 7500 Security Boulevard, Baltimore, Maryland 21244; phone: (410) 786–3000; website: *www.cms.gov.*

* * * * *

(6) Medicare Provider and Supplier Taxonomy Crosswalk, 2021; IBR approved for § 170.207(r).

(f) Council of State and Territorial Epidemiologists, 2635 Century Parkway NE, Suite 700, Atlanta, GA 30345; phone: (770) 458–3811; website: *www.cste.org/*

(1) Reportable Conditions Trigger Codes Value Set for Electronic Case Reporting. RCTC OID: 2.16.840.1.114222.4.11.7508, Release March 29, 2022; IBR approved for § 170.205(t).

(2) [Reserved]

(g) Health Level Seven, 3300 Washtenaw Avenue, Suite 227, Ann Arbor, MI 48104; phone: (734) 677–7777; website: *www.hl7.org/*

* * * * *

(35) HL7 CDA® R2 Implementation Guide: C–CDA Templates for Clinical Notes STU Companion Guide, Release 4.1 (US Realm) Standard for Trial Use, Specification Version: 4.1.1, June 2023 (including appendices A and B); IBR approved for § 170.205(a).

(36) HL7 FHIR® Implementation Guide: Electronic Case Reporting (eCR)—US Realm, Version 2.1.0—STU 2 US (HL7 FHIR eCR IG), August 31, 2022; IBR approved for § 170.205(t).

(37) HL7 CDA® R2 Implementation Guide: Public Health Case Report—the Electronic Initial Case Report (eICR) Release 2, STU Release 3.1—US Realm (HL7 CDA eICR IG), July 2022, volumes 1 and 2; IBR approved for § 170.205(t).

(38) HL7 CDA® R2 Implementation Guide: Reportability Response, Release 1, STU Release 1.1—US Realm (HL7 CDA RR IG), July 2022, volumes 1 through 4; IBR approved for § 170.205(t).

(39) HL7 FHIR US Core Implementation Guide Version 6.1.0—STU 6, June 19, 2023; IBR approved for § 170.215(b).

(40) HL7 FHIR® SMART App Launch [Implementation Guide], 2.0.0—Standard for Trial Use, November 26, 2021; IBR approved for § 170.215(c).

* * * * *

(m) Office of the National Coordinator for Health Information Technology (ONC), 330 C Street SW, Washington, DC 20201; phone: (202) 690–7151; website: *https://healthit.gov.*

* * * * *

(6) United States Core Data for Interoperability (USCDI), Version 3 (v3), October 2022 Errata; IBR approved for § 170.213(b).

* * * * *

(o) Public Health Data Standards Consortium, 111 South Calvert Street, Suite 2700, Baltimore, MD 21202; phone: (801) 532–2299; website: *www.Ph.D.sc.org/.*

* * * * *

(2) Users Guide for Source of Payment Typology, Version 9.2, December 2020; IBR approved for § 170.207(s).

(p) Regenstrief Institute, Inc., LOINC® c/o Regenstrief Center for Biomedical Informatics, Inc., 410 West 10th Street, Suite 2000, Indianapolis, IN 46202–3012; phone: (317) 274–9000; website: *https://loinc.org/* and *https://ucum.org/ucum.*

* * * * *

(5) Logical Observation Identifiers Names and Codes (LOINC®) Database Version 2.72, February 2022; IBR approved for § 170.207(c).

(6) The Unified Code for Units of Measure, Version 2.1, November 21, 2017; IBR approved for § 170.207(m).

* * * * *

(r) U.S. National Library of Medicine, 8600 Rockville Pike, Bethesda, MD 20894; phone (301) 594–5983; website: *www.nlm.nih.gov/.*

* * * * *

(8) SNOMED CT® [Systematized Nomenclature of Medicine Clinical Terms] U.S. Edition, March 2022 Release; IBR approved for § 170.207(a).

(9) RxNorm, Full Update Release, July 5, 2022; IBR approved for § 170.207(d).

* * * * *

■ 9. Amend § 170.315 by:

■ a. Revising the section heading, introductory text, and paragraphs (a)(5) paragraph heading, (a)(5)(i) introductory text, (a)(5)(i)(A)(*1*) and (*2*), (a)(5)(i)(C), (D), and (E);

■ b. Adding paragraphs (a)(5)(i)(F), (G), and (H) and (a)(9)(vi);

■ c. Revising paragraphs (a)(12), (b)(1)(iii)(A)(*1*) and (*2*); (b)(1)(iii)(B)(*2*), (b)(1)(iii)(G) introductory text, (b)(1)(iii)(G)(*3*), (b)(2)(i) and (ii), (b)(2)(iii)(D), and (b)(2)(iv), (b)(3), (b)(6)(ii)(B)(*2*), (b)(9)(ii);

■ d. Adding paragraph (b)(11);

■ e. Revising paragraphs (c)(4)(iii)(C), (E), (G), (H), and (I);

■ f. Revising paragraphs (e)(1)(i)(A)(*1*) and (*2*), (e)(1)(i)(B)(*1*) and (*2*), and adding paragraph (e)(1)(iii);

■ g. Revising paragraphs (f)(1)(i)(B) and (C), (f)(3)(ii), (f)(4)(ii), (f)(5); and

■ h. Revising paragraphs (g)(3) introductory text, (g)(6)(i)(A) and (B), (g)(9)(i)(A)(*1*) and (*2*), (g)(10)(i)(A) and (B), (g)(10)(ii)(A) and (B), (g)(10)(iv)(A) and (B), (g)(10)(v)(A)(*1*)(i), (*ii*) and (B), (*2*)(*i*) and (*ii*), (g)(10)(vi), and (g)(10)(vii).

The revisions and additions read as follows:

§ 170.315 ONC Certification Criteria for Health IT.

The Secretary adopts the following certification criteria for health IT. Health IT must be able to electronically perform the following capabilities in accordance with applicable standards and implementation specifications adopted in this part. For all criteria in this section, a health IT developer with a Health IT Module certified to any revised certification criterion, as defined in § 170.102, shall update the Health IT Module and shall provide such update to their customers in accordance with the dates identified for each revised certification criterion and for each applicable standard in 45 CFR part 170 subpart B.

(a) * * *

(5) *Patient demographics and observations.* (i) Enable a user to record, change, and access patient demographic and observations data including race, ethnicity, preferred language, sex, sex parameter for clinical use, sexual orientation, gender identity, name to use, pronouns, and date of birth.

