SUBCHAPTER D—HEALTH INFORMATION TECHNOLOGY

PART 170—HEALTH INFORMATION TECHNOLOGY STANDARDS, IMPLEMENTATION SPECIFICATIONS, AND CERTIFICATION CRITERIA AND CERTIFICATION PROGRAMS FOR HEALTH INFORMATION TECHNOLOGY

Subpart A—General Provisions

Subpart B—Standards and Implementation Specifications for Health Information Technology

Subpart C—Certification Criteria for Health Information Technology

Subpart D—Conditions and Maintenance of Certification Requirements for Health IT Developers

Subpart E—ONC Health IT Certification Program

AUTHORITY: 42 U.S.C. 300jj–11; 42 U.S.C 300jj–14; 5 U.S.C. 552.

SOURCE: 75 FR 2042, Jan. 13, 2010, unless otherwise noted.

Subpart A—General Provisions

§ 170.100 Statutory basis and purpose.

The provisions of this subchapter implement sections 3001(c)(5) and 3004 of the Public Health Service Act.

[75 FR 36203, June 24, 2010]

§ 170.101 Applicability.

The standards, implementation specifications, and certification criteria

adopted in this part apply to health information technology and the testing and certification of Health IT Modules.

[85 FR 70082, Nov. 4, 2020]

§ 170.102 Definitions.

For the purposes of this part:

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.

Certification criteria means criteria:

(1) To establish that health information technology meets applicable standards and implementation specifications adopted by the Secretary; or

(2) That are used to test and certify that health information technology includes required capabilities.

Common Clinical Data Set means the following data expressed, where indicated, according to the specified standard(s):

(1) Patient name.

(2) *Sex:* The standard specified in §170.207(n)(1).

(3) Date of birth.

(4) *Race:*

(i) The standard specified in §170.207(f)(2); and

(ii) The standard specified in §170.207(f)(1) for each race identified in accordance §170.207(f)(2).

(5) *Ethnicity:*

(i) The standard specified in §170.207(f)(2); and

(ii) The standard specified in §170.207(f)(1) for each ethnicity identified in accordance §170.207(f)(2).

(6) *Preferred language:* The standard specified in §170.207(g)(2).

(7) Smoking status.

(8) *Problems:* At a minimum, the standard specified in §170.207(a)(4).

(9) *Medications:* At a minimum, the standard specified in §170.207(d)(3).

(10) *Medication allergies:* At a minimum, the standard specified in §170.207(d)(3).

(11) *Laboratory test(s):* At a minimum, the standard specified in §170.207(c)(3).

(12) Laboratory value(s)/result(s).

(13) *Vital signs:*

(i) The patient's diastolic blood pressure, systolic blood pressure, body height, body weight, heart rate, respiratory rate, body temperature, pulse oximetry, and inhaled oxygen concentration must be exchanged in numerical values only; and

(ii) In accordance with the standard specified in §170.207(c)(3) and with the associated applicable unit of measure for the vital sign measurement in the standard specified in §170.207(m)(1).

(iii) *Optional:* The patient's BMI percentile per age and sex for youth 2–20 years of age, weight for age per length and sex for children less than 3 years of age, and head occipital-frontal circumference for children less than 3 years of age must be recorded in numerical values only in accordance with the standard specified in §170.207(c)(3) and with the associated applicable unit of measure for the vital sign measurement in the standard specified in §170.207(m)(1). For BMI percentile per age and sex for youth 2–20 years of age and weight for age per length and sex for children less than 3 years of age, the reference range/scale or growth curve should be included as appropriate.

(14) *Procedures:*

(i) At a minimum, the version of the standard specified in §170.207(a)(4) or §170.207(b)(2); or

(ii) For technology primarily developed to record dental procedures, the standard specified in §170.207(b)(3).

(iii) *Optional:* The standard specified in §170.207(b)(4).

(15) Care team member(s).

(16) *Immunizations:* In accordance with, at a minimum, the standards specified in § 170.207(e)(3) and (4).

(17) Unique device identifier(s) for a patient's implantable device(s): In accordance with the ''Product Instance'' in the ''Procedure Activity Procedure Section'' of the standard specified in § 170.205(a)(4).

(18) *Assessment and plan of treatment:*

(i) In accordance with the ''Assessment and Plan Section (V2)'' of the standard specified in § 170.205(a)(4); or

(ii) In accordance with the ''Assessment Section (V2)'' and ''Plan of Treatment Section (V2)'' of the standard specified in § 170.205(a)(4).

(19) *Goals:* In accordance with the ''Goals Section'' of the standard specified in § 170.205(a)(4).

(20) *Health concerns:* In accordance with the ''Health Concerns Section'' of the standard specified in § 170.205(a)(4).

Day or Days means a calendar day or calendar days.

Device identifier is defined as it is in 21 CFR 801.3.

Disclosure is defined as it is in 45 CFR 160.103.

Electronic health information (EHI) is defined as it is in § 171.102.

Fee is defined as it is in § 171.102 of this subchapter.

Global Unique Device Identification Database (GUDID) is defined as it is in 21 CFR 801.3.

Health information technology means hardware, software, integrated technologies or related licenses, IP, upgrades, or packaged solutions sold as services that are designed for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information.

Health IT Module means any service, component, or combination thereof that can meet the requirements of at least one certification criterion adopted by the Secretary.

Human readable format means a format that enables a human to read and easily comprehend the information presented to him or her regardless of the method of presentation.

Implantable device is defined as it is in 21 CFR 801.3.

Implementation specification means specific requirements or instructions for implementing a standard.

Interoperability is, with respect to health information technology, such health information technology that—

(1) 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;

(2) Allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law; and

(3) Does not constitute information blocking as defined in § 171.103 of this subchapter.

Interoperability element is defined as it is in § 171.102 of this subchapter.

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.

Production identifier is defined as it is in 21 CFR 801.3.

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.

Qualified 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; and

(2) Has the capacity:

(i) To provide clinical decision support;

(ii) To support physician order entry;

(iii) To capture and query information relevant to health care quality; and

(iv) To exchange electronic health information with, and integrate such information from other sources.

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.

Standard means a technical, functional, or performance-based rule, condition, requirement, or specification that stipulates instructions, fields, codes, data, materials, characteristics, or actions.

Unique device identifier is defined as it is in 21 CFR 801.3.

[75 FR 2042, Jan. 13, 2010, as amended at 75 FR 36203, June 24, 2010; 75 FR 44649, July 28, 2010; 77 FR 54283, Sept. 4, 2012; 78 FR 65887, Nov. 4, 2013; 79 FR 52933, Sept. 4, 2014; 79 FR 54477, 54478, Sept. 11, 2014; 80 FR 62741, Oct. 16, 2015; 80 FR 76871, Dec. 11, 2015; 85 FR 25939, May 1, 2020; 85 FR 70082, Nov. 4, 2020; 89 FR 1426, Jan. 9, 2024]

Subpart B—Standards and Implementation Specifications for Health Information Technology

SOURCE: 75 FR 44649, July 28, 2010, unless otherwise noted.

§ 170.200 Applicability.

The standards and implementation specifications adopted in this part apply with respect to Health Information technology.

[85 FR 70082, Nov. 4, 2020]

§ 170.202 Transport standards and other protocols.

The Secretary adopts the following transport standards:

(a) *Direct Project*. (1) [Reserved]

(2) *Standard*. ONC Applicability Statement for Secure Health Transport, Version 1.2 (incorporated by reference in § 170.299).

(b) *Standard*. ONC XDR and XDM for Direct Messaging Specification (incorporated by reference in § 170.299).

(c) *Standard*. ONC Transport and Security Specification (incorporated by reference in § 170.299).

(d) *Standard*. ONC Implementation Guide for Direct Edge Protocols (incorporated by reference in § 170.299).

(e) *Delivery notification*—(1) *Standard*. ONC Implementation Guide for Delivery Notification in Direct (incorporated by reference in § 170.299).

(2) [Reserved]

[77 FR 54284, Sept. 4, 2012, as amended at 79 FR 54478, Sept. 11, 2014; 80 FR 62743, Oct. 16, 2015; 85 FR 25940, May 1, 2020]

§ 170.204 Functional standards.

The Secretary adopts the following functional standards:

(a) *Accessibility*—(1) *Standard*. Web Content Accessibility Guidelines (WCAG) 2.0, Level A Conformance (incorporated by reference in § 170.299).

(2) *Standard*. Web Content Accessibility Guidelines (WCAG) 2.0, Level AA Conformance (incorporated by reference in § 170.299).

(b) *Reference source*. *Standard*. HL7 Version 3 Standard: Context-Aware Retrieval Application (Infobutton) (incorporated by reference in § 170.299).

(1)–(2) [Reserved]

(3) *Standard*. HL7 Version 3 Standard: Context Aware Knowledge Retrieval Application. (''Infobutton''), Knowledge Request, Release 2 (incorporated by reference in § 170.299). *Implementation specifications*. HL7 Implementation Guide: Service-Oriented Architecture Implementations of the Context-aware Knowledge Retrieval (Infobutton) Domain, Release 1 (incorporated by reference in § 170.299).

(4) *Standard*. HL7 Version 3 Standard: Context Aware Knowledge Retrieval Application (''Infobutton''), Knowledge Request, Release 2 (incorporated by reference in § 170.299). *Implementation specifications*. HL7 Version 3 Implementation Guide: Context-Aware Knowledge Retrieval (Infobutton), Release 4 (incorporated by reference in § 170.299).

[77 FR 54284, Sept. 4, 2012, as amended at 80 FR 62743, Oct. 16, 2015; 85 FR 25940, May 1, 2020]

§ 170.205 Content exchange standards and implementation specifications for exchanging electronic health information.

The Secretary adopts the following content exchange standards and associated implementation specifications:

(a) *Patient summary record.* (1) [Reserved]

(2) [Reserved]

(3) *Standard.* HL7 Implementation Guide for CDA® Release 2: IHE Health Story Consolidation, (incorporated by reference in § 170.299). The use of the ''unstructured document'' document-level template is prohibited.

(4) *Standard.* HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use, Volume 1—Introductory Material, Release 2.1 and HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use, Volume 2—Templates and Supporting Material, Release 2.1 (incorporated by reference in § 170.299).

(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).

(b) *Electronic prescribing*—(1) *Standard.* National Council for Prescription Drug Programs (NCPDP): SCRIPT Standard Implementation Guide; Version 2017071 (incorporated by reference in § 170.299). The Secretary's adoption of this standard expires on January 1, 2028.

(2) *Standard.* NCPDP SCRIPT Standard, Implementation Guide, Version 2023011 (incorporated by reference in § 170.299).

(c) *Real-time prescription benefit*—(1) *Standard.* NCPDP Real-Time Prescription Benefit Standard, Implementation Guide, Version 13 (incorporated by reference in § 170.299).

(2) [Reserved]

(d) *Electronic submission to public health agencies for surveillance or reporting.* (1) [Reserved]

(2) *Standard.* HL7 2.5.1 (incorporated by reference in § 170.299).

(3) [Reserved]

(4) *Standard.* HL7 2.5.1 (incorporated by reference in § 170.299). *Implementation specifications.* PHIN Messaging Guide for Syndromic Surveillance: Emergency Department, Urgent Care, Inpatient and Ambulatory Care Settings, Release 2.0, April 21, 2015 (incorporated by reference in § 170.299) and Erratum to the CDC PHIN 2.0 Implementation Guide, August 2015; Erratum to the CDC PHIN 2.0 Messaging Guide, April 2015 Release for Syndromic Surveillance: Emergency Department, Urgent Care, Inpatient and Ambulatory Care Settings (incorporated by reference in § 170.299).

(e) *Electronic submission to immunization registries.* (1) [Reserved]

(2)–(3) [Reserved]

(4) *Standard.* HL7 2.5.1 (incorporated by reference in § 170.299). *Implementation specifications.* HL7 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5 (incorporated by reference in § 170.299) and HL7 Version 2.5.1 Implementation Guide for Immunization Messaging (Release 1.5)—Addendum, July 2015 (incorporated by reference in § 170.299).

(f) [Reserved]

(g) *Electronic transmission of lab results to public health agencies. Standard.* HL7 2.5.1 (incorporated by reference in § 170.299). *Implementation specifications.* HL7 Version 2.5.1 Implementation Guide: Electronic Laboratory Reporting to Public Health, Release 1 (US Realm) (incorporated by reference in § 170.299) with Errata and Clarifications, (incorporated by reference in § 170.299) and ELR 2.5.1 Clarification Document for EHR Technology Certification, (incorporated by reference in § 170.299).

(h) *Clinical quality measure data import, export and reporting.* (1) [Reserved]

(2) *Standard.* HL7 CDA® R2 Implementation Guide: Quality Reporting Document Architecture—Category I (QRDA I); Release 1, DSTU Release 3 (US Realm), Volume 1—Introductory Material and HL7 CDA® R2 Implementation Guide: Quality Reporting Document Architecture—Category I (QRDA I); Release 1, DSTU Release 3 (US Realm), Volume 2—Templates and Supporting

Material (incorporated by reference in §170.299).

(3) *Standard.* CMS Implementation Guide for Quality Reporting Document Architecture: Category I; Hospital Quality Reporting; Implementation Guide for 2020 (incorporated by reference in §170.299).

(i) *Cancer information.* (1) [Reserved]

(2) *Standard.* HL7 Clinical Document Architecture (CDA), Release 2.0, Normative Edition (incorporated by reference in §170.299). *Implementation specifications.* HL7 CDA© Release 2 Implementation Guide: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1; DSTU Release 1.1, Volume 1—Introductory Material and HL7 CDA© Release 2 Implementation Guide: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1; DSTU Release 1.1 (US Realm), Volume 2—Templates and Supporting Material (incorporated by reference in §170.299).