(A) * * *

(*1*) Enable each one of a patient's races to be recorded in accordance with, at a minimum, the standard specified in § 170.207(f)(3) and whether a patient declines to specify race.

(*2*) Enable each one of a patient's ethnicities to be recorded in accordance with, at a minimum, the standard

specified in § 170.207(f)(3) and whether a patient declines to specify ethnicity.

* * * * *

(C) *Sex.* Enable sex to be recorded in accordance with the standard specified in § 170.207(n)(1) for the period up to and including December 31, 2025; or § 170.207(n)(2).

(D) *Sexual orientation.* Enable sexual orientation to be recorded in accordance with, at a minimum, the version of the standard specified in § 170.207(o)(1) for the period up to and including December 31, 2025; or § 170.207(o)(3), as well as whether a patient declines to specify sexual orientation.

(E) *Gender identity.* Enable gender identity to be recorded in accordance with, at a minimum, the version of the standard specified in § 170.207(o)(2) for the period up to and including December 31, 2025; or § 170.207(o)(3), as well as whether a patient declines to specify gender identity.

(F) *Sex Parameter for Clinical Use.* Enable at least one sex parameter for clinical use to be recorded in accordance with, at a minimum, the version of the standard specified in § 170.207(n)(3). Conformance with this paragraph is required by January 1, 2026.

(G) *Name to Use.* Enable at least one preferred name to use to be recorded. Conformance with this paragraph is required by January 1, 2026.

(H) *Pronouns.* Enable at least one pronoun to be recorded in accordance with, at a minimum, the version of the standard specified in § 170.207(o)(4). Conformance with this paragraph is required by January 1, 2026.

* * * * *

(9) * * *

(vi) *Expiration of Criterion.* The adoption of this criterion for purposes of the ONC Health IT Certification Program expires on January 1, 2025.

* * * * *

(12) *Family health history.* Enable a user to record, change, and access a patient's family health history in accordance with the familial concepts or expressions included in, at a minimum, the version of the standard in § 170.207(a)(1).

* * * * *

(b) * * *

(1) * * *

(iii) * * *

(A) * * *

(*1*) The data classes expressed in the standards in § 170.213 and in accordance with § 170.205(a)(4), (5), and paragraphs (b)(1)(iii)(A)(*3*)(*i*) through (*iii*) of this section for the time period up to and including December 31, 2025, or

(*2*) The data classes expressed in the standards in § 170.213 and in accordance with § 170.205(a)(4), (6), and paragraphs (b)(1)(iii)(A)(*3*)(*i*) through (*iii*) of this section, and

* * * * *

(B) * * *

(*2*) At a minimum, the version of the standard specified in § 170.207(a)(1).

* * * * *

(G) *Patient matching data.* First name, last name, previous name, middle name (including middle initial), suffix, date of birth, current address, phone number, and sex. The following constraints apply:

* * * * *

(*3*) *Sex Constraint:* Represent sex with the standards adopted in § 170.207(n)(2).

(2) * * *

(i) *General Requirements.* Paragraphs (b)(2)(ii) and (iii) of this section must be completed based on the receipt of a transition of care/referral summary formatted in accordance with the standards adopted in § 170.205(a)(3) through (5) using the Continuity of Care Document, Referral Note, and (inpatient setting only) Discharge Summary document templates, for time period up to and including December 31, 2025; or in accordance with the standards adopted in § 170.205(a)(3), (4), (6).

(ii) *Correct patient.* Upon receipt of a transition of care/referral summary formatted according to the standards adopted § 170.205(a)(3) through (5) for the period up to and including December 31, 2025; or according to the standards adopted § 170.205(a)(3), (4), and (6), technology must be able to demonstrate that the transition of care/referral summary received can be properly matched to the correct patient.

(iii) * * *

(D) Upon a user's confirmation, automatically update the list, and incorporate the following data expressed according to the specified standards:

* * * * *

(iv) *System verification.* Based on the data reconciled and incorporated, the technology must be able to create a file formatted according to the standard specified in § 170.205(a)(4) using the Continuity of Care Document template and the standard specified in paragraph (a)(5) of this section for the time period up to and including December 31, 2025; or according to the standard specified in § 170.205(a)(4) using the Continuity of Care Document template and the standard specified in paragraph (a)(6) of this section.

* * * * *

(3) * * *

(ii) * * *

(A) Enable a user to perform the following prescription-related electronic transactions in accordance with the standard specified in § 170.205(b)(1) and, at a minimum, the version of the standard specified in § 170.207(d)(1) as follows:

(6) * * *

(ii) * * *

(B) * * *

(*2*) At a minimum, the version of the standard specified in § 170.207(a)(1).

* * * * *

(9) * * *

(ii) The standard in § 170.205(a)(5) for the time period up to and including December 31, 2025; or § 170.205(a)(6).

* * * * *

(11) Decision support interventions —

(i) *Decision support intervention interaction.* Interventions provided to a user must occur when a user is interacting with technology.

(ii) *Decision support configuration.* (A) Enable interventions specified in paragraphs (b)(11)(iii) of this section to be configured by a limited set of identified users based on a user's role.

(B) Enable interventions when a patient's medications, allergies and intolerance, and problems are incorporated from a transition of care or referral summary received and pursuant to paragraph (b)(2)(iii)(D) of this section.

(C) Enable a user to provide electronic feedback data for evidence-based decision support interventions selected via the capability provided in paragraph (b)(11)(iii)(A) of this section and make available such feedback data to a limited set of identified users for export, in a computable format, including at a minimum the intervention, action taken, user feedback provided (if applicable), user, date, and location.

(iii) *Decision support intervention selection.* Enable a limited set of identified users to select (*i.e.,* activate) electronic decision support interventions (in addition to drug-drug and drug-allergy contraindication checking) that are:

(A) Evidence-based decision support interventions and use any data based on the following data expressed in the standards in § 170.213:

(*1*) Problems;

(*2*) Medications;

(*3*) Allergies and Intolerances;

(*4*) At least one demographic specified in paragraph (a)(5)(i) of this section;

(*5*) Laboratory;

(*6*) Vital Signs;

(*7*) Unique Device Identifier(s) for a Patient's Implantable Device(s); and

(*8*) Procedures.

(B) Predictive Decision Support Interventions and use any data expressed in the standards in § 170.213.

(iv) *Source attributes.* Source attributes listed in paragraphs (b)(11)(iv)(A) and (B) of this section must be supported.