(j) [Reserved]

(k) *Clinical quality measure aggregate reporting*—(1) *Standard.* Quality Reporting Document Architecture Category III, Implementation Guide for CDA Release 2 (incorporated by reference in §170.299).

(2) *Standard.* Errata to the HL7 Implementation Guide for CDA® Release 2: Quality Reporting Document Architecture—Category III, DSTU Release 1 (US Realm), September 2014 (incorporated by reference in §170.299).

(3) *Standard.* CMS Implementation Guide for Quality Reporting Document Architecture: Category III; Eligible Clinicians and Eligible Professionals Programs; Implementation Guide for 2020 (incorporated by reference in §170.299).

(l)–(n) [Reserved]

(o) *Data segmentation for privacy*—(1) *Standard.* HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1 (incorporated by reference in §170.299).

(2) [Reserved]

(p) *XDM package processing*—(1) *Standard.* IHE IT Infrastructure Technical Framework Volume 2b (ITI TF–2b) (incorporated by reference in §170.299).

(2) [Reserved]

(q) [Reserved]

(r) *Public health—antimicrobial use and resistance information*—(1) *Standard.* The following sections of HL7 Implementation Guide for CDA® Release 2—Level 3: Healthcare Associated Infection Reports, Release 1, U.S. Realm (incorporated by reference in §170.299). Technology is only required to conform to the following sections of the implementation guide:

(i) HAI Antimicrobial Use and Resistance (AUR) Antimicrobial Resistance Option (ARO) Report (Numerator) specific document template in Section 2.1.2.1 (pages 69–72);

(ii) Antimicrobial Resistance Option (ARO) Summary Report (Denominator) specific document template in Section 2.1.1.1 (pages 54–56); and

(iii) Antimicrobial Use (AUP) Summary Report (Numerator and Denominator) specific document template in Section 2.1.1.2 (pages 56–58).

(2) [Reserved]

(s) *Public health—health care survey information*—(1) *Standard.* HL7 Implementation Guide for CDA® Release 2: National Health Care Surveys (NHCS), Release 1—US Realm, HL7 Draft Standard for Trial Use, Volume 1—Introductory Material and HL7 Implementation Guide for CDA® Release 2: National Health Care Surveys (NHCS), Release 1—US Realm, HL7 Draft Standard for Trial Use, Volume 2—Templates and Supporting Material (incorporated by reference in §170.299).

(2) [Reserved]

(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).

(u) *Formulary and benefit*—(1) *Standard.* NCPDP Formulary and Benefit Standard Version 60 (incorporated by reference in § 170.299).

(2) [Reserved]

[75 FR 44649, July 28, 2010, as amended at 75 FR 62690, Oct. 13, 2010; 77 FR 54284, Sept. 4, 2012; 79 FR 54478, Sept. 11, 2014; 80 FR 62743, Oct. 16, 2015; 85 FR 25940, May 1, 2020; 85 FR 70082, Nov. 4, 2020; 89 FR 1426, Jan. 9, 2024; 89 FR 51265, June 17, 2024]

§ 170.207 Vocabulary standards for representing electronic health information.

The Secretary adopts the following code sets, terminology, and nomenclature as the vocabulary standards for the purpose of representing electronic health information:

(a) *Problems.*

(1) *Standard.* SNOMED CT®, U.S. Edition, March 2022 Release (incorporated by reference, see § 170.299).

(2)–(3) [Reserved]

(4) *Standard.* IHTSDO SNOMED CT®, U.S. Edition, September 2015 Release (incorporated by reference in § 170.299).

(b) *Procedures.* (1) [Reserved]

(2) *Standard.* The code set specified at 45 CFR 162.1002(a)(5).

(3) *Standard.* The code set specified at 45 CFR 162.1002(a)(4).

(4) *Standard.* The code set specified at 45 CFR 162.1002(c)(3) for the indicated procedures or other actions taken.

(c) *Laboratory tests.*

(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).

(2) [Reserved]

(3) *Standard.* Logical Observation Identifiers Names and Codes (LOINC®) Database version 2.52, a universal code system for identifying laboratory and clinical observations produced by the Regenstrief Institute, Inc. (incorporated by reference in § 170.299).

(d) *Medications.*

(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).

(2) [Reserved]

(3) *Standard.* RxNorm, a standardized nomenclature for clinical drugs produced by the United States National Library of Medicine, September 8, 2015 Release (incorporated by reference in § 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) *Immunizations.*

(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).

(3) *Standard.* HL7 Standard Code Set CVX—Vaccines Administered, updates through August 17, 2015 (incorporated by reference in § 170.299).

(4) *Standard.* National Drug Code Directory (NDC)—Vaccine NDC Linker, updates through August 17, 2015 (incorporated by reference in § 170.299).

(f) *Race and Ethnicity*—(1) *Standard.* The Office of Management and Budget Standards for Maintaining, Collecting, and Presenting Federal Data on Race and Ethnicity, Statistical Policy Directive No. 15, as revised, October 30, 1997 (incorporated by reference in § 170.299).

(2) *Standard.* CDC Race and Ethnicity Code Set Version 1.0 (March 2000) (incorporated by reference in § 170.299).

(3) *Standard.* CDC Race and Ethnicity Code Set Version 1.2 (July 08, 2021) (incorporated by reference, see § 170.299).

(g) *Preferred language.* (1) [Reserved]

(2) *Standard.* Request for Comments (RFC) 5646 (incorporated by reference in § 170.299).

(h) [Reserved]

(i) *Encounter diagnoses. Standard.* The code set specified at 45 CFR 162.1002(c)(2) for the indicated conditions.

(j)–(l) [Reserved]

(m) *Numerical references*—(1) *Standard.* The Unified Code of Units of Measure, Revision 1.9 (incorporated by reference in § 170.299).

(2) *Standard.* The Unified Code for Units of Measure, Version 2.1, November 21, 2017 (incorporated by reference, see § 170.299).

(n) *Sex*—(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).

(q) *Patient matching*—(1) *Phone number standard.* ITU–T E.123, Series E: Overall Network Operation, Telephone Service, Service Operation and Human Factors, International operation—General provisions concerning users: Notation for national and international telephone numbers, email addresses and web addresses (incorporated by reference in §170.299); and ITU–T E.164, Series E: Overall Network Operation, Telephone Service, Service Operation and Human Factors, International operation—Numbering plan of the international telephone service: The international public telecommunication numbering plan (incorporated by reference in §170.299).

(2) [Reserved]

(r) *Provider type*—(1) *Standard.* Crosswalk: Medicare Provider/Supplier to Healthcare Provider Taxonomy, April 2, 2015 (incorporated by reference in §170.299).

(2) *Standard.* Medicare Provider and Supplier Taxonomy Crosswalk, 2021 (incorporated by reference, see §170.299).

(s) *Patient insurance*—(1) *Standard.* Public Health Data Standards Consortium Source of Payment Typology Code Set Version 5.0 (October 2011) (incorporated by reference in §170.299).

(2) *Standard.* Public Health Data Standards Consortium Users Guide for Source of Payment Typology, Version 9.2 (incorporated by reference, see §170.299).

[75 FR 44649, July 28, 2010, as amended at 77 FR 54284, Sept. 4, 2012; 79 FR 54478, Sept. 11, 2014; 80 FR 62744, Oct. 16, 2015; 80 FR 76871, Dec. 11, 2015; 85 FR 25940, May 1, 2020; 89 FR 1426, Jan. 9, 2024]

§ 170.210 Standards for health information technology to protect electronic health information created, maintained, and exchanged.

The Secretary adopts the following standards to protect electronic health information created, maintained, and exchanged:

(a) *Encryption and decryption of electronic health information.* (1) [Reserved]

(2) *General.* Any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS)

Publication 140–2, October 8, 2014 (incorporated by reference in § 170.299).

(b) [Reserved]

(c) *Hashing of electronic health information.* (1) [Reserved]

(2) *Standard.* A hashing algorithm with a security strength equal to or greater than SHA–2 as specified by NIST in FIPS Publication 180–4 (August 2015) (incorporated by reference in § 170.299).

(d) *Record treatment, payment, and health care operations disclosures.* The date, time, patient identification, user identification, and a description of the disclosure must be recorded for disclosures for treatment, payment, and health care operations, as these terms are defined at 45 CFR 164.501.

(e) *Record actions related to electronic health information, audit log status, and encryption of end-user devices.* (1)(i) The audit log must record the information specified in sections 7.1.1 and 7.1.2 and 7.1.6 through 7.1.9 of the standard specified in § 170.210(h) and changes to user privileges when health IT is in use.

(ii) The date and time must be recorded in accordance with the standard specified at § 170.210(g).

(2)(i) The audit log must record the information specified in sections 7.1.1 and 7.1.7 of the standard specified at § 170.210(h) when the audit log status is changed.

(ii) The date and time each action occurs in accordance with the standard specified at § 170.210(g).

(3) The audit log must record the information specified in sections 7.1.1 and 7.1.7 of the standard specified at § 170.210(h) when the encryption status of electronic health information locally stored by health IT on end-user devices is changed. The date and time each action occurs in accordance with the standard specified at § 170.210(g).

(f) *Encryption and hashing of electronic health information.* Any encryption and hashing algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the FIPS Publication 140–2 (incorporated by reference in § 170.299).

(g) *Synchronized clocks.* The date and time recorded utilize a system clock that has been synchronized using any Network Time Protocol (NTP) standard.

(h) *Audit log content.* ASTM E2147–18, (incorporated by reference in § 170.299).

[75 FR 44649, July 28, 2010, as amended at 77 FR 54285, Sept. 4, 2012; 79 FR 54478, Sept. 11, 2014; 80 FR 62745, Oct. 16, 2015; 85 FR 25940, May 1, 2020; 85 FR 70082, Nov. 4, 2020; 89 FR 1428, Jan. 9, 2024]

§ 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).

[89 FR 1428, Jan. 9, 2024]

§ 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]

[89 FR 1428, Jan. 9, 2024]

§ 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.

(b) American National Standards Institute, Health Information Technology Standards Panel (HITSP) Secretariat, 25 West 43rd Street—Fourth Floor, New York, NY 10036, *http://www.hitsp.org*.

(1) HITSP Summary Documents Using HL7 Continuity of Care Document (CCD) Component, HITSP/C32, July 8, 2009, Version 2.5, IBR approved for § 170.205.

(2) [Reserved]

(c) ASTM International, 100 Barr Harbor Drive, PO Box C700, West Conshohocken, PA, 19428–2959 USA; Telephone (610) 832–9585 or *http://www.astm.org/*.

(1) ASTM E2147–18 Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems, approved May 1, 2018, IBR approved for § 170.210(h).

(2)–(3) [Reserved]

(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*

(1) HL7 Standard Code Set CVX—Vaccines Administered, July 30, 2009, IBR approved for § 170.207.

(2) [Reserved]

(3) Implementation Guide for Immunization Data Transactions using Version 2.3.1 of the Health Level Seven (HL7)Standard Protocol Implementation Guide Version 2.2, June 2006, IBR approved for § 170.205.

(4) HL7 2.5.1 Implementation Guide for Immunization Messaging Release 1.0, May 1, 2010, IBR approved for § 170.205.

(5) PHIN Messaging Guide for Syndromic Surveillance: Emergency Department and Urgent Care Data, ADT Messages A01, A03, A04, and A08,

HL7 Version 2.5.1 (Version 2.3.1 Compatible), Release 1.1, August 2012, IBR approved for §170.205.

(6) Conformance Clarification for EHR Certification of Electronic Syndromic Surveillance, ADT MESSAGES A01, A03, A04, and A08, HL7 Version 2.5.1, Addendum to PHIN Messaging Guide for Syndromic Surveillance: Emergency Department and Urgent Care Data (Release 1.1), August 2012, IBR approved for §170.205.

(7)–(8) [Reserved]

(9) ELR 2.5.1 Clarification Document for EHR Technology Certification, July 16, 2012, IBR approved for §170.205.

(10) PHIN Messaging Guide for Syndromic Surveillance: Emergency Department, Urgent Care, Inpatient and Ambulatory Care Settings, Release 2.0, April 21, 2015, IBR approved for §170.205(d).

(11) Erratum to the CDC PHIN 2.0 Implementation Guide, August 2015; Erratum to the CDC PHIN 2.0 Messaging Guide, April 2015 Release for Syndromic Surveillance: Emergency Department, Urgent Care, Inpatient and Ambulatory Care Settings, IBR approved for §170.205(d).

(12) HL7 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5, October 1, 2014, IBR approved for §170.205(e).

(13) HL7 Version 2.5.1 Implementation Guide for Immunization Messaging (Release 1.5)—Addendum, July 2015, IBR approved for §170.205(e).

(14) HL7 Standard Code Set CVX—Vaccines Administered, updates through August 17, 2015, IBR approved for §170.207(e).

(15) National Drug Code Directory (NDC)—Vaccine NDC Linker, updates through August 17, 2015, IBR approved for §170.207(e).

(16) CDC Race and Ethnicity Code Set Version 1.0 (March 2000), IBR approved for §170.207(f).

(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*.

(1) CMS PQRI 2009 Registry XML Specifications, IBR approved for §170.205.

(2) 2009 Physician Quality Reporting Initiative Measure Specifications Manual for Claims and Registry, Version 3.0, December 8, 2008 IBR approved for §170.205.

(3) Crosswalk: Medicare Provider/Supplier to Healthcare Provider Taxonomy, April 2, 2015, IBR approved for §170.207(r).

(4) CMS Implementation Guide for Quality Reporting Document Architecture: Category I; Hospital Quality Reporting Implementation Guide for 2020; published December 3, 2019, IBR approved for §170.205(h).