(A) For evidence-based decision support interventions:

(*1*) Bibliographic citation of the intervention (clinical research or guideline);

(*2*) Developer of the intervention (translation from clinical research or guideline);

(*3*) Funding source of the technical implementation for the intervention(s) development;

(*4*) Release and, if applicable, revision dates of the intervention or reference source;

(*5*) Use of race as expressed in the standards in § 170.213;

(*6*) Use of ethnicity as expressed in the standards in § 170.213;

(*7*) Use of language as expressed in the standards in § 170.213;

(*8*) Use of sexual orientation as expressed in the standards in § 170.213;

(*9*) Use of gender identity as expressed in the standards in § 170.213;

(*10*) Use of sex as expressed in the standards in § 170.213;

(*11*) Use of date of birth as expressed in the standards in § 170.213;

(*12*) Use of social determinants of health data as expressed in the standards in § 170.213; and

(*13*) Use of health status assessments data as expressed in the standards in § 170.213.

(B) For Predictive Decision Support Interventions:

(*1*) Details and output of the intervention, including:

(*i*) Name and contact information for the intervention developer;

(*ii*) Funding source of the technical implementation for the intervention(s) development;

(*iii*) Description of value that the intervention produces as an output; and

(*iv*) Whether the intervention output is a prediction, classification, recommendation, evaluation, analysis, or other type of output.

(*2*) Purpose of the intervention, including:

(*i*) Intended use of the intervention;

(*ii*) Intended patient population(s) for the intervention's use;

(*iii*) Intended user(s); and

(*iv*) Intended decision-making role for which the intervention was designed to be used/for (*e.g.,* informs, augments, replaces clinical management).

(*3*) Cautioned out-of-scope use of the intervention, including:

(*i*) Description of tasks, situations, or populations where a user is cautioned against applying the intervention; and

(*ii*) Known risks, inappropriate settings, inappropriate uses, or known limitations.

(*4*) Intervention development details and input features, including at a minimum:

(*i*) Exclusion and inclusion criteria that influenced the training data set;

(*ii*) Use of variables in paragraphs (b)(11)(iv)(A)(*5*) through (*13*) of this section as input features;

(*iii*) Description of demographic representativeness according to variables in paragraphs (b)(11)(iv)(A)(*5*) through (*13*) of this section including, at a minimum, those used as input features in the intervention;

(*iv*) Description of relevance of training data to intended deployed setting; and

(*5*) Process used to ensure fairness in development of the intervention, including:

(*i*) Description of the approach the intervention developer has taken to ensure that the intervention's output is fair; and

(*ii*) Description of approaches to manage, reduce, or eliminate bias.

(*6*) External validation process, including:

(*i*) Description of the data source, clinical setting, or environment where an intervention's validity and fairness has been assessed, other than the source of training and testing data

(*ii*) Party that conducted the external testing;

(*iii*) Description of demographic representativeness of external data according to variables in paragraph (b)(11)(iv)(A)(*5*)–(*13*) including, at a minimum, those used as input features in the intervention; and

(*iv*) Description of external validation process.

(*7*) Quantitative measures of performance, including:

(*i*) Validity of intervention in test data derived from the same source as the initial training data;

(*ii*) Fairness of intervention in test data derived from the same source as the initial training data;

(*iii*) Validity of intervention in data external to or from a different source than the initial training data;

(*iv*) Fairness of intervention in data external to or from a different source than the initial training data;

(*v*) References to evaluation of use of the intervention on outcomes, including, bibliographic citations or hyperlinks to evaluations of how well the intervention reduced morbidity, mortality, length of stay, or other outcomes;

(*8*) Ongoing maintenance of intervention implementation and use, including:

(*i*) Description of process and frequency by which the intervention's validity is monitored over time;

(*ii*) Validity of intervention in local data;

(*iii*) Description of the process and frequency by which the intervention's fairness is monitored over time;

(*iv*) Fairness of intervention in local data; and

(*9*) Update and continued validation or fairness assessment schedule, including:

(*i*) Description of process and frequency by which the intervention is updated; and

(*ii*) Description of frequency by which the intervention's performance is corrected when risks related to validity and fairness are identified.

(v) *Source attribute access and modification.* (A) *Access.* (*1*) For evidence-based decision support interventions and Predictive Decision Support Interventions supplied by the health IT developer as part of its Health IT Module, the Health IT Module must enable a limited set of identified users to access complete and up-to-date plain language descriptions of source attribute information specified in paragraphs (b)(11)(iv)(A) and (B) of this section.

(*2*) For Predictive Decision Support Interventions supplied by the health IT developer as part of its Health IT Module, the Health IT Module must indicate when information is not available for review for source attributes in paragraphs (b)(11)(iv)(B)(*6*); (b)(11)(iv)(B)(*7*)(*iii*), (*iv*), and (*v*); (b)(11)(iv)(B)(*8*)(*ii*) and (*iv*); and (b)(11)(iv)(B)(*9*) of this section.

(B) *Modify.* (*1*) For evidence-based decision support interventions and Predictive Decision Support Interventions, the Health IT Module must enable a limited set of identified users to record, change, and access source attributes in paragraphs (b)(11)(iv)(A) and (B) of this section.

(*2*) For Predictive Decision Support Interventions, the Health IT Module must enable a limited set of identified users to record, change, and access additional source attributes not specified in paragraph (b)(11)(iv)(B) of this section.

(vi) *Intervention risk management.* Intervention risk management practices must be applied for each Predictive Decision Support Intervention supplied by the health IT developer as part of its Health IT Module.

(A) *Risk analysis.* The Predictive Decision Support Intervention(s) must be subject to analysis of potential risks and adverse impacts associated with the following characteristics: validity, reliability, robustness, fairness,

intelligibility, safety, security, and privacy.

(B) *Risk mitigation.* The Predictive Decision Support Intervention (s) must be subject to practices to mitigate risks, identified in accordance with paragraph (b)(11)(vi)(A) of this section; and

(C) *Governance.* The Predictive Decision Support Intervention(s) must be subject to policies and implemented controls for governance, including how data are acquired, managed, and used.

(c) * * *

(4) * * *

(iii) * * *

(C) Provider type in accordance with, at a minimum, the standard specified in § 170.207(r)(2).

* * * * *

(E) Patient insurance in accordance with the standard specified in § 170.207(s)(2).

* * * * *

(G) Patient sex in accordance with the version of the standard specified in § 170.207(n)(2).

(H) Patient race and ethnicity in accordance with, at a minimum, the version of the standard specified in § 170.207(f)(3).

(I) Patient problem list data in accordance with, at a minimum, the version of the standard specified in § 170.207(a)(1).

(e) * * *

(1) * * *

(i) * * *

(A) * * *

(*1*) The data classes expressed in the standards in § 170.213 (which should be in their English (*i.e.,* non-coded) representation if they associate with a vocabulary/code set), and in accordance with § 170.205(a)(4) and (a)(5), and paragraphs (e)(1)(i)(A)(*3*)(*i*) through (*iii*) of this section for the time period up to and including December 31, 2025, or

(*2*) The data classes expressed in the standards in § 170.213 (which should be in their English (*i.e.,* non-coded) representation if they associate with a vocabulary/code set), and in accordance with § 170.205(a)(4) and (a)(6), and paragraphs (e)(1)(i)(A)(*3*)(*i*) through (*iii*) of this section.

* * * * *

(B) * * *

(*1*) Patients (and their authorized representatives) must be able to use technology to download an ambulatory summary or inpatient summary (as applicable to the health IT setting for which certification is requested) in the following formats:

(*i*) Human readable format; and

(*ii*) The format specified in accordance with the standard specified in § 170.205(a)(4) and (5) for the time period up to and including December 31, 2025, or § 170.205(a)(4) and (6), and following the CCD document template.

(*2*) When downloaded according to the standard specified in § 170.205(a)(4) through (6) following the CCD document template, the ambulatory summary or inpatient summary must include, at a minimum, the following data (which, for the human readable version, should be in their English representation if they associate with a vocabulary/code set):

* * * * *

(iii) *Request for restrictions.* Patients (and their authorized representatives) must be able to use an internet-based method to request a restriction to be applied for any data expressed in the standards in § 170.213. Conformance with this paragraph is required by January 1, 2026.

* * * * *

(f) * * *

(1) * * *

(i) * * *

(B) At a minimum, the version of the standard specified in § 170.207(e)(1) for historical vaccines.

(C) At a minimum, the version of the standard specified in § 170.207(e)(2) for administered vaccines.

(3) * * *

(ii) At a minimum, the versions of the standards specified in § 170.207(a)(1) and (c)(1).

(4) * * *

(ii) At a minimum, the versions of the standards specified in § 170.207(a)(1) and (c)(1).

(5) *Transmission to public health agencies—electronic case reporting.* Enable a user to create a case report for electronic transmission meeting the requirements described in paragraphs (f)(5)(i) of this section for the time period up to and including December 31, 2025; or the requirements described in paragraph (f)(5)(ii) of this section.

(i) *Functional electronic case reporting.* A Health IT Module must enable a user to create a case report for electronic transmission in accordance with the following:

(A) Consume and maintain a table of trigger codes to determine which encounters may be reportable.

(B) Match a patient visit or encounter to the trigger code based on the parameters of the trigger code table.

(C) *Case report creation.* Create a case report for electronic transmission:

(*1*) Based on a matched trigger from paragraph (f)(5)(i)(B).

(*2*) That includes, at a minimum:

(*i*) The data classes expressed in the standards in § 170.213.

(ii) Encounter diagnoses formatted according to at least one of the standards specified in § 170.207(i) or § 170.207(a)(1).

(*iii*) The provider's name, office contact information, and reason for visit.

(*iv*) An identifier representing the row and version of the trigger table that triggered the case report.

(ii) *Standards-based electronic case reporting.* A Health IT Module must enable a user to create a case report for electronic transmission in accordance with the following:

(A) Consume and process case reporting trigger codes and identify a reportable patient visit or encounter based on a match from the Reportable Conditions Trigger Code value set in § 170.205(t)(4).

(B) Create a case report consistent with at least one of the following standards:

(*1*) The eICR profile of the HL7 FHIR eCR IG in § 170.205(t)(1); or

(*2*) The HL7 CDA eICR IG in § 170.205(t)(2).

(C) Receive, consume, and process a case report response that is formatted to either the reportability response profile of the HL7 FHIR eCR IG in § 170.205(t)(1) or the HL7 CDA RR IG in § 170.205(t)(3) as determined by the standard used in (f)(5)(ii)(B) of this section.

(D) Transmit a case report electronically to a system capable of receiving a case report.

* * * * *

(g) * * *

(3) *Safety-enhanced design.* User-centered design processes must be applied to each capability technology includes that is specified in the following certification criteria: paragraphs (a)(1) through (5), (9) until the criterion's expiration date, and (14), and (b)(2), (3), and (11) of this section.

* * * * *

(6) * * *

(i) * * *

(A) The data classes expressed in the standards in § 170.213 in accordance with § 170.205(a)(4) and (a)(5) and paragraphs (g)(6)(i)(C)(*1*) through (*4*) of this section for the time period up to and including December 31, 2025; or

(B) The data classes expressed in the standards in § 170.213, and in accordance with § 170.205(a)(4) and (6) and paragraphs (g)(6)(i)(C)(*1*) through (*3*) of this section.

* * * * *

(9) * * *

(i) * * *

(A) * * *

(*1*) Respond to requests for patient data (based on an ID or other token) for all of the data classes expressed in the

standards in § 170.213 at one time and return such data (according to the specified standards, where applicable) in a summary record formatted in accordance with § 170.205(a)(4) and (5) following the CCD document template, and as specified in paragraphs (g)(9)(i)(A)(*3*)(*i*) through (*iv*) of this section for the time period up to and including December 31, 2025; or

(*2*) Respond to requests for patient data (based on an ID or other token) for all of the data classes expressed in the standards in § 170.213 at one time and return such data (according to the specified standards, where applicable) in a summary record formatted in accordance with § 170.205(a)(4) and (6) following the CCD document template, and as specified in paragraphs (g)(9)(i)(A)(*3*)(*i*) through (*iv*) of this section.

* * * * *

(10) * * *

(i) * * *

(A) Respond to requests for a single patient's data according to the standards and implementation specifications adopted in 170.215(a) and in § 170.215(b)(1), including the mandatory capabilities described in ''US Core Server CapabilityStatement,'' for each of the data included in the standards adopted in § 170.213. All data elements indicated as ''mandatory'' and ''must support'' by the standards and implementation specifications must be supported.

(B) Respond to requests for multiple patients' data as a group according to the standards and implementation specifications adopted in § 170.215(a), (b)(1), and (d), for each of the data included in the standards adopted in § 170.213. All data elements indicated as ''mandatory'' and ''must support'' by the standards and implementation specifications must be supported.

(ii) * * *

(A) Respond to search requests for a single patient's data consistent with the search criteria included in the implementation specifications adopted in § 170.215(b)(1), specifically the mandatory capabilities described in ''US Core Server CapabilityStatement.''