(5) CMS Implementation Guide for Quality Reporting Document Architecture: Category III; Eligible Clinicians and Eligible Professionals Programs Implementation Guide for 2020; published April 30, 2020, IBR approved for §170.205(k).

(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/*

(1) Health Level Seven Standard Version 2.3.1 (HL7 2.3.1), An Application Protocol for Electronic Data Exchange in Healthcare Environments, April 14, 1999, IBR approved for §170.205.

(2) Health Level Seven Messaging Standard Version 2.5.1 (HL7 2.5.1), An Application Protocol for Electronic Data Exchange in Healthcare Environments, February 21, 2007, IBR approved for §170.205.

(3) [Reserved]

(4) HL7 Version 2.5.1 Implementation Guide: Electronic Laboratory Reporting to Public Health, Release 1 (US Realm) HL7 Version 2.5.1: ORU^R01, HL7 Informative Document, February, 2010, IBR approved for § 170.205.

(5) HL7 Version 3 Standard: Context-Aware Retrieval Application (Infobutton); Release 1, July 2010, IBR approved for § 170.204.

(6)–(7) [Reserved]

(8) HL7 Implementation Guide for CDA® Release 2: IHE Health Story Consolidation, DSTU Release 1.1 (US Realm) Draft Standard for Trial Use July 2012, IBR approved for § 170.205.

(9) HL7 Clinical Document Architecture, Release 2.0, Normative Edition, May 2005, IBR approved for § 170.205.

(10)–(11) [Reserved]

(12) HL7 Implementation Guide for CDA® Release 2: Quality Reporting Document Architecture, DTSU Release 2 (Universal Realm), Draft Standard for Trial Use, July 2012, IBR approved for § 170.205.

(13) HL7 v2.5.1 IG: Electronic Laboratory Reporting to Public Health (US Realm), Release 1 Errata and Clarifications, September, 29, 2011, IBR approved for § 170.205.

(14) HL7 Implementation Guide for CDA® Release 2: Quality Reporting Document Architecture—Category III, DSTU Release 1 (US Realm) Draft Standard for Trial Use, November 2012, IBR approved for § 170.205.

(15) HL7 Version 3 Standard: Context Aware Retrieval Application (''Infobutton''), Knowledge Request, Release 2, 2014 Release, IBR approved for § 170.204(b).

(16) HL7 Implementation Guide: Service-Oriented Architecture Implementations of the Context-aware Knowledge Retrieval (Infobutton) Domain, Release 1, August 9, 2013, IBR approved for § 170.204(b).

(17) HL7 Version 3 Implementation Guide: Context-Aware Knowledge Retrieval (Infobutton), Release 4, June 13, 2014, IBR approved for § 170.204(b).

(18) HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use, Volume 1—Introductory Material, Release 2.1, August 2015, IBR approved for § 170.205(a).

(19) HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use, Volume 2—Templates and Supporting Material, Release 2.1, August 2015, IBR approved for § 170.205(a).

(20) HL7 CDA® R2 Implementation Guide: Quality Reporting Document Architecture—Category I (QRDA I); Release 1, DSTU Release 3 (US Realm), Volume 1—Introductory Material, June 2015, IBR approved for § 170.205(h).

(21) HL7 CDA® R2 Implementation Guide: Quality Reporting Document Architecture—Category I (QRDA I); Release 1, DSTU Release 3 (US Realm), Volume 2—Templates and Supporting Material, June 2015, IBR approved for § 170.205(h).

(22) HL7 CDA© Release 2 Implementation Guide: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1; DSTU Release 1.1 (US Realm), Volume 1—Introductory Material, April 2015, IBR approved for § 170.205(i).

(23) HL7 CDA© Release 2 Implementation Guide: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1; DSTU Release 1.1 (US Realm), Volume 2—Templates and Supporting Material, April 2015, IBR approved for § 170.205(i).

(24) Errata to the HL7 Implementation Guide for CDA® Release 2: Quality Reporting Document Architecture—Category III, DSTU Release 1 (US Realm), September 2014, IBR approved for § 170.205(k).

(25) HL7 Version 3 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1, Part 1: CDA R2 and Privacy Metadata Reusable Content Profile, May 16, 2014, IBR approved for § 170.205(o).

(26) HL7 Implementation Guide for CDA® Release 2—Level 3: Healthcare Associated Infection Reports, Release 1 (U.S. Realm), August 9, 2013, IBR approved for § 170.205(r).

(27) HL7 Implementation Guide for CDA® Release 2: National Health Care Surveys (NHCS), Release 1—US Realm, HL7 Draft Standard for Trial Use, Volume 1—Introductory Material, December 2014, IBR approved for § 170.205(s).

(28) HL7 Implementation Guide for CDA® Release 2: National Health Care Surveys (NHCS), Release 1—US Realm, HL7 Draft Standard for Trial Use, Volume 2—Templates and Supporting Material, December 2014, IBR approved for §170.205(s).

(29) HL7 Version 3 (V3) Standard, Value Sets for AdministrativeGender and NullFlavor, published August 1, 2013, IBR approved for §170.207(n) and (o).

(30) HL7® CDA® R2 Implementation Guide: C–CDA Templates for Clinical Notes R2.1 Companion Guide, Release 2–US Realm, October 2019, IBR approved for §170.205(a).

(31) HL7 FHIR® Bulk Data Access (Flat FHIR®) (v1.0.0: STU 1), August 22, 2019, IBR approved for §170.215(a).

(32) HL7 FHIR SMART Application Launch Framework Implementation Guide Release 1.0.0, November 13, 2018, IBR approved for §170.215(a).

(33) HL7 Fast Healthcare Interoperability Resources Specification (FHIR®) Release 4, Version 4.0.1: R4, October 30, 2019, including Technical Correction #1, November 1, 2019, IBR approved for §170.215(a).

(34) HL7 FHIR® US Core Implementation Guide STU3 Release 3.1.1, August 28, 2020, IBR approved for §170.215(a).

(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).

(h) Integrating the Healthcare Enterprise (IHE), 820 Jorie Boulevard, Oak Brook, IL, Telephone (630) 481–1004, *http://www.ihe.net/*.

(1) IHE IT Infrastructure Technical Framework Volume 2b (ITI TF–2b), Transactions Part B—Sections 3.29—2.43, Revision 7.0, August 10, 2010, IBR approved for §170.205(p).

(2) [Reserved]

(i) Internet Engineering Task Force (IETF) Secretariat, c/o Association Management Solutions, LLC (AMS), 48377 Fremont Blvd., Suite 117, Fremont, CA, 94538, Telephone (510) 492–4080, *http://www.ietf.org/rfc.html*.

(1) [Reserved]

(2) Network Time Protocol Version 4: Protocol and Algorithms Specification, June 2010, IBR approved for §170.210.

(3) Request for Comment (RFC) 5646, ''Tags for Identifying Languages, September 2009,'' copyright 2009, IBR approved for §170.207(g).

(j) International Telecommunication Union (ITU), Place des Nations, 1211 Geneva 20 Switzerland, Telephone (41) 22 730 511, *http://www.itu.int/en/pages/default.aspx*.

(1) ITU–T E.123, Series E: Overall Network Operation, Telephone Service, Service Operation and Human Factors, International operation—General provisions concerning users: Notation for national and international telephone numbers, e-mail addresses and web addresses, February 2001, IBR approved for §170.207(q).

(2) ITU–T E.164, Series E: Overall Network Operation, Telephone Service, Service Operation and Human Factors, International operation—Numbering plan of the international telephone service, The international public telecommunication numbering plan, November 2010, IBR approved for §170.207(q).

(k) National Council for Prescription Drug Programs (NCPDP), Incorporated, 9240 E Raintree Drive, Scottsdale, AZ 85260–7518; phone (480) 477–1000; fax: (480) 767–1042: website: *www.ncpdp.org*.

(1) NCPDP SCRIPT Standard, Implementation Guide, Version 2017071,

ANSI-approved July 28, 2017; IBR approved for § 170.205(b).

(2) NCPDP SCRIPT Standard, Implementation Guide, Version 2023011, ANSI-approved January 17, 2023; IBR approved for § 170.205(b).

(3) NCPDP Real-Time Prescription Benefit Standard, Implementation Guide, Version 13, ANSI-approved May 19, 2022; IBR approved for § 170.205(c).

(4) NCPDP Formulary and Benefit Standard, Implementation Guide, Version 60, ANSI-approved April 12, 2023; IBR approved for § 170.205(u).

(l) National Institute of Standards and Technology, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899–8930, *http://csrc.nist.gov/groups/STM/cmvp/standards.html*.

(1) Annex A: Approved Security Functions for FIPS PUB 140–2, Security Requirements for Cryptographic Modules, Draft, January 27, 2010, IBR approved for § 170.210.

(2) Annex A: Approved Security Functions for FIPS PUB 140–2, Security Requirements for Cryptographic Modules, Draft, May 30, 2012, IBR approved for § 170.210.

(3) [Reserved]

(4) FIPS PUB 180–4, Secure Hash Standard (August 2015), IBR approved for § 170.210(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*.

(1) Applicability Statement for Secure Health Transport, Version 1.1, July 10, 2012, IBR approved for § 170.202; available at *http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__direct_project/3338*.

(2) XDR and XDM for Direct Messaging Specification, Version 1, March 9, 2011, IBR approved for § 170.202; available at *http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__direct_project/3338*.

(3) Transport and Security Specification, Version 1.0, June 19, 2012, IBR approved for § 170.202.

(4) ONC Implementation Guide for Direct Edge Protocols, Version 1.1, June 25, 2014, IBR approved for § 170.202; available at *http://www.healthit.gov/sites/default/files/implementationguidefordirectedgeprotocolsv1_1.pdf*.

(5) United States Core Data for Interoperability (USCDI), Version 1, July 2020 Errata, IBR approved for § 170.213; available at *https://www.healthit.gov/USCDI*.

(6) United States Core Data for Interoperability (USCDI), Version 3 (v3), October 2022 Errata; IBR approved for § 170.213(b).

(n) OpenID Foundation, 2400 Camino Ramon, Suite 375, San Ramon, CA 94583, Telephone +1 925–275–6639, *http://openid.net/*.

(1) OpenID Connect Core 1.0 Incorporating errata set 1, November 8, 2014, IBR approved for § 170.215(b).

(2) [Reserved]

(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/*.

(1) Public Health Data Standards Consortium Source of Payment Typology Code Set Version 5.0 (October 2011), IBR approved for § 170.207(s).

(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*.

(1) Logical Observation Identifiers Names and Codes (LOINC®) version 2.27, June 15, 2009, IBR approved for § 170.207.

(2) Logical Observation Identifiers Names and Codes (LOINC®) Database version 2.40, Released June 2012, IBR approved for § 170.207.

(3) Logical Observation Identifiers Names and Codes (LOINC®) Database version 2.52, Released June 2015, IBR approved for § 170.207(c).

(4) The Unified Code of Units for Measure, Revision 1.9, October 23, 2013, IBR approved for § 170.207.

(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).

(q) The Direct Project, c/o the Office of the National Coordinator for Health Information Technology (ONC), 330 C Street SW., Washington, DC 20201, *http://healthit.hhs.gov*.

(1) Applicability Statement for Secure Health Transport, Version 1.2, August 2015, IBR approved for §170.202(a).

(2) Implementation Guide for Delivery Notification in Direct, Version 1.0, June 29, 2012, IBR approved for §170.202(e).

(r) U.S. National Library of Medicine, 8600 Rockville Pike, Bethesda, MD 20894; phone (301) 594–5983; website: *www.nlm.nih.gov/*.

(1) International Health Terminology Standards Development Organization Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®), International Release, July 2009, IBR approved for §170.207.

(2) International Health Terminology Standards Development Organisation (IHTSDO) Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®) International Release July 31, 2012, IBR approved for §170.207.

(3) US Extension to SNOMED CT® March 2012 Release, IBR approved for §170.207.

(4)–(5) [Reserved]

(6) International Health Terminology Standards Development Organization (IHTSDO) Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®) U.S. Edition, September 2015 Release, IBR approved for §170.207(a).

(7) RxNorm, September 8, 2015 Full Release Update, IBR approved for §170.207(d).

(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).

(s) World Wide Web Consortium (W3C)/MIT, 32 Vassar Street, Room 32–G515, Cambridge, MA 02139 USA, *http://www.w3.org/standards/*

(1) Web Content Accessibility Guidelines (WCAG) 2.0, December 11, 2008, IBR approved for §170.204.

(2) [Reserved]

[75 FR 44649, July 28, 2010, as amended at 75 FR 62690, Oct. 13, 2010; 77 FR 54285, Sept. 4, 2012; 77 FR 72991, Dec. 7, 2012; 79 FR 54478, Sept. 11, 2014; 80 FR 62745, Oct. 16, 2015; 81 FR 72463, Oct. 19, 2016; 85 FR 25941, May 1, 2020; 85 FR 70082, Nov. 4, 2020; 89 FR 1428, Jan. 9, 2024; 89 FR 51265, June 17, 2024]

Subpart C—Certification Criteria for Health Information Technology

SOURCE: 75 FR 44651, July 28, 2010, unless otherwise noted.

§ 170.300 Applicability.

(a) The certification criteria adopted in this subpart apply to the testing and certification of Health IT Modules.

(b) When a certification criterion refers to two or more standards as alternatives, use of at least one of the alternative standards will be considered compliant.

(c) Health Modules are not required to be compliant with certification criteria or capabilities specified within a certification criterion that are designated as optional.

(d) In §170.315, all certification criteria and all capabilities specified within a certification criterion have general applicability (*i.e.*, apply to any health care setting) unless designated as ''inpatient setting only'' or ''ambulatory setting only.''