(B) Respond to search requests for multiple patients' data consistent with the search criteria included in the implementation specification adopted in § 170.215(d).

* * * * *

(iv) * * *

(A) Establish a secure and trusted connection with an application that requests data for patient and user scopes in accordance with the implementation specifications adopted in § 170.215(b)(1) and (c).

(B) Establish a secure and trusted connection with an application that requests data for system scopes in accordance with the implementation specification adopted in § 170.215(d).

* * * * *

(v) * * *

(A) * * *

(*1*) * * *

(*i*) Authentication and authorization must occur during the process of granting access to patient data in accordance with the implementation specification adopted in § 170.215(c) and standard adopted in § 170.215(e).

(*ii*) A Health IT Module's authorization server must issue a refresh token valid for a period of no less than three months to applications using the ''confidential app'' profile according to an implementation specification adopted in § 170.215(c).

* * * * *

(B) *Authentication and authorization for system scopes.* Authentication and authorization must occur during the process of granting an application access to patient data in accordance with the ''SMART Backend Services: Authorization Guide'' section of the implementation specification adopted in § 170.215(d) and the application must be issued a valid access token.

(*2*) * * *

(*i*) Access must be granted to patient data in accordance with the implementation specification adopted in § 170.215(c) without requiring re-authorization and re-authentication when a valid refresh token is supplied by the application.

(*ii*) A Health IT Module's authorization server must issue a refresh token valid for a new period of no less than three months to applications using the ''confidential app'' profile according to an implementation specification adopted in § 170.215(c).

* * * * *

(vi) *Patient authorization revocation.* A Health IT Module's authorization server must be able to revoke and must revoke an authorized application's access at a patient's direction within 1 hour of the request.

(vii) *Token introspection.* A Health IT Module's authorization server must be able to receive and validate tokens it has issued in accordance with an implementation specification in § 170.215(c).

* * * * *

■ 10. Amend § 170.402 by adding paragraphs (a)(5), and (b)(3) and (4) to read as follows:

§ 170.402 Assurances.

(a) * * *

(5) A health IT developer must not inhibit its customer's timely access to interoperable health IT certified under the Program.

(b) * * *

(3)(i) *Update.* A health IT developer must update a Health IT Module, once certified to a certification criterion adopted in § 170.315, to all applicable revised certification criteria, including the most recently adopted capabilities and standards included in the revised certification criterion.

(ii) *Provide.* A health IT developer must provide all Health IT Modules certified to a revised certification criterion, including the most recently adopted capabilities and standards included in the revised certification criterion, to its customers of such certified health IT.

(iii) *Timeliness.* A health IT developer must complete the actions specified in paragraphs (b)(3)(i) and (ii) of this section:

(A) Consistent with the timeframes specified in part 170; or

(B) If the developer obtains new customers of health IT certified to the revised criterion after the effective date of the final rule adopting the revised criterion or criteria, then the health IT developer must provide the health IT certified to the revised criterion to such customers within whichever of the following timeframes that expires last:

(*1*) The timeframe provided in paragraph (b)(3)(iii)(A) of this section; or

(*2*) No later than 12 months after the purchasing or licensing relationship has been established between the health IT developer and the new customer for the health IT certified to the revised criterion.

(4) For developers of Health IT Modules certified to § 170.315(b)(11), starting January 1, 2025, and on an ongoing basis thereafter, review and update as necessary source attribute information in § 170.315(b)(11)(iv)(A) and (B), intervention risk management practices described in § 170.315(b)(11)(vi), and summary information provided through § 170.523(f)(1)(xxi).

■ 11. Amend § 170.404 by revising paragraph (b)(2) to read as follows:

§ 170.404 Application programming interfaces.

* * * * *

(b) * * *

(2) *Service base URL publication.* For all Health IT Modules certified to § 170.315(g)(10), a Certified API Developer must publish, at no charge, the service base URLs and related organization details that can be used by patients to access their electronic health

information, by December 31, 2024. This includes all customers regardless of whether the Health IT Modules certified to § 170.315(g)(10) are centrally managed by the Certified API Developer or locally deployed by an API Information Source. These service base URLs and organization details must conform to the following:

(i) Service base URLs must be publicly published in Endpoint resource format according to the standard adopted in § 170.215(a).

(ii) Organization details for each service base URL must be publicly published in Organization resource format according to the standard adopted in § 170.215(a). Each Organization resource must contain:

(A) A reference, in the Organization.endpoint element, to the Endpoint resources containing service base URLs managed by this organization.

(B) The organization's name, location, and facility identifier.

(iii) Endpoint and Organization resources must be:

(A) Collected into a Bundle resource formatted according to the standard adopted in § 170.215(a) for publication; and

(B) Reviewed quarterly and, as necessary, updated.

* * * * *

■ 12. Amend § 170.405 by:

■ a. Revising paragraphs (a) and (b)(2)(ii); and

■ b. Removing and reserving paragraphs (b)(3) through (7) and (b)(10).

The revisions read as follows:

§ 170.405 Real world testing.

(a) *Condition of Certification requirement.* A health IT developer with one or more Health IT Module(s) certified to any one or more of the ONC Certification Criteria for Health IT in § 170.315(b), (c)(1) through (3), (e)(1), (f), (g)(7) through (10), and (h) must successfully test the real world use of those Health IT Module(s) for interoperability (as defined in 42 U.S.C. 300jj(9) and § 170.102) in the type of setting in which such Health IT Module(s) would be/is marketed.

(b) * * *

(2) * * *

(ii) For real world testing activities conducted during the immediately preceding calendar year, a health IT developer must submit to its ONC–ACB an annual real world testing results report addressing each of its certified Health IT Modules that include certification criteria referenced in paragraph (a) of this section by a date determined by the ONC–ACB that enables the ONC–ACB to publish a publicly available hyperlink to the results report on CHPL no later than March 15 of each calendar year, beginning in 2023. For certified Health IT Modules included in paragraph (a) of this section that are updated using Inherited Certified Status after August 31 of the year in which the plan is submitted, a health IT developer must include the newer version of the certified Health IT Module(s) in its annual real world testing results report. The real world testing results must report the following for each of the certification criteria identified in paragraph (a) of this section that are included in the Health IT Module's scope of certification:

* * * * *

■ 13. Add § 170.407 to read as follows:

§ 170.407 Insights Condition and Maintenance of Certification.

(a) *Condition of Certification.* (1) *Measure responses.* A health IT developer must submit (to the independent entity designated by the Secretary) for each reporting period pursuant to paragraph (b) of this section:

(i) Responses for the measures specified in this section, which must include:

(A) Data aggregated at the product level (across versions);

(B) Documentation related to the data sources and methodology used to generate measures; and

(C) Percentage of total customers (*e.g.,* hospital sites, individual clinician users) represented in provided data; or

(ii) A response (attestation) that it does not:

(A) Meet the minimum reporting qualifications requirement in paragraph (a)(2) of this section; or

(B) Have health IT certified to the certification criteria specified in each measure in paragraphs (a)(3)(i) through (vii) of this section; or

(C) Have any users using the certified health IT specified in each measure in paragraphs (a)(3)(i) through (vii) of this section during the reporting period.

(2) *Minimum reporting qualifications requirement.* At least 50 hospital sites or 500 individual clinician users across the developer's certified health IT.

(3) *Measures.* (i) *Individuals' access to electronic health information through certified health IT.* If a health IT developer has a Health IT Module certified to § 170.315(e)(1) or (g)(10) or both, then the health IT developer must submit responses for the number of unique individuals who access electronic health information (EHI) overall and by different methods of access through certified health IT.

(ii) *Consolidated clinical document architecture (C–CDA) problems, medications, and allergies reconciliation and incorporation through certified health IT.* If a health IT developer has a Health IT Module certified to § 170.315(b)(2), then the health IT developer must submit responses for:

(A) Encounters;

(B) Unique patients with an encounter;

(C) C–CDA documents obtained (unique and overall); and

(D) C–CDA documents reconciled and incorporated both through manual and automated processes.

(iii) *Applications supported through certified health IT.* If a health IT developer has a Health IT Module certified to § 170.315(g)(10), then the health IT developer must submit responses on how their certified health IT is supporting the application ecosystem, by providing the following information for applications that are connected to their certified health IT including:

(A) Application Name(s);

(B) Application Developer Name(s);

(C) Intended Purpose(s) of Application;

(D) Intended Application User(s); and

(E) Application Status.

(iv) *Use of FHIR in apps through certified health IT.* (i) If a health IT developer has a Health IT Module certified to § 170.315(g)(10), then the health IT developer must submit responses on the number of requests made to distinct certified health IT deployments that returned FHIR resources, number of distinct of certified health IT deployments active at any time, the number of distinct deployments active at any time that returned FHIR resources in response to API calls from apps connected to certified health IT, including stratifying responses by the following:

(A) User type;

(B) FHIR resource; and

(C) US Core Implementation Guide version.

(v) *Use of FHIR bulk data access through certified health IT.* (i) If a health IT developer has a Health IT Module certified to § 170.315(g)(10), then the health IT developer must submit responses for the total number of FHIR bulk data access requests completed through the certified health IT, and the number of distinct deployments of the certified health IT active at any time overall, and by whether at least one bulk data download request was completed.

(vi) *Immunization administrations electronically submitted to immunization information systems*

through certified health IT. (i) If a health IT developer has a Health IT Module certified to § 170.315(f)(1), then the health IT developer must submit responses for the use of certified health IT to electronically send immunizations administered to immunization information systems (IIS), including stratifying responses based on the following subgroups:

(A) IIS; and

(B) Age group.

(vii) *Immunization history and forecasts through certified health IT.* (i) If a health IT developer has a Health IT Module certified to § 170.315(f)(1), then the health IT developer must submit responses for the use of certified health IT to query immunization history and forecast information from immunization information systems (IIS), including stratifying responses based on the following subgroup:

(A) IIS.

(B) [Reserved]

(b) *Maintenance of Certification.* (1) A health IT developer must provide responses to the Insights Condition of Certification specified in paragraph (a) of this section annually for any Health IT Module that has or has had an active certification at any time under the ONC Health IT Certification Program during the prior six months:

(i) A health IT developer must provide responses for measures specified in:

(A) Paragraphs (a)(3)(i), (iii), (iv)(A) and (B), and (vi) of this section beginning July 2027;

(B) Paragraphs (a)(3)(ii)(A) through (C), (iv)(C), (v), (vi)(A) and (B), and (vii) of this section beginning July 2028; and

(C) Paragraph (a)(3)(ii)(D), (vii)(A) of this section beginning July 2029.

(2) [Reserved]

■ 14. Amend § 170.523 by:

■ a. Revising paragraph (f)(1) introductory text and adding paragraph (f)(1)(xxi);

■ b. Revising paragraphs (g)(1), (k)(1)(i) and (ii); and

■ c. Adding paragraph (u).

The revisions and addition read as follows:

§ 170.523 Principles of proper conduct for ONC–ACBs.

* * * * *

(f) * * *

(1) For the ONC Certification Criteria for Health IT:

* * * * *

(xxi) Where applicable, summary information of the intervention risk management practices listed in § 170.315(b)(11)(vi) is submitted by the health IT developer via publicly accessible hyperlink that allows any person to access the summary information directly without any preconditions or additional steps.

* * * * *

(g) * * *

(1) Retain all records related to the certification of Health IT Modules to the ONC Certification Criteria for Health IT beginning with the codification of those certification criteria in the Code of Federal Regulations through a minimum of 3 years after the end of calendar year that included the effective date of the removal of those certification criteria from the Code of Federal Regulations; and

* * * * *

(k) * * *

(1) * * *

(i) The disclaimer ''This Health IT Module is compliant with the ONC Certification Criteria for Health IT and has been certified by an ONC–ACB in accordance with the applicable certification criteria adopted by the Secretary of Health and Human Services. This certification does not represent an endorsement by the U.S. Department of Health and Human Services.''

(ii) For a Health IT Module certified to the ONC Certification Criteria for Health IT, the information specified by paragraphs (f)(1)(i), (vi) through (viii), (xv), and (xvi) of this section as applicable for the specific Health IT Module.

* * * * *

(u) *Insights.* Confirm that developers of certified health IT submit responses for Insights Conditions and Maintenance of Certification requirements in accordance with § 170.407.

■ 15. Amend § 170.524 by revising paragraph (f)(1) to read as follows:

§ 170.524 Principles of proper conduct for ONC–ATLs.

* * * * *

(f) * * *

(1) Retain all records related to the testing of Health IT Modules to the ONC Certification Criteria for Health IT beginning with the codification of those certification criteria in the Code of Federal Regulations through a minimum of three years after the end of calendar year that included the effective date of the removal of those certification criteria from the Code of Federal Regulations; and

* * * * *

■ 16. Amend § 170.550 by revising paragraphs (g) introductory text and (m) introductory text to read as follows:

§ 170.550 Health IT Module certification.