[75 FR 44649, July 28, 2010, as amended at 77 FR 54286, Sept. 4, 2012; 80 FR 62747, Oct. 16, 2015; 85 FR 25941, May 1, 2020; 85 FR 70083, Nov. 4, 2020]

§§ 170.302–170.306 [Reserved]

§ 170.314 [Reserved]

§ 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) *Clinical*—(1) *Computerized provider order entry—medications.* (i) Enable a user to record, change, and access medication orders.

(ii) *Optional.* Include a ''reason for order'' field.

(2) *Computerized provider order entry—laboratory.* (i) Enable a user to record, change, and access laboratory orders.

(ii) *Optional.* Include a ''reason for order'' field.

(3) *Computerized provider order entry—diagnostic imaging.* (i) Enable a user to record, change, and access diagnostic imaging orders.

(ii) *Optional.* Include a ''reason for order'' field.

(4) *Drug-drug, drug-allergy interaction checks for CPOE*—(i) *Interventions.* Before a medication order is completed and acted upon during computerized provider order entry (CPOE), interventions must automatically indicate to a user drug-drug and drug-allergy contraindications based on a patient's medication list and medication allergy list.

(ii) *Adjustments.* (A) Enable the severity level of interventions provided for drug-drug interaction checks to be adjusted.

(B) Limit the ability to adjust severity levels in at least one of these two ways:

(*1*) To a specific set of identified users.

(*2*) As a system administrative function.

(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) *Race and ethnicity.* (*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.

(*3*) Aggregate each one of the patient's races and ethnicities recorded in accordance with paragraphs (a)(5)(i)(A)(*1*) and (*2*) of this section to the categories in the standard specified in §170.207(f)(1).

(B) *Preferred language.* Enable preferred language to be recorded in accordance with the standard specified in §170.207(g)(2) and whether a patient declines to specify a preferred language.

(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.

(ii) *Inpatient setting only.* Enable a user to record, change, and access the preliminary cause of death and date of death in the event of mortality.

(6)–(8) [Reserved]

(9) *Clinical decision support (CDS)*—(i) *CDS intervention interaction.* Interventions provided to a user must occur when a user is interacting with technology.

(ii) *CDS configuration.* (A) Enable interventions and reference resources specified in paragraphs (a)(9)(iii) and (iv) of this section to be configured by a limited set of identified users (*e.g.*, system administrator) based on a user's role.

(B) Enable interventions:

(*1*) Based on the following data:

(*i*) Problem list;

(*ii*) Medication list;

(*iii*) Allergy and intolerance list;

(*iv*) At least one demographic specified in paragraph (a)(5)(i) of this section;

(*v*) Laboratory tests; and

(*vi*) Vital signs.

(*2*) When a patient's medications, allergies and intolerance, and problems are incorporated from a transition of care/referral summary received and pursuant to paragraph (b)(2)(iii)(D) of this section.

(iii) *Evidence-based decision support interventions.* Enable a limited set of identified users to select (*i.e.*, activate) electronic CDS interventions (in addition to drug-drug and drug-allergy contraindication checking) based on each one and at least one combination of the data referenced in paragraphs (a)(9)(ii)(B)(*1*)(*i*) through (*vi*) of this section.

(iv) *Linked referential CDS.* (A) Identify for a user diagnostic and therapeutic reference information in accordance at least one of the following standards and implementation specifications:

(*1*) The standard and implementation specifications specified in §170.204(b)(3).

(*2*) The standard and implementation specifications specified in §170.204(b)(4).

(B) For paragraph (a)(9)(iv)(A) of this section, technology must be able to identify for a user diagnostic or therapeutic reference information based on each one and at least one combination of the data referenced in paragraphs (a)(9)(ii)(B)(*1*)(*i*), (*ii*), and (*iv*) of this section.

(v) *Source attributes.* Enable a user to review the attributes as indicated for all CDS resources:

(A) For evidence-based decision support interventions under paragraph (a)(9)(iii) of this section:

(*1*) Bibliographic citation of the intervention (clinical research/guideline);

(*2*) Developer of the intervention (translation from clinical research/guideline);

(*3*) Funding source of the intervention development technical implementation; and

(*4*) Release and, if applicable, revision date(s) of the intervention or reference source.

(B) For linked referential CDS in paragraph (a)(9)(iv) of this section and drug-drug, drug-allergy interaction checks in paragraph (a)(4) of this section, the developer of the intervention, and where clinically indicated, the bibliographic citation of the intervention (clinical research/guideline).

(vi) *Expiration of criterion.* The adoption of this criterion for purposes of the ONC Health IT Certification Program expires on January 1, 2025.

(10) *Drug-formulary and preferred drug list checks.* The requirements specified in one of the following paragraphs (that is, paragraphs (a)(10)(i) and (a)(10)(ii) of this section) must be met to satisfy this certification criterion:

(i) *Drug formulary checks.* Automatically check whether a drug formulary exists for a given patient and medication.

(ii) *Preferred drug list checks.* Automatically check whether a preferred drug list exists for a given patient and medication.

(11) [Reserved]

(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).

(13) *Patient-specific education resources.* (i) Identify patient-specific education resources based on data included in the patient's problem list and medication list in accordance with at least one of the following standards and implementation specifications:

(A) The standard and implementation specifications specified in §170.204(b)(3).

(B) The standard and implementation specifications specified in § 170.204(b)(4).

(ii) *Optional.* Request that patient-specific education resources be identified in accordance with the standard in § 170.207(g)(2).

(14) *Implantable device list.* (i) Record Unique Device Identifiers associated with a patient's Implantable Devices.

(ii) Parse the following identifiers from a Unique Device Identifier:

(A) Device Identifier; and

(B) The following identifiers that compose the Production Identifier:

(*1*) The lot or batch within which a device was manufactured;

(*2*) The serial number of a specific device;

(*3*) The expiration date of a specific device;

(*4*) The date a specific device was manufactured; and

(*5*) For an HCT/P regulated as a device, the distinct identification code required by 21 CFR 1271.290(c).

(iii) Obtain and associate with each Unique Device Identifier:

(A) A description of the implantable device referenced by at least one of the following:

(*1*) The ''GMDN PT Name'' attribute associated with the Device Identifier in the Global Unique Device Identification Database.

(*2*) The ''SNOMED CT® Description'' mapped to the attribute referenced in in paragraph (a)(14)(iii)(A)(*1*) of this section.

(B) The following Global Unique Device Identification Database attributes:

(*1*) ''Brand Name'';

(*2*) ''Version or Model'';

(*3*) ''Company Name'';

(*4*) ''What MRI safety information does the labeling contain?''; and

(*5*) ''Device required to be labeled as containing natural rubber latex or dry natural rubber (21 CFR 801.437).''

(iv) Display to a user an implantable device list consisting of:

(A) The active Unique Device Identifiers recorded for the patient;

(B) For each active Unique Device Identifier recorded for a patient, the description of the implantable device specified by paragraph (a)(14)(iii)(A) of this section; and

(C) A method to access all Unique Device Identifiers recorded for a patient.

(v) For each Unique Device Identifier recorded for a patient, enable a user to access:

(A) The Unique Device Identifier;

(B) The description of the implantable device specified by paragraph (a)(14)(iii)(A) of this section;

(C) The identifiers associated with the Unique Device Identifier, as specified by paragraph (a)(14)(ii) of this section; and

(D) The attributes associated with the Unique Device Identifier, as specified by paragraph (a)(14)(iii)(B) of this section.

(vi) Enable a user to change the status of a Unique Device Identifier recorded for a patient.

(15) *Social, psychological, and behavioral data.* Enable a user to record, change, and access the following patient social, psychological, and behavioral data:

(i) *Financial resource strain.* Enable financial resource strain to be recorded in accordance with the standard specified in § 170.207(p)(1) and whether a patient declines to specify financial resource strain.

(ii) *Education.* Enable education to be recorded in accordance with the standard specified in § 170.207(p)(2) and whether a patient declines to specify education.

(iii) *Stress.* Enable stress to be recorded in accordance with the standard specified in § 170.207(p)(3) and whether a patient declines to specify stress.

(iv) *Depression.* Enable depression to be recorded in accordance with the standard specified in § 170.207(p)(4) and whether a patient declines to specify depression.

(v) *Physical activity.* Enable physical activity to be recorded in accordance with the standard specified in § 170.207(p)(5) and whether a patient declines to specify physical activity.

(vi) *Alcohol use.* Enable alcohol use to be recorded in accordance with the standard specified in § 170.207(p)(6) and whether a patient declines to specify alcohol use.

(vii) *Social connection and isolation.* Enable social connection and isolation to be recorded in accordance the standard specified in § 170.207(p)(7) and

whether a patient declines to specify social connection and isolation.

(viii) *Exposure to violence (intimate partner violence).* Enable exposure to violence (intimate partner violence) to be recorded in accordance with the standard specified in §170.207(p)(8) and whether a patient declines to specify exposure to violence (intimate partner violence).

(b) *Care coordination*—(1) *Transitions of care*—(i) *Send and receive via edge protocol.* (A) Send transition of care/referral summaries through a method that conforms to the standard specified in §170.202(d) and that leads to such summaries being processed by a service that has implemented the standard specified in §170.202(a)(2); and

(B) Receive transition of care/referral summaries through a method that conforms to the standard specified in §170.202(d) from a service that has implemented the standard specified in §170.202(a)(2).

(C) *XDM processing.* Receive and make available the contents of a XDM package formatted in accordance with the standard adopted in §170.205(p)(1) when the technology is also being certified using an SMTP-based edge protocol.

(ii) *Validate and display*—(A) *Validate C–CDA conformance—system performance.* Demonstrate the ability to detect valid and invalid transition of care/referral summaries received and formatted in accordance with the standards specified in §170.205(a)(3), (4), and (5) for the Continuity of Care Document, Referral Note, and (inpatient setting only) Discharge Summary document templates. This includes the ability to:

(*1*) Parse each of the document types.

(*2*) Detect errors in corresponding ''document-templates,'' ''section-templates,'' and ''entry-templates,'' including invalid vocabulary standards and codes not specified in the standards adopted in §170.205(a)(3), (4), and (5).

(*3*) Identify valid document-templates and process the data elements required in the corresponding section-templates and entry-templates from the standards adopted in §170.205(a)(3), (4), and (5).

(*4*) Correctly interpret empty sections and null combinations.

(*5*) Record errors encountered and allow a user through at least one of the following ways to:

(*i*) Be notified of the errors produced.

(*ii*) Review the errors produced.

(B) *Display.* Display in human readable format the data included in transition of care/referral summaries received and formatted according to the standards specified in §170.205(a)(3), (4), and (5).

(C) *Display section views.* Allow for the individual display of each section (and the accompanying document header information) that is included in a transition of care/referral summary received and formatted in accordance with the standards adopted in §170.205(a)(3), (4), and (5) in a manner that enables the user to:

(*1*) Directly display only the data within a particular section;

(*2*) Set a preference for the display order of specific sections; and

(*3*) Set the initial quantity of sections to be displayed.

(iii) *Create.* Enable a user to create a transition of care/referral summary formatted in accordance with the standard specified in §170.205(a)(3), (4), and (5) using the Continuity of Care Document, Referral Note, and (inpatient setting only) Discharge Summary document templates that includes, at a minimum:

(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

(*3*) The following data classes:

(*i*) *Assessment and plan of treatment.* In accordance with the ''Assessment and Plan Section (V2)'' of the standard specified in §170.205(a)(4); or in accordance with the ''Assessment Section (V2)'' and ''Plan of Treatment Section (V2)'' of the standard specified in §170.205(a)(4).

(*ii*) *Goals.* In accordance with the ''Goals Section'' of the standard specified in §170.205(a)(4).

(*iii*) *Health concerns.* In accordance with the ''Health Concerns Section'' of the standard specified in § 170.205(a)(4).

(*iv*) *Unique device identifier(s) for a patient's implantable device(s).* In accordance with the ''Product Instance'' in the ''Procedure Activity Procedure Section'' of the standard specified in § 170.205(a)(4).

(B) *Encounter diagnoses.* Formatted according to at least one of the following standards:

(*1*) The standard specified in § 170.207(i).

(*2*) At a minimum, the version of the standard specified in § 170.207(a)(1).

(C) Cognitive status.

(D) Functional status.

(E) *Ambulatory setting only.* The reason for referral; and referring or transitioning provider's name and office contact information.

(F) *Inpatient setting only.* Discharge instructions.

(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:

(*1*) *Date of birth constraint.* (*i*) The year, month and day of birth must be present for a date of birth. The technology must include a null value when the date of birth is unknown.

(*ii*) *Optional.* When the hour, minute, and second are associated with a date of birth the technology must demonstrate that the correct time zone offset is included.

(*2*) *Phone number constraint.* Represent phone number (home, business, cell) in accordance with the standards adopted in § 170.207(q)(1). All phone numbers must be included when multiple phone numbers are present.

(*3*) *Sex Constraint:* Represent sex with the standard adopted in § 170.207(n)(1) up to and including December 31, 2025; or with the standard adopted in § 170.207(n)(2).

(2) *Clinical information reconciliation and incorporation*—(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) *Reconciliation.* Enable a user to reconcile the data that represent a patient's active medication list, allergies and intolerance list, and problem list as follows. For each list type:

(A) Simultaneously display (*i.e.*, in a single view) the data from at least two sources in a manner that allows a user to view the data and their attributes, which must include, at a minimum, the source and last modification date.

(B) Enable a user to create a single reconciled list of each of the following: Medications; Allergies and Intolerances; and problems.

(C) Enable a user to review and validate the accuracy of a final set of data.

(D) Upon a user's confirmation, automatically update the list, and incorporate the following data expressed according to the specified standards:

(*1*) *Medications.* At a minimum, the version of the standard specified in § 170.213;

(*2*) *Allergies and intolerance.* At a minimum, the version of the standard specified in § 170.213; and

(*3*) *Problems.* At a minimum, the version of the standard specified in § 170.213.

(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 § 170.205(a)(5) on and after December 31, 2022.

(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) *Electronic prescribing.* (i) For technology certified prior to June 30, 2020, subject to the real world testing provisions at §170.405(b)(5),

(A) Enable a user to perform the following prescription-related electronic transactions in accordance with, at a minimum, the version of the standard specified in §170.207(d)(3) as follows:

(*1*) Create new prescriptions (NEWRX).

(*2*) Change prescriptions (RXCHG, CHGRES).

(*3*) Cancel prescriptions (CANRX, CANRES).

(*4*) Refill prescriptions (REFREQ, REFRES).

(*5*) Receive fill status notifications (RXFILL).

(*6*) Request and receive medication history information (RXHREQ, RXHRES).

(B) For each transaction listed in paragraph (b)(3)(i)(A) of this section, the technology must be able to receive and transmit the reason for the prescription using the diagnosis elements in the DRU Segment.

(C) *Optional:* For each transaction listed in paragraph (b)(3)(i)(A) of this section, the technology must be able to receive and transmit the reason for prescription using the indication elements in the SIG Segment.

(D) Limit a user's ability to prescribe all oral liquid medications in only metric standard units of mL (*i.e.,* not cc).

(E) Always insert leading zeroes before the decimal point for amounts less than one and must not allow trailing zeroes after a decimal point when a user prescribes medications.

(ii) For technology certified subsequent to June 30, 2020:

(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:

(*1*) Create new prescriptions (NewRx).

(*2*) Request and respond to change prescriptions (RxChangeRequest, RxChangeResponse).

(*3*) Request and respond to cancel prescriptions (CancelRx, CancelRxResponse).

(*4*) Request and respond to renew prescriptions (RxRenewalRequest, RxRenewalResponse).

(*5*) Receive fill status notifications (RxFill).

(*6*) Request and receive medication history (RxHistoryRequest, RxHistoryResponse).

(*7*) Relay acceptance of a transaction back to the sender (Status).

(*8*) Respond that there was a problem with the transaction (Error).

(*9*) Respond that a transaction requesting a return receipt has been received (Verify).

(B) Optionally, 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)(3) as follows:

(*1*) Create and respond to new prescriptions (NewRxRequest, NewRxResponseDenied).

(*2*) Send fill status notifications (RxFillIndicatorChange).

(*3*) Ask the Mailbox if there are any transactions (GetMessage).

(*4*) Request to send an additional supply of medication (Resupply).

(*5*) Communicate drug administration events (DrugAdministration).

(*6*) Request and respond to transfer one or more prescriptions between pharmacies (RxTransferRequest, RxTransferResponse, RxTransferConfirm).

(*7*) Recertify the continued administration of a medication order (Recertification).

(*8*) Complete Risk Evaluation and Mitigation Strategy (REMS) transactions (REMSInitiationRequest, REMSInitiationResponse, REMSRequest, and REMSResponse).

(*9*) Electronic prior authorization transactions (PAInitiationRequest, PAInitiationResponse, PARequest,

PAResponse, PAAppealRequest, PAAppealResponse, PACancelRequest, and PACancelResponse).

(C) For the following prescription-related transactions, the technology must be able to receive and transmit the reason for prescription using the diagnosis elements: <Diagnosis> <Primary> or <Secondary>:

(*1*) *Required transactions:*

(*i*) Create new prescriptions (NewRx).

(*ii*) Request and respond to change prescriptions (RxChangeRequest, RxChangeResponse).

(*iii*) Cancel prescriptions (CancelRx).

(*iv*) Request and respond to renew prescriptions (RxRenewalRequest, RxRenewalResponse).

(*v*) Receive fill status notifications (RxFill).

(*vi*) Receive medication history (RxHistoryResponse).

(*2*) *Optional transactions:*

(*i*) Request to send an additional supply of medication (Resupply)

(*ii*) Request and respond to transfer one or more prescriptions between pharmacies (RxTransferRequest, RxTransferResponse)

(*iii*) Complete Risk Evaluation and Mitigation Strategy (REMS) transactions (REMSInitiationRequest, REMSInitiationResponse, REMSRequest, and REMSResponse).

(*iv*) Electronic prior authorization (ePA) transactions (PAInitiationRequest, PAInitiationResponse, PARequest, PAResponse, PAAppealRequest, PAAppealResponse and PACancelRequest, PACancelResponse).

(D) *Optional:* For each transaction listed in paragraph (b)(3)(ii)(C) of this section, the technology must be able to receive and transmit reason for prescription using the <IndicationforUse> element in the SIG segment.

(E) Limit a user's ability to prescribe all oral liquid medications in only metric standard units of mL (*i.e.*, not cc).

(F) Always insert leading zeroes before the decimal point for amounts less than one and must not allow trailing zeroes after a decimal point when a user prescribes medications.

(4)–(5) [Reserved]

(6) *Data export*—(i) *General requirements for export summary configuration.* (A) Enable a user to set the configuration options specified in paragraphs (b)(6)(iii) and (iv) of this section when creating an export summary as well as a set of export summaries for patients whose information is stored in the technology. A user must be able to execute these capabilities at any time the user chooses and without subsequent developer assistance to operate.

(B) Limit the ability of users who can create export summaries in at least one of these two ways:

(*1*) To a specific set of identified users.

(*2*) As a system administrative function.

(ii) *Creation.* Enable a user to create export summaries formatted in accordance with the standard specified in §170.205(a)(4) using the Continuity of Care Document document template that includes, at a minimum:

(A) The Common Clinical Data Set.

(B) *Encounter diagnoses.* Formatted according to at least one of the following standards:

(*1*) The standard specified in §170.207(i).

(*2*) At a minimum, the version of the standard specified in §170.207(a)(1).

(C) Cognitive status.

(D) Functional status.

(E) *Ambulatory setting only.* The reason for referral; and referring or transitioning provider's name and office contact information.

(F) *Inpatient setting only.* Discharge instructions.

(iii) *Timeframe configuration.* (A) Enable a user to set the date and time period within which data would be used to create the export summaries. This must include the ability to enter in a start and end date and time range.

(B) Consistent with the date and time period specified in paragraph (b)(6)(iii)(A) of this section, enable a user to do each of the following:

(*1*) Create export summaries in real-time;

(*2*) Create export summaries based on a relative date and time (*e.g.*, the first of every month at 1:00 a.m.); and

(*3*) Create export summaries based on a specific date and time (*e.g.*, on 10/24/2015 at 1:00 a.m.).

(iv) *Location configuration.* Enable a user to set the storage location to

which the export summary or export summaries are intended to be saved.

(7) *Security tags—summary of care—send.* Enable a user to create a summary record formatted in accordance with the standard adopted in §170.205(a)(4) that is tagged as restricted and subject to restrictions on re-disclosure according to the standard adopted in §170.205(o)(1) at the:

(i) Document, section, and entry (data element) level; or

(ii) Document level for the period before December 31, 2022.

(8) *Security tags—summary of care—receive.* (i) Enable a user to receive a summary record that is formatted in accordance with the standard adopted in §170.205(a)(4) that is tagged as restricted and subject to restrictions on re-disclosure according to the standard adopted in §170.205(o)(1) at the:

(A) Document, section, and entry (data element) level; or

(B) Document level for the period before December 31, 2022; and

(ii) Preserve privacy markings to ensure fidelity to the tagging based on consent and with respect to sharing and re-disclosure restrictions.

(9) *Care plan.* Enable a user to record, change, access, create, and receive care plan information in accordance with:

(i) The Care Plan document template, including the Health Status Evaluations and Outcomes Section and Interventions Section (V2), in the standard specified in §170.205(a)(4); and

(ii) The standard in §170.205(a)(5) for the time period up to and including December 31, 2025; or §170.205(a)(6).

(10) *Electronic Health Information export*—(i) *Single patient electronic health information export.* (A) Enable a user to timely create an export file(s) with all of a single patient's electronic health information that can be stored at the time of certification by the product, of which the Health IT Module is a part.

(B) A user must be able to execute this capability at any time the user chooses and without subsequent developer assistance to operate.

(C) Limit the ability of users who can create export file(s) in at least one of these two ways:

(*1*) To a specific set of identified users

(*2*) As a system administrative function.

(D) The export file(s) created must be electronic and in a computable format.

(E) The publicly accessible hyperlink of the export's format must be included with the exported file(s).

(ii) *Patient population electronic health information export.* Create an export of all the electronic health information that can be stored at the time of certification by the product, of which the Health IT Module is a part.

(A) The export created must be electronic and in a computable format.

(B) The publicly accessible hyperlink of the export's format must be included with the exported file(s).

(iii) *Documentation.* The export format(s) used to support paragraphs (b)(10)(i) and (ii) of this section must be kept up-to-date.

(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) *Clinical quality measures*—(1) *Clinical quality measures—record and export*—(i) *Record.* For each and every CQM for which the technology is presented for certification, the technology must be able to record all of the data that would be necessary to calculate each CQM. Data required for CQM exclusions or exceptions must be codified entries, which may include specific terms as defined by each CQM, or may include codified expressions of ''patient reason,'' ''system reason,'' or ''medical reason.''

(ii) *Export.* A user must be able to export a data file at any time the user chooses and without subsequent developer assistance to operate:

(A) Formatted in accordance with the standard specified in §170.205(h)(2);

(B) Ranging from one to multiple patients; and

(C) That includes all of the data captured for each and every CQM to which technology was certified under paragraph (c)(1)(i) of this section.

(2) *Clinical quality measures—import and calculate*—(i) *Import.* Enable a user to import a data file in accordance with the standard specified in §170.205(h)(2) for one or multiple patients and use such data to perform the capability specified in paragraph (c)(2)(ii) of this section. A user must be able to execute this capability at any time the user chooses and without subsequent developer assistance to operate.

(ii) Calculate each and every clinical quality measure for which it is presented for certification.

(3) *Clinical quality measures—report.* Enable a user to electronically create a data file for transmission of clinical quality measurement data:

(i) In accordance with the applicable implementation specifications specified by the CMS implementation guides for Quality Reporting Document Architecture (QRDA), category I, for inpatient measures in §170.205(h)(3) and CMS implementation guide for QRDA, category III for ambulatory measures in §170.205 (k)(3); or

(ii) In accordance with the standards specified in §170.205(h)(2) and §170.205(k)(1) and (2) for the period before December 31, 2022.

(4) *Clinical quality measures—filter.* (i) Record the data listed in paragraph (c)(4)(iii) of this section in accordance with the identified standards, where specified.

(ii) Filter CQM results at the patient and aggregate levels by each one and any combination of the data listed in paragraph (c)(4)(iii) of this section and be able to:

(A) Create a data file of the filtered data in accordance with the standards adopted in §170.205(h)(2) and §170.205(k)(1) and (2); and

(B) Display the filtered data results in human readable format.

(iii) *Data.*

(A) Taxpayer Identification Number.

(B) National Provider Identifier.

(C) Provider type in accordance with, at a minimum, the standard specified in §170.207(r)(2).

(D) Practice site address.

(E) Patient insurance in accordance with the standard specified in §170.207(s)(2).

(F) Patient age.

(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).

(d) *Privacy and security*—(1) *Authentication, access control, and authorization.* (i) Verify against a unique identifier(s) (*e.g.*, username or number) that a user seeking access to electronic health information is the one claimed; and

(ii) Establish the type of access to electronic health information a user is permitted based on the unique identifier(s) provided in paragraph (d)(1)(i) of this section, and the actions the user is permitted to perform with the technology.

(2) *Auditable events and tamper-resistance*—(i) *Record actions.* Technology must be able to:

(A) Record actions related to electronic health information in accordance with the standard specified in §170.210(e)(1);

(B) Record the audit log status (enabled or disabled) in accordance with the standard specified in §170.210(e)(2) unless it cannot be disabled by any user; and

(C) Record the encryption status (enabled or disabled) of electronic health information locally stored on end-user devices by technology in accordance with the standard specified in §170.210(e)(3) unless the technology prevents electronic health information from being locally stored on end-user devices (see paragraph (d)(7) of this section).

(ii) *Default setting.* Technology must be set by default to perform the capabilities specified in paragraph (d)(2)(i)(A) of this section and, where applicable, paragraphs (d)(2)(i)(B) and (d)(2)(i)(C) of this section.

(iii) *When disabling the audit log is permitted.* For each capability specified in paragraphs (d)(2)(i)(A) through (C) of this section that technology permits to be disabled, the ability to do so must be restricted to a limited set of users.

(iv) *Audit log protection.* Actions and statuses recorded in accordance with paragraph (d)(2)(i) of this section must not be capable of being changed, overwritten, or deleted by the technology.

(v) *Detection.* Technology must be able to detect whether the audit log has been altered.

(3) *Audit report(s).* Enable a user to create an audit report for a specific time period and to sort entries in the audit log according to each of the data specified in the standards in §170.210(e).

(4) *Amendments.* Enable a user to select the record affected by a patient's request for amendment and perform the capabilities specified in paragraph (d)(4)(i) or (ii) of this section.

(i) *Accepted amendment.* For an accepted amendment, append the amendment to the affected record or include a link that indicates the amendment's location.

(ii) *Denied amendment.* For a denied amendment, at a minimum, append the request and denial of the request in at least one of the following ways:

(A) To the affected record.

(B) Include a link that indicates this information's location.

(5) *Automatic access time-out.* (i) Automatically stop user access to health information after a predetermined period of inactivity.

(ii) Require user authentication in order to resume or regain the access that was stopped.

(6) *Emergency access.* Permit an identified set of users to access electronic health information during an emergency.