* * * * *

(g) *Health IT Module dependent criteria.* When certifying a Health IT Module to the ONC Certification Criteria for Health IT, an ONC–ACB must certify the Health IT Module in accordance with the certification criteria at:

* * * * *

(m) *Time-limited certification and certification status for certain ONC Certification Criteria for Health IT.* An ONC–ACB may only issue a certification to a Health IT Module and permit continued certified status for:

* * * * *

PART 171—INFORMATION BLOCKING

■ 17. The authority citation for part 171 continues to read as follows:

Authority: 42 U.S.C. 300jj–52; 5 U.S.C. 552.

■ 18. Amend § 171.102 by

■ a. Adding, in alphabetical order, the definition of ''Business associate'';

■ b. Revising the definition of ''Health IT developer of certified health IT''; and

■ c. Adding, in alphabetical order, the definition of ''Offer health information technology or offer health IT''.

The additions and revision read as follows:

§ 171.102 Definitions

* * * * *

Business associate is defined as it is in 45 CFR 160.103.

* * * * *

Health IT developer of certified health IT means an individual or entity, other than a health care provider that self-develops health IT that is not offered to others, that develops or offers health information technology (as that term is defined in 42 U.S.C. 300jj(5)), and which has, at the time it engages in a practice that is the subject of an information blocking claim, one or more Health IT Modules certified under a program for the voluntary certification of health information technology that is kept or recognized by the National Coordinator pursuant to 42 U.S.C. 300jj–11(c)(5) (ONC Health IT Certification Program).

* * * * *

Offer health information technology or *offer health IT* means to hold out for sale, resale, license, or relicense or to sell, resell, license, relicense, or otherwise provide or supply health information technology (as that term is defined in 42 U.S.C. 300jj(5) and where such health information technology includes one or more Health IT Modules certified under the ONC Health IT Certification Program) for deployment by or for other individual(s) or entity(ies) under any arrangement

except an arrangement consistent with subparagraph (3)(iii), below. Activities and arrangements described in subparagraphs (1) through (3) are considered to be excluded from what it means to offer health IT.

(1) Donation and subsidized supply arrangements are not considered offerings when an individual or entity donates, gives, or otherwise makes available funding to subsidize or fully cover the costs of a health care provider's acquisition, augmentation, or upkeep of health IT, provided such individual or entity offers and makes such subsidy without condition(s) limiting the interoperability or use of the technology to access, exchange or use electronic health information for any lawful purpose.

(2) Implementation and use activities conducted by an individual or entity as follows:

(i) Issuing user accounts or login credentials to the individual's or entity's employees in the course of their employment or contractors within the scope of their contract in order for such employees or contractors to: use, operate, implement, configure, test, maintain, update or upgrade, or to give or receive training on, the individual's or entity's health IT system(s) or specific application(s) within such system(s).

(ii) Implementing, operating, or otherwise making available production instances of application programming interface (API) technology that supports access, exchange, and use of electronic health information that the individual or entity has in its possession, custody, control, or ability to query or transmit from or across a health information network or health information exchange.

(iii) Implementing, operating, and making available production instances of online portals for patients, clinicians or other health care providers, or public health entities to access, exchange, and use electronic health information that the individual or entity has in its possession, custody, control, or ability to query or transmit from or across a health information network or health information exchange.

(iv) Issuing login credentials or user accounts for the individual's or entity's production, development, or testing environments to public health authorities, or such authorities' employees or contractors, as a means of accomplishing or facilitating access, exchange, and use of electronic health information for public health purposes including but not limited to syndromic surveillance.

(v) Issuing login credentials or user accounts for independent healthcare professionals who furnish services in a healthcare facility to use the facility's electronic health record or other health IT system(s) in: furnishing, documenting, and accurately billing for care furnished in the facility; participating in clinical education or improvement activities conducted by or in the healthcare facility; or receiving training in use of the healthcare facility's health IT system(s).

(3) Consulting and legal services arrangements as follows:

(i) Legal services furnished by outside counsel—when furnishing legal services to a client in any matter or matters pertaining to the client's seeking, assessing, selecting, or resolving disputes over contracts or other arrangements by which the client obtains use of certified health IT. Outside counsel also does not offer health IT when facilitating limited access or use of a client's health IT by independent expert witnesses engaged by the outside counsel, opposing parties' counsel and experts, and special masters and court personnel, as appropriate to legal discovery.

(ii) Health IT consultant assistance with selection, implementation, and use of health IT —furnished to a health IT customer or user to help the customer do (or to do on behalf of a customer) any or all of the following with respect to any health IT product that the consultant does not sell or resell, license or relicense, or otherwise supply to the customer under any arrangement on a commercial basis or otherwise:

(A) Define the business needs of the customer or user or evaluate health IT product(s) against such business needs, or both;

(B) Negotiate for the purchase, lease, license, or other arrangement under which the health IT product(s) will be used; or

(C) Oversee or carry out configuration, implementation, or operation of health IT product(s).

(iii) Comprehensive and predominantly non-health IT administrative or operations management services—when an individual or entity furnishes a health care provider with administrative or operational management consultant services and the consultant acts as the agent of the provider or otherwise acts on behalf of the provider in dealings with one or more health IT developer(s) or vendor(s), or managing the day-to-day operations and administrative duties for the health IT, or both. To be consistent with this subparagraph, such services must be furnished as part of a comprehensive array of predominantly non-health IT administrative and operational functions that would otherwise be executed by the health care provider.

* * * * *

■ 19. Revise § 171.103 to read as follows:

§ 171.103 Information blocking.

(a) Information blocking means a practice that except as required by law or covered by an exception set forth in subparts B, C, or D of this part, is likely to interfere with access, exchange, or use of electronic health information; and

(b) If conducted by:

(1) A health IT developer of certified health IT, health information network or health information exchange, such developer, network or exchange knows, or should know, that such practice is likely to interfere with access, exchange, or use of electronic health information; or

(2) A health care provider, such provider knows that such practice is unreasonable and is likely to interfere with access, exchange, or use of electronic health information.

■ 20. Amend § 171.204 by revising paragraphs (a)(1) and (3) and adding paragraphs (a)(4) and (5) to read as follows:

§ 171.204 Infeasibility exception—When will an actor's practice of not fulfilling a request to access, exchange, or use electronic health information due to the infeasibility of the request not be considered information blocking?