(7) *End-user device encryption.* The requirements specified in one of the following paragraphs (that is, paragraphs (d)(7)(i) and (d)(7)(ii) of this section) must be met to satisfy this certification criterion.

(i) Technology that is designed to locally store electronic health information on end-user devices must encrypt the electronic health information stored on such devices after use of the technology on those devices stops.

(A) Electronic health information that is stored must be encrypted in accordance with the standard specified in §170.210(a)(2).

(B) *Default setting.* Technology must be set by default to perform this capability and, unless this configuration cannot be disabled by any user, the ability to change the configuration must be restricted to a limited set of identified users.

(ii) Technology is designed to prevent electronic health information from being locally stored on end-user devices after use of the technology on those devices stops.

(8) *Integrity.* (i) Create a message digest in accordance with the standard specified in §170.210(c)(2).

(ii) Verify in accordance with the standard specified in §170.210(c)(2) upon receipt of electronically exchanged health information that such information has not been altered.

(9) *Trusted connection.* Establish a trusted connection using one of the following methods:

(i) *Message-level.* Encrypt and integrity protect message contents in accordance with the standards specified in §170.210(a)(2) and (c)(2).

(ii) *Transport-level.* Use a trusted connection in accordance with the standards specified in §170.210(a)(2) and (c)(2).

(10) *Auditing actions on health information.* (i) By default, be set to record actions related to electronic health information in accordance with the standard specified in § 170.210(e)(1).

(ii) If technology permits auditing to be disabled, the ability to do so must be restricted to a limited set of users.

(iii) Actions recorded related to electronic health information must not be capable of being changed, overwritten, or deleted by the technology.

(iv) Technology must be able to detect whether the audit log has been altered.

(11) *Accounting of disclosures.* Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in § 170.210(d).

(12) *Encrypt authentication credentials.* Health IT developers must make one of the following attestations and may provide the specified accompanying information, where applicable:

(i) Yes—the Health IT Module encrypts stored authentication credentials in accordance with standards adopted in § 170.210(a)(2).

(ii) No—the Health IT Module does not encrypt stored authentication credentials. When attesting ''no,'' the health IT developer may explain why the Health IT Module does not support encrypting stored authentication credentials.

(13) *Multi-factor authentication.* Health IT developers must make one of the following attestations and, as applicable, provide the specified accompanying information:

(i) Yes—the Health IT Module supports the authentication, through multiple elements, of the user's identity with the use of industry-recognized standards. When attesting ''yes,'' the health IT developer must describe the use cases supported.

(ii) No—the Health IT Module does not support authentication, through multiple elements, of the user's identity with the use of industry-recognized standards. When attesting ''no,'' the health IT developer may explain why the Health IT Module does not support authentication, through multiple elements, of the user's identity with the use of industry-recognized standards.

(e) *Patient engagement*—(1) *View, download, and transmit to 3rd party.* (i) Patients (and their authorized representatives) must be able to use internet-based technology to view, download, and transmit their health information to a 3rd party in the manner specified below. Such access must be consistent and in accordance with the standard adopted in § 170.204(a)(1) and may alternatively be demonstrated in accordance with the standard specified in § 170.204(a)(2).

(A) *View.* Patients (and their authorized representatives) must be able to use health IT to view, at a minimum, the following data:

(*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.

(*3*) The following data classes:

(*i*) *Assessment and plan of treatment.* In accordance with the ''Assessment and Plan Section (V2)'' of the standard specified in § 170.205(a)(4); or in accordance with the ''Assessment Section (V2)'' and ''Plan of Treatment Section (V2)'' of the standard specified in § 170.205(a)(4).

(*ii*) *Goals.* In accordance with the ''Goals Section'' of the standard specified in § 170.205(a)(4).

(*iii*) *Health concerns.* In accordance with the ''Health Concerns Section'' of the standard specified in § 170.205(a)(4).

(*iv*) *Unique device identifier(s) for a patient's implantable device(s).* In accordance with the ''Product Instance'' in the ''Procedure Activity Procedure Section'' of the standards specified in § 170.205(a)(4).

(*4*) Ambulatory setting only. Provider's name and office contact information.

(*5*) Inpatient setting only. Admission and discharge dates and locations; discharge instructions; and reason(s) for hospitalization.

(*6*) Laboratory test report(s). Laboratory test report(s), including:

(*i*) The information for a test report as specified all the data specified in 42 CFR 493.1291(c)(1) through (7);

(*ii*) The information related to reference intervals or normal values as specified in 42 CFR 493.1291(d); and

(*iii*) The information for corrected reports as specified in 42 CFR 493.1291(k)(2).

(*7*) Diagnostic image report(s).

(B) *Download.* (*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):

(*i*) *Ambulatory setting only.* All of the data specified in paragraph (e)(1)(i)(A)(*1*), (*2*), (*4*), and (*5*) of this section.

(*ii*) *Inpatient setting only.* All of the data specified in paragraphs (e)(1)(i)(A)(*1*), and (*3*) through (*5*) of this section.

(*3*) *Inpatient setting only.* Patients (and their authorized representatives) must be able to download transition of care/referral summaries that were created as a result of a transition of care (pursuant to the capability expressed in the certification criterion specified in paragraph (b)(1) of this section).

(C) *Transmit to third party.* Patients (and their authorized representatives) must be able to:

(*1*) Transmit the ambulatory summary or inpatient summary (as applicable to the health IT setting for which certification is requested) created in paragraph (e)(1)(i)(B)(*2*) of this section in accordance with both of the following ways:

(*i*) Email transmission to any email address; and

(*ii*) An encrypted method of electronic transmission.

(*2*) *Inpatient setting only.* Transmit transition of care/referral summaries (as a result of a transition of care/referral as referenced by (e)(1)(i)(B)(*3*)) of this section selected by the patient (or their authorized representative) in both of the ways referenced (e)(1)(i)(C)(*1*)(*i*) and (*ii*) of this section).

(D) *Timeframe selection.* With respect to the data available to view, download, and transmit as referenced paragraphs (e)(1)(i)(A), (B), and (C) of this section, patients (and their authorized representatives) must be able to:

(*1*) Select data associated with a specific date (to be viewed, downloaded, or transmitted); and

(*2*) Select data within an identified date range (to be viewed, downloaded, or transmitted).

(ii) *Activity history log.* (A) When any of the capabilities included in paragraphs (e)(1)(i)(A) through (C) of this section are used, the following information must be recorded and made accessible to the patient (or his/her authorized representative):

(*1*) The action(s) (*i.e.*, view, download, transmission) that occurred;

(*2*) The date and time each action occurred in accordance with the standard specified in §170.210(g);

(*3*) The user who took the action; and

(*4*) Where applicable, the addressee to whom an ambulatory summary or inpatient summary was transmitted.

(B) [Reserved]

(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.

(2) *Secure messaging.* Enable a user to send messages to, and receive messages from, a patient in a secure manner.

(3) *Patient health information capture.* Enable a user to:

(i) Identify, record, and access information directly and electronically shared by a patient (or authorized representative).

(ii) Reference and link to patient health information documents.

(f) *Public health*—(1) *Transmission to immunization registries.* (i) Create immunization information for electronic transmission in accordance with:

(A) The standard and applicable implementation specifications specified in § 170.205(e)(4).

(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.

(ii) Enable a user to request, access, and display a patient's evaluated immunization history and the immunization forecast from an immunization registry in accordance with the standard at § 170.205(e)(4).

(2) *Transmission to public health agencies—syndromic surveillance.* Create syndrome-based public health surveillance information for electronic transmission in accordance with the standard (and applicable implementation specifications) specified in § 170.205(d)(4).

(3) *Transmission to public health agencies—reportable laboratory tests and values/results.* Create reportable laboratory tests and values/results for electronic transmission in accordance with:

(i) The standard (and applicable implementation specifications) specified in § 170.205(g).

(ii) At a minimum, the versions of the standards specified in § 170.207(a)(1) and (c)(1).

(4) *Transmission to cancer registries.* Create cancer case information for electronic transmission in accordance with:

(i) The standard (and applicable implementation specifications) specified in § 170.205(i)(2).

(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.

(6) *Transmission to public health agencies—antimicrobial use and resistance reporting.* Create antimicrobial use and resistance reporting information for electronic transmission in accordance with the standard specified in §170.205(r)(1).

(7) *Transmission to public health agencies—health care surveys.* Create health care survey information for electronic transmission in accordance with the standard specified in §170.205(s)(1).

(g) *Design and performance*—(1) *Automated numerator recording.* For each Promoting Interoperability Programs percentage-based measure, technology must be able to create a report or file that enables a user to review the patients or actions that would make the patient or action eligible to be included in the measure's numerator. The information in the report or file created must be of sufficient detail such that it enables a user to match those patients or actions to meet the measure's denominator limitations when necessary to generate an accurate percentage.

(2) *Automated measure calculation.* For each Promoting Interoperability Programs percentage-based measure that is supported by a capability included in a technology, record the numerator and denominator and create a report including the numerator, denominator, and resulting percentage associated with each applicable measure.

(3) *Safety-enhanced design.* (i) 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.

(ii) *Number of test participants.* A minimum of 10 test participants must be used for the testing of each capability identified in paragraph (g)(3)(i) of this section.

(iii) One of the following must be submitted on the user-centered design processed used:

(A) Name, description and citation (URL and/or publication citation) for an industry or federal government standard.

(B) Name the process(es), provide an outline of the process(es), a short description of the process(es), and an explanation of the reason(s) why use of any of the existing user-centered design standards was impractical.

(iv) The following information/sections from NISTIR 7742 must be submitted for each capability to which user-centered design processes were applied:

(A) Name and product version; date and location of the test; test environment; description of the intended users; and total number of participants;

(B) Description of participants, including: Sex; age; education; occupation/role; professional experience; computer experience; and product experience;

(C) Description of the user tasks that were tested and association of each task to corresponding certification criteria;

(D) The specific metrics captured during the testing of each user task performed in (g)(3)(iv)(C) of this section, which must include: Task success (%); task failures (%); task standard deviations (%); task performance time; and user satisfaction rating (based on a scale with 1 as very difficult and 5 as very easy) or an alternative acceptable user satisfaction measure;

(E) Test results for each task using the metrics identified above in paragraph (g)(3)(iv)(D) of this section; and

(F) Results and data analysis narrative, including: Major test finding; effectiveness; efficiency; satisfaction; and areas for improvement.

(v) Submit test scenarios used in summative usability testing.

(4) *Quality management system.* (i) For each capability that a technology includes and for which that capability's certification is sought, the use of a Quality Management System (QMS) in

the development, testing, implementation, and maintenance of that capability must be identified that satisfies one of the following ways:

(A) The QMS used is established by the Federal government or a standards developing organization.

(B) The QMS used is mapped to one or more QMS established by the Federal government or standards developing organization(s).

(ii) When a single QMS was used for applicable capabilities, it would only need to be identified once.

(iii) When different QMS were applied to specific capabilities, each QMS applied would need to be identified.

(5) *Accessibility-centered design.* For each capability that a Health IT Module includes and for which that capability's certification is sought, the use of a health IT accessibility-centered design standard or law in the development, testing, implementation and maintenance of that capability must be identified.

(i) When a single accessibility-centered design standard or law was used for applicable capabilities, it would only need to be identified once.

(ii) When different accessibility-centered design standards and laws were applied to specific capabilities, each accessibility-centered design standard or law applied would need to be identified. This would include the application of an accessibility-centered design standard or law to some capabilities and none to others.

(iii) When no accessibility-centered design standard or law was applied to all applicable capabilities such a response is acceptable to satisfy this certification criterion.

(6) *Consolidated CDA creation performance.* The following technical and performance outcomes must be demonstrated related to Consolidated CDA creation. The capabilities required under paragraphs (g)(6)(i) through (v) of this section can be demonstrated in tandem and do not need to be individually addressed in isolation or sequentially.

(i) This certification criterion's scope includes:

(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.

(C) The following data classes:

(*1*) *Assessment and plan of treatment.* In accordance with the ''Assessment and Plan Section (V2)'' of the standard specified in §170.205(a)(4); or in accordance with the ''Assessment Section (V2)'' and ''Plan of Treatment Section (V2)'' of the standard specified in §170.205(a)(4).

(*2*) *Goals.* In accordance with the ''Goals Section'' of the standard specified in §170.205(a)(4).

(*3*) *Health concerns.* In accordance with the ''Health Concerns Section'' of the standard specified in §170.205(a)(4).

(*4*) *Unique device identifier(s) for a patient's implantable device(s).* In accordance with the ''Product Instance'' in the ''Procedure Activity Procedure Section'' of the standard specified in §170.205(a)(4).

(ii) *Reference C–CDA match.* (A) For health IT certified to (g)(6)(i)(A) of this section, create a data file formatted in accordance with the standard adopted in §170.205(a)(4) and (5) that matches a gold-standard, reference data file.

(B) For health IT certified to (g)(6)(i)(B) of this section, create a data file formatted in accordance with the standard adopted in §170.205(a)(4) that matches a gold-standard, reference data file.

(iii) *Document-template conformance.* (A) For health IT certified to (g)(6)(i)(A) of this section, create a data file formatted in accordance with the standard adopted in §170.205(a)(4) and (5) that demonstrates a valid implementation of each document template applicable to the certification criterion or criteria within the scope of the certificate sought.

(B) For health IT certified to (g)(6)(i)(B) of this section, create a data file formatted in accordance with the standard adopted in §170.205(a)(4) that demonstrates a valid implementation of each document template applicable

to the certification criterion or criteria within the scope of the certificate sought.

(iv) *Vocabulary conformance.* (A) For health IT certified to (g)(6)(i)(A) of this section, create a data file formatted in accordance with the standard adopted in §170.205(a)(4) and (5) that demonstrates the required vocabulary standards (and value sets) are properly implemented.

(B) For health IT certified to (g)(6)(i)(B) of this section, create a data file formatted in accordance with the standard adopted in §170.205(a)(4) that demonstrates the required vocabulary standards (and value sets) are properly implemented.

(v) *Completeness verification.* Create a data file for each of the applicable document templates referenced in paragraph (g)(6)(iii) of this section without the omission of any of the data included in either paragraph (g)(6)(i)(A) or (B) of this section, as applicable.

(7) *Application access—patient selection.* The following technical outcome and conditions must be met through the demonstration of an application programming interface (API).

(i) *Functional requirement.* The technology must be able to receive a request with sufficient information to uniquely identify a patient and return an ID or other token that can be used by an application to subsequently execute requests for that patient's data.

(ii) *Documentation.* (A) The API must include accompanying documentation that contains, at a minimum:

(*1*) API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.

(*2*) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).

(B) The documentation used to meet paragraph (g)(7)(ii)(A) of this section must be available via a publicly accessible hyperlink.

(8) *Application access—data category request.* The following technical outcome and conditions must be met through the demonstration of an application programming interface.

(i) *Functional requirements.* (A) Respond to requests for patient data (based on an ID or other token) for each of the individual data categories specified in the Common Clinical Data Set and return the full set of data for that data category (according to the specified standards, where applicable) in a computable format.

(B) Respond to requests for patient data associated with a specific date as well as requests for patient data within a specified date range.

(ii) *Documentation*—(A) The API must include accompanying documentation that contains, at a minimum:

(*1*) API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.

(*2*) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).

(B) The documentation used to meet paragraph (g)(8)(ii)(A) of this section must be available via a publicly accessible hyperlink.

(9) *Application access—all data request.* The following technical outcome and conditions must be met through the demonstration of an application programming interface.

(i) *Functional requirements.* (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.

(*3*) The following data classes:

(*i*) *Assessment and plan of treatment.* In accordance with the ''Assessment and Plan Section (V2)'' of the standards specified in §170.205(a)(4); or in accordance with the ''Assessment Section (V2)'' and ''Plan of Treatment Section (V2)'' of the standards specified in §170.205(a)(4).

(*ii*) *Goals.* In accordance with the ''Goals Section'' of the standards specified in §170.205(a)(4).

(*iii*) *Health concerns.* In accordance with the ''Health Concerns Section'' of the standards specified in §170.205(a)(4).

(*iv*) *Unique device identifier(s) for a patient's implantable device(s).* In accordance with the ''Product Instance'' in the ''Procedure Activity Procedure Section'' of the standards specified in §170.205(a)(4).

(B) Respond to requests for patient data associated with a specific date as well as requests for patient data within a specified date range.

(ii) *Documentation*—(A) The API must include accompanying documentation that contains, at a minimum:

(*1*) API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.

(*2*) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).

(B) The documentation used to meet paragraph (g)(9)(ii)(A) of this section must be available via a publicly accessible hyperlink.

(10) *Standardized API for patient and population services.* The following technical outcomes and conditions must be met through the demonstration of application programming interface technology.

(i) *Data response.* (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) *Supported search operations.* (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).

(iii) *Application registration.* Enable an application to register with the Health IT Module's ''authorization server.''

(iv) *Secure connection.* (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) *Authentication and authorization*—(A) *Authentication and authorization for patient and user scopes*—(*1*) *First time connections.* (*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).

(*iii*) A Health IT Module's authorization server must issue a refresh token for a period of no less than three months to native applications capable of securing a refresh token

(*2*) *Subsequent connections.* (*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).

(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.

(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).

(viii) *Documentation.* (A) The API(s) must include complete accompanying documentation that contains, at a minimum:

(*1*) API syntax, function names, required and optional parameters supported and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.

(*2*) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).

(*3*) All applicable technical requirements and attributes necessary for an application to be registered with a Health IT Module's authorization server.

(B) The documentation used to meet paragraph (g)(10)(viii)(A) of this section must be available via a publicly accessible hyperlink without any preconditions or additional steps.

(h) *Transport methods and other protocols*—(1) *Direct Project*—(i) *Applicability Statement for Secure Health Transport.* Able to send and receive health information in accordance with the standard specified in §170.202(a)(2), including formatted only as a ''wrapped'' message.

(ii) *Delivery Notification in Direct.* Able to send and receive health information in accordance with the standard specified in §170.202(e)(1).

(2) *Direct Project, Edge Protocol, and XDR/XDM.* (i) Able to send and receive health information in accordance with:

(A) The standard specified in §170.202(a)(2), including formatted only as a ''wrapped'' message;

(B) The standard specified in §170.202(b), including support for both limited and full XDS metadata profiles; and

(C) Both edge protocol methods specified by the standard in §170.202(d).

(ii) *Delivery Notification in Direct.* Able to send and receive health information in accordance with the standard specified in §170.202(e)(1).

[80 FR 62747, Oct. 16, 2015, as amended at 80 FR 76871, Dec. 11, 2015; 85 FR 25941, May 1, 2020; 85 FR 47099, Aug. 4, 2020; 85 FR 70083, Nov. 4, 2020; 85 FR 78236, Dec. 4, 2020; 89 FR 1429, Jan. 9, 2024; 89 FR 8548, Feb. 8, 2024; 89 FR 16470, Mar. 7, 2024]

Subpart D—Conditions and Maintenance of Certification Requirements for Health IT Developers

SOURCE: 85 FR 25945, May 1, 2020, unless otherwise noted.

§ 170.400 Basis and scope.

This subpart implements section 3001(c)(5)(D) of the Public Health Service Act by setting forth certain Conditions and Maintenance of Certification requirements for health IT developers participating in the ONC Health IT Certification Program.

§ 170.401 Information blocking.

(a) *Condition of Certification requirement.* A health IT developer must not take any action that constitutes information blocking as defined in 42 U.S.C. 300jj–52 and § 171.103 on or after April 5, 2021.

(b) [Reserved]

[85 FR 25945, May 1, 2020, as amended at 85 FR 70084, Nov. 4, 2020]

§ 170.402 Assurances.

(a) *Condition of Certification requirement.* (1) A health IT developer must provide assurances satisfactory to the Secretary that the health IT developer will not take any action that constitutes information blocking as defined in 42 U.S.C. 300jj–52 and § 171.103 of this chapter on and after April 5, 2021, unless for legitimate purposes as specified by the Secretary; or any other action that may inhibit the appropriate exchange, access, and use of electronic health information.

(2) A health IT developer must ensure that its health IT certified under the ONC Health IT Certification Program conforms to the full scope of the certification criteria.

(3) A health IT developer 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.

(4) A health IT developer of a certified Health IT Module that is part of a health IT product which electronically stores EHI must certify to the certification criterion in § 170.315(b)(10).

(5) A health IT developer must not inhibit its customer's timely access to interoperable health IT certified under the Program.

(b) *Maintenance of Certification requirements.* (1) A health IT developer must retain all records and information necessary to demonstrate initial and ongoing compliance with the requirements of the ONC Health IT Certification Program for:

(i) A period of 10 years beginning from the date a developer's Health IT Module(s) is first certified under the Program; or

(ii) If for a shorter period of time, a period of 3 years from the effective date that removes all of the certification criteria to which the developer's health IT is certified from the Code of Federal Regulations.

(2)(i) By December 31, 2023, a health IT developer that must comply with the requirements of paragraph (a)(4) of this section must provide all of its customers of certified health IT with the health IT certified to the certification criterion in § 170.315(b)(10).

(ii) On and after December 31, 2023, a health IT developer that must comply with the requirements of paragraph (a)(4) of this section must provide all of its customers of certified health IT with the health IT certified to the certification criterion in § 170.315(b)(10).

(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).

[85 FR 25945, May 1, 2020, as amended at 85 FR 70084, Nov. 4, 2020; 85 FR 70084, Nov. 4, 2020; 89 FR 1433, Jan. 9, 2024]

§170.403 Communications.

(a) *Condition of Certification requirements.* (1) A health IT developer may not prohibit or restrict any communication regarding—

(i) The usability of its health IT;

(ii) The interoperability of its health IT;

(iii) The security of its health IT;

(iv) Relevant information regarding users' experiences when using its health IT;

(v) The business practices of developers of health IT related to exchanging electronic health information; and

(vi) The manner in which a user of the health IT has used such technology.

(2) A health IT developer must not engage in any practice that prohibits or restricts a communication regarding the subject matters enumerated in paragraph (a)(1) of this section, unless the practice is specifically permitted by this paragraph and complies with all applicable requirements of this paragraph.

(i) *Unqualified protection for certain communications.* A health IT developer must not prohibit or restrict any person or entity from communicating any information whatsoever (including proprietary information, confidential information, and intellectual property) when the communication is about one or more of the subject matters enumerated in paragraph (a)(1) of this section and is made for any of the following purposes:

(A) Making a disclosure required by law;

(B) Communicating information about adverse events, hazards, and other unsafe conditions to government agencies, health care accreditation organizations, and patient safety organizations;

(C) Communicating information about cybersecurity threats and incidents to government agencies;

(D) Communicating information about information blocking and other unlawful practices to government agencies; or

(E) Communicating information about a health IT developer's failure to comply with a Condition of Certification requirement, or with any other requirement of this part, to ONC or an ONC–ACB.

(ii) *Permitted prohibitions and restrictions.* For communications about one or more of the subject matters enumerated in paragraph (a)(1) of this section that is not entitled to unqualified protection under paragraph (a)(2)(i) of this section, a health IT developer may prohibit or restrict communications only as expressly permitted by paragraphs (a)(2)(ii)(A) through (E) of this section.

(A) *Developer employees and contractors.* (*1*) A health IT developer may prohibit or restrict the communications of the developer's employees or contractors.

(*2*) A self-developer must not prohibit or restrict communications of users of their health IT who are also employees or contractors.

(B) *Non-user-facing aspects of health IT.* A health IT developer may prohibit or restrict communications that disclose information about non-user-facing aspects of the developer's health IT.

(C) *Intellectual property.* A health IT developer may prohibit or restrict communications that involve the use or disclosure of intellectual property existing in the developer's health IT (including third-party intellectual property), provided that any prohibition or restriction imposed by a developer must be no broader than necessary to protect the developer's legitimate intellectual property interests

and consistent with all other requirements of paragraph (a)(2)(ii) of this section. A restriction or prohibition is deemed broader than necessary and inconsistent with the requirements of paragraph (a)(2)(ii) of this section if it would restrict or preclude a public display of a portion of a work subject to copyright protection (without regard to whether the copyright is registered) that would reasonably constitute a ''fair use'' of that work.

(D) *Screenshots and video.* A health IT developer may require persons who communicate screenshots or video to—

(*1*) Not alter the screenshots or video, except to annotate the screenshots or video or resize the screenshots or video;

(*2*) Limit the sharing of screenshots to the relevant number of screenshots needed to communicate about the health IT regarding one or more of the six subject areas in paragraph (a)(1) of this section; and

(*3*) Limit the sharing of video to:

(*i*) The relevant amount of video needed to communicate about the health IT regarding one or more of the six subject areas in paragraph (a)(1) of this section; and

(*ii*) Only videos that address temporal matters that cannot be communicated through screenshots or other forms of communication.

(E) *Pre-market testing and development.* A health IT developer may prohibit or restrict communications that disclose information or knowledge solely acquired in the course of participating in pre-market product development and testing activities carried out for the benefit of the developer or for the joint benefit of the developer and communicator. A developer must not, once the subject health IT is released or marketed for purposes other than product development and testing, and subject to the permitted prohibitions and restrictions described in paragraph (a)(2)(ii) of this section, prohibit or restrict communications about matters enumerated in paragraph (a)(1) of this section.

(b) *Maintenance of Certification requirements*—(1) *Notice.* Health IT developers must issue a written notice to all customers and those with which it has contracts or agreements containing provisions that contravene paragraph (a) of this section annually, beginning in calendar year 2021, until paragraph (b)(2)(ii) of this section is fulfilled, stating that any communication or contract provision that contravenes paragraph (a) of this section will not be enforced by the health IT developer.

(2) *Contracts and agreements.* (i) A health IT developer must not establish, renew, or enforce any contract or agreement that contravenes paragraph (a) of this section.

(ii) If a health IT developer has a contract or agreement in existence as of June 30, 2020, that contravenes paragraph (a) of this section, then the developer must amend the contract or agreement to remove or void the contractual provision that contravenes paragraph (a) of this section whenever the contract is next modified for other reasons or renewed.

(c) *Communication, defined.* ''Communication'' as used in this section means any communication, irrespective of the form or medium. The term includes visual communications, such as screenshots and video.

[85 FR 25945, May 1, 2020, as amended at 85 FR 43711, July 20, 2020; 85 FR 70084, Nov. 4, 2020]

§ 170.404 Application programming interfaces.

The following Condition and Maintenance of Certification requirements apply to developers of Health IT Modules certified to any of the certification criteria adopted in § 170.315(g)(7) through (10).

(a) *Condition of certification requirements*—(1) *General.* A Certified API Developer must publish APIs and allow electronic health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law, including providing access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws.

(2) *Transparency conditions*—(i) *Complete business and technical documentation.* A Certified API Developer must publish complete business and technical documentation, including the

documentation described in paragraph (a)(2)(ii) of this section, via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps.

(ii) *Terms and conditions*—(A) *Material information.* A Certified API Developer must publish all terms and conditions for its certified API technology, including any fees, restrictions, limitations, obligations, registration process requirements, or other similar requirements that would be:

(*1*) Needed to develop software applications to interact with the certified API technology;

(*2*) Needed to distribute, deploy, and enable the use of software applications in production environments that use the certified API technology;

(*3*) Needed to use software applications, including to access, exchange, and use electronic health information by means of the certified API technology;

(*4*) Needed to use any electronic health information obtained by means of the certified API technology;

(*5*) Used to verify the authenticity of API Users; and

(*6*) Used to register software applications.

(B) *API fees.* Any and all fees charged by a Certified API Developer for the use of its certified API technology must be described in detailed, plain language. The description of the fees must include all material information, including but not limited to:

(*1*) The persons or classes of persons to whom the fee applies;

(*2*) The circumstances in which the fee applies; and

(*3*) The amount of the fee, which for variable fees must include the specific variable(s) and methodology(ies) that will be used to calculate the fee.

(3) *Fees conditions*—(i) *General conditions*—(A) *All fees.* All fees related to certified API technology not otherwise permitted by this section are prohibited from being imposed by a Certified API Developer. The permitted fees in paragraphs (a)(3)(ii) and (iv) of this section may include fees that result in a reasonable profit margin in accordance with §171.302.

(B) *Permitted fees requirements.* For all permitted fees, a Certified API Developer must:

(*1*) Ensure that such fees are based on objective and verifiable criteria that are uniformly applied to all similarly situated API Information Sources and API Users;

(*2*) Ensure that such fees imposed on API Information Sources are reasonably related to the Certified API Developer's costs to supply certified API technology to, and if applicable, support certified API technology for, API Information Sources;

(*3*) Ensure that such fees to supply and, if applicable, support certified API technology are reasonably allocated among all similarly situated API Information Sources; and

(*4*) Ensure that such fees are not based on whether API Information Sources or API Users are competitors, potential competitors, or will be using the certified API technology in a way that facilitates competition with the Certified API Developer.

(C) *Prohibited fees.* A Certified API Developer is prohibited from charging fees for the following:

(*1*) Costs associated with intangible assets other than actual development or acquisition costs of such assets;

(*2*) Opportunity costs unrelated to the access, exchange, or use of electronic health information; and

(*3*) The permitted fees in this section cannot include any costs that led to the creation of intellectual property if the actor charged a royalty for that intellectual property pursuant to §171.303 and that royalty included the development costs for the creation of the intellectual property.

(D) *Record-keeping requirements.* A Certified API Developer must keep for inspection detailed records of any fees charged with respect to the certified API technology, the methodology(ies) used to calculate such fees, and the specific costs to which such fees are attributed.

(ii) *Permitted fee—development, deployment, and upgrades.* A Certified API Developer is permitted to charge fees to an API Information Source to recover the costs reasonably incurred by the

Certified API Developer to develop, deploy, and upgrade certified API technology.

(iii) *Permitted fee—recovering API usage costs.* A Certified API Developer is permitted to charge fees to an API Information Source related to the use of certified API technology. The fees must be limited to the recovery of incremental costs reasonably incurred by the Certified API Developer when it hosts certified API technology on behalf of the API Information Source.

(iv) *Permitted fee—value-added services.* A Certified API Developer is permitted to charge fees to an API User for value-added services related to certified API technology, so long as such services are not necessary to efficiently and effectively develop and deploy production-ready software that interacts with certified API technology.

(4) *Openness and pro-competitive conditions; general condition.* A Certified API Developer must grant an API Information Source the independent ability to permit an API User to interact with the certified API technology deployed by the API Information Source.

(*i*) *Non-discrimination.* (A) A Certified API Developer must provide certified API technology to an API Information Source on terms that are no less favorable than it provides to itself and its own customers, suppliers, partners, and other persons with whom it has a business relationship.

(B) The terms on which a Certified API Developer provides certified API technology must be based on objective and verifiable criteria that are uniformly applied to all substantially similar or similarly situated classes of persons and requests.

(C) A Certified API Developer must not offer different terms or services based on:

(*1*) Whether a competitive relationship exists or would be created;

(*2*) The revenue or other value that another party may receive from using the API technology.

(ii) *Rights to access and use certified API technology*—(A) *Rights that must be granted.* A Certified API Developer must have and, upon request, must grant to API Information Sources and API Users all rights that may be reasonably necessary to:

(*1*) Access and use the Certified API Developer's certified API technology in a production environment;

(*2*) Develop products and services that are designed to interact with the Certified API Developer's certified API technology; and

(*3*) Market, offer, and distribute products and services associated with the Certified API Developer's certified API technology.

(B) *Prohibited conduct.* A Certified API Developer is prohibited from conditioning the receipt of the rights described in paragraph (a)(4)(ii)(A) of this section on:

(*1*) Receiving a fee, including but not limited to a license fee, royalty, or revenue-sharing arrangement;

(*2*) Agreeing to not compete with the Certified API Developer in any product, service, or market;

(*3*) Agreeing to deal exclusively with the Certified API Developer in any product, service, or market;

(*4*) Obtaining additional licenses, products, or services that are not related to or can be unbundled from the certified API technology;

(*5*) Licensing, granting, assigning, or transferring any intellectual property to the Certified API Developer;

(*6*) Meeting any Certified API Developer-specific testing or certification requirements; and.

(*7*) Providing the Certified API Developer or its technology with reciprocal access to application data.

(iii) *Service and support obligations.* A Certified API Developer must provide all support and other services reasonably necessary to enable the effective development, deployment, and use of certified API technology by API Information Sources and API Users in production environments.

(A) *Changes and updates to* certified *API technology.* A Certified API Developer must 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.

(B) *Changes to terms and conditions.* Except as exigent circumstances require, prior to making changes to its

certified API technology or to the terms and conditions thereof, a Certified API Developer must provide notice and a reasonable opportunity for API Information Sources and API Users to update their applications to preserve compatibility with certified API technology and to comply with applicable terms and conditions.

(b) *Maintenance of certification requirements*—(1) *Authenticity verification and registration for production use.* The following apply to a Certified API Developer with a Health IT Module certified to the certification criterion adopted in §170.315(g)(10):

(i) *Authenticity verification.* A Certified API Developer is permitted to institute a process to verify the authenticity of API Users so long as such process is objective and the same for all API Users and completed within ten business days of receipt of an API User's request to register their software application for use with the Certified API Developer's Health IT Module certified to §170.315(g)(10).

(ii) *Registration for production use.* A Certified API Developer must register and enable all applications for production use within five business days of completing its verification of an API User's authenticity, pursuant to paragraph (b)(1)(i) of this section.

(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.

(3) *Rollout of (g)(10)-certified APIs.* A Certified API Developer with certified API technology previously certified to the certification criterion in §170.315(g)(8) must provide all API Information Sources with such certified API technology deployed with certified API technology certified to the certification criterion in §170.315(g)(10) by no later than December 31, 2022.

(4) *Compliance for existing certified API technology.* By no later than April 5, 2021, a Certified API Developer with Health IT Module(s) certified to the certification criteria in §170.315(g)(7), (8), or (9) must comply with paragraph (a) of this section, including revisions to their existing business and technical API documentation and make such documentation available via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps.

(c) *Definitions.* The following definitions apply to this section:

API Information Source means an organization that deploys certified API technology created by a ''Certified API Developer;''

API User means 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;''

Certified API Developer means a health IT developer that creates the ''certified API technology'' that is certified to any of the certification criteria adopted in §170.315(g)(7) through (10); and

Certified API technology means the capabilities of Health IT Modules that are certified to any of the API-focused certification criteria adopted in §170.315(g)(7) through (10).

[85 FR 25945, May 1, 2020, as amended at 85 FR 70084, Nov. 4, 2020; 89 FR 1433, Jan. 9, 2024]

§ 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) *Maintenance of Certification requirements*—(1) *Real world testing plan submission.* A health IT developer with Health IT Module(s) certified to any one or more of the criteria referenced in paragraph (a) of this section must submit to its ONC–ACB an annual real world testing plan addressing each of those certified Health IT Modules by a date determined by the ONC–ACB that enables the ONC–ACB to publish a publicly available hyperlink to the plan on CHPL no later than December 15 of each calendar year, beginning in 2021.

(i) The plan must be approved by a health IT developer authorized representative capable of binding the health IT developer for execution of the plan and include the representative's contact information.

(ii) The plan must include all health IT certified to any one or more of the criteria referenced in paragraph (a) of this section as of August 31 of the year in which the plan is submitted, and address the real world testing to be conducted in the calendar year immediately following plan submission.

(iii) The plan must address the following for each of the certification criteria identified in paragraph (a) of this section that are included in each Health IT Module's scope of certification:

(A) The testing method(s)/methodology(ies) that will be used to demonstrate real world interoperability and conformance to the full scope of the certification criterion's requirements, including scenario- and use case-focused testing;

(B) The care setting(s) that will be tested for real world interoperability and an explanation for the health IT developer's choice of care setting(s) to test;

(C) For any standards and implementation specifications referenced by the criterion that the developer has chosen to certify to National Coordinator-approved newer versions pursuant to paragraph (b)(8) or (9) of this section, a description of how the developer will test and demonstrate conformance to all requirements of the criterion using all versions of the adopted standards to which each Health IT Module was certified as of August 31 of the year in which the real world testing plan is due.

(D) A schedule of key real world testing milestones;

(E) A description of the expected outcomes of real world testing;

(F) At least one measurement/metric associated with the real world testing; and

(G) A justification for the health IT developer's real world testing approach.

(2) *Real world testing results reporting.* (i) If in the course of conducting real world testing the developer discovers one or more non-conformities with the full scope of any certification criterion under the Program, the developer must report that non-conformity to the ONC–ACB within 30 days.

(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:

(A) The method(s) that was used to demonstrate real world interoperability;

(B) The care setting(s) that was tested for real world interoperability;

(C) The voluntary updates to standards and implementation specifications that the National Coordinator has approved through the Standards Version Advancement Process;

(D) A list of the key milestones met during real world testing;

(E) The outcomes of real world testing including a description of any challenges encountered during real world testing; and

(F) At least one measurement/metric associated with the real world testing.

(3)–(7) [Reserved]

(8) *Standards Version Advancement Process—voluntary updates of certified health IT to newer versions of standards and implementation specifications.* A health IT developer subject to this paragraph (b) is permitted to update Health IT Module(s) certified to any one or more of the certification criteria referenced in paragraph (a) of this section to a newer version of any adopted standard or implementation specification included in the criterion, provided that newer version is approved by the National Coordinator for use in certifications issued under the ONC Health IT Certification Program. A developer that pursues such updates to its certified Health IT Module(s) must:

(i) Provide advance notice to all affected customers and its ONC–ACB—

(A) Expressing its intent to update the certified Health IT Module(s) to the National Coordinator-approved advanced version of the standard implementation specification;

(B) The developer's expectations for how the update(s) will affect real world interoperability for the Health IT Module(s);

(C) Whether the developer intends to continue to support the certificate(s) for the existing certified Health IT Module(s) version(s) for some period of time and how long or if the existing certified Health IT Module(s) version(s) will be deprecated; and

(ii) Successfully demonstrate conformance with approved more recent versions of the standard(s) or implementation specification(s) included in each certification criterion under which the developer chooses to update its certified Health IT Module(s).

(iii) Maintain the updated certified Health IT Module(s) in full conformance with all applicable Program requirements.

(9) *Standards Version Advancement Process—voluntary certification to newer versions of standards and implementation specifications.* A Health IT developer is permitted to seek certification for its Health IT Module(s) to any one or more of the certification criteria referenced in paragraph (a) of this section using a newer version of any adopted standard(s) or implementation specification(s) included in the criterion without first obtaining certification to the version of that adopted standard or implementation specification that is incorporated by reference in §170.299, provided that the newer version is approved by the National Coordinator for use in certifications issued under the ONC Health IT Certification Program. Developers may, for each standard and implementation specification included in each criterion, choose on an itemized basis whether to seek certification to the version incorporated by reference in §170.299, or to one or more newer version(s) approved by the National Coordinator for use in Health IT Module certifications issued pursuant to section 3001(c)(5) of the Public Health Service Act, or to both.

(10) [Reserved]

[85 FR 25945, May 1, 2020, as amended at 85 FR 43711, July 20, 2020; 85 FR 70084, Nov. 4, 2020; 85 FR 78236, Dec. 4, 2020; 89 FR 1434, Jan. 9, 2024]

§ 170.406 Attestations.

(a) *Condition of Certification requirement.* A health IT developer, or its authorized representative that is capable of binding the health IT developer,

must provide the Secretary an attestation of compliance with the following Conditions and Maintenance of Certification requirements:

(1) Section 170.401;

(2) Section 170.402, but only for §170.402(a)(4) and (b)(2) if the health IT developer certified a Health IT Module(s) that is part of a health IT product which can store electronic health information;

(3) Section 170.403;

(4) Section 170.404 if the health IT developer has a Health IT Module(s) certified to any of the certification criteria adopted in §170.315(g)(7) through (10); and such health IT developer must also ensure that health IT allows for health information to be exchanged, accessed, and used, in the manner described in §170.404; and

(5) Section 170.405 if a health IT developer has a Health IT Module(s) certified to any one or more ONC Certification Criteria for Health IT in §170.315(b), (c)(1) through (3), (e)(1), (f), (g)(7) through (10), and (h).

(b) *Maintenance of Certification requirement*. (1) A health IT developer, or its authorized representative that is capable of binding the health IT developer, must provide the attestation specified in paragraph (a) of this section semiannually for any Health IT Modules that have or have had an active certification at any time under the ONC Health IT Certification Program during the prior six months.

(2) [Reserved][85 FR 25945, May 1, 2020, as amended at 89 FR 8549, Feb. 8, 2024]

§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.* 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 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.* 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.* 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.* 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.

(ii) [Reserved]

(2) [Reserved]

[89 FR 1434, Jan. 