* * * * *

(a) * * *

(1) *Uncontrollable events.* The actor cannot fulfill the request for access, exchange, or use of electronic health information because of a natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority that in fact negatively impacts the actor's ability to fulfill the request.

* * * * *

(3) *Third party seeking modification use.* The request is to enable use of EHI in order to modify EHI provided that the request for such use is not from a health care provider requesting such use from an actor that is its business associate.

(4) *Manner exception exhausted.* The actor is unable to fulfill a request for access, exchange, or use of electronic health information because paragraphs (a)(4)(i), (ii), and (iii) of this section are all true; and the actor complied with paragraph (a)(4)(iv) of this section.

(i) The actor could not reach agreement with a requestor in accordance with § 171.301(a) or was technically unable to fulfill a request for electronic health information in the manner requested.

(ii) The actor offered at least two alternative manners in accordance with § 171.301(b), one of which must use either technology certified to standard(s) adopted in part 170 (§ 171.301(b)(1)(i)) or published content and transport standards consistent with § 171.301(b)(1)(ii).

(iii) The actor does not provide the same access, exchange, or use of the requested electronic health information to a substantial number of individuals or entities that are similarly situated to the requester.

(iv) In determining whether a requestor is similarly situated under paragraph (a)(4)(iii), an actor shall not discriminate based on:

(A) Whether the requestor is an individual as defined in § 171.202(a)(2)

(B) The health care provider type and size; and

(C) Whether the requestor is a competitor of the actor or whether providing such access, exchange, or use, would facilitate competition with the actor.

(5) *Infeasible under the circumstances.* (i) The actor demonstrates, prior to responding to the request pursuant to paragraph (b) of this section, through a contemporaneous written record or other documentation, its consistent and non-discriminatory consideration of the following factors that led to its determination that complying with the request would be infeasible under the circumstances:

(A) The type of electronic health information and the purposes for which it may be needed;

(B) The cost to the actor of complying with the request in the manner requested;

(C) The financial and technical resources available to the actor;

(D) Whether the actor's practice is non-discriminatory and the actor provides the same access, exchange, or use of electronic health information to its companies or to its customers, suppliers, partners, and other persons with whom it has a business relationship;

(E) Whether the actor owns or has control over a predominant technology, platform, health information exchange, or health information network through which electronic health information is accessed or exchanged; and

(F) Why the actor was unable to provide access, exchange, or use of electronic health information consistent with the exception in § 171.301.

(ii) In determining whether the circumstances were infeasible under paragraph (a)(3)(i) of this section, it shall not be considered whether the manner requested would have:

(A) Facilitated competition with the actor; or

(B) Prevented the actor from charging a fee or resulted in a reduced fee.

* * * * *

■ 21. Revise § 171.301 to read as follows:

§ 171.301 Manner exception—When will an actor's practice of limiting the manner in which it fulfills a request to access, exchange, or use electronic health information not be considered information blocking?

An actor's practice of limiting the manner in which it fulfills a request to access, exchange, or use electronic health information will not be considered information blocking when the practice follows the conditions of this section.

(a) *Manner requested.* (1) An actor must fulfill a request for electronic health information in any manner requested, unless the actor is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request in the manner requested.

(2) If an actor fulfills a request for electronic health information in any manner requested:

(i) Any fees charged by the actor in relation to fulfilling the request are not required to satisfy the exception in § 171.302; and

(ii) Any license of interoperability elements granted by the actor in relation to fulfilling the request is not required to satisfy the exception in § 171.303.

(b) *Alternative manner.* If an actor does not fulfill a request for electronic health information in any manner requested because it is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request in the manner requested, the actor must fulfill the request in an alternative manner, as follows:

(1) The actor must fulfill the request without unnecessary delay in the following order of priority, starting with paragraph (b)(1)(i) of this section and only proceeding to the next consecutive paragraph if the actor is technically unable to fulfill the request in the manner identified in a paragraph.

(i) Using technology certified to standard(s) adopted in part 170 that is specified by the requestor.

(ii) Using content and transport standards specified by the requestor and published by:

(A) The Federal Government; or

(B) A standards developing organization accredited by the American National Standards Institute.

(iii) Using an alternative machine-readable format, including the means to interpret the electronic health information, agreed upon with the requestor.

(2) Any fees charged by the actor in relation to fulfilling the request are required to satisfy the exception in § 171.302.

(3) Any license of interoperability elements granted by the actor in relation to fulfilling the request is required to satisfy the exception in § 171.303.

■ 22. Add Subpart D, consisting of §§ 171.400 through 171.403 to read as follows:

Subpart D—Exceptions That Involve Practices Related to Actors' Participation in The Trusted Exchange Framework and Common Agreement (TEFCA℠)

Sec.

171.400 Availability and effect of exceptions.
171.401 [Reserved]
171.402 [Reserved]
171.403 TEFCA manner exception.

Authority: 42 U.S.C. 300jj–52; 5 U.S.C. 552.

§ 171.400 Availability and effect of exceptions.

A practice shall not be treated as information blocking if the actor satisfies an exception to the information blocking provision as set forth in this subpart D by meeting all applicable requirements and conditions of the exception at all relevant times.

§ 171.401 [Reserved].

§ 171.402 [Reserved].

§ 171.403 —TEFCA manner exception—When will an actor's practice of limiting the manner in which it fulfills a request to access, exchange, or use electronic health information to only via TEFCA not be considered information blocking?

An actor's practice of limiting the manner in which it fulfills a request for access, exchange, or use of electronic health information to only via TEFCA will not be considered information blocking when the practice follows the conditions specified in paragraphs (a) through (d) of this section.

(a) *Mutually part of TEFCA.* The actor and requestor are both part of TEFCA.

(b) *Requestor capability.* The requestor is capable of such access,

exchange, or use of the requested electronic health information from the actor via TEFCA.

(c) *Limitation.* The request for access, exchange, or use of EHI is not via the standards adopted in 45 CFR 170.215, including version(s) of those standards approved pursuant to 45 CFR 170.405(b)(8).

(d) *Fees and licensing.* (1) Any fees charged by the actor in relation to fulfilling the request are required to satisfy the exception in § 171.302; and

(2) Any license of interoperability elements granted by the actor in relation to fulfilling the request is required to satisfy the exception in § 171.303.

Xavier Becerra,

Secretary, Department of Health and Human Services.

[FR Doc. 2023–28857 Filed 1–2–24; 4:15 pm]

BILLING CODE 4150–45–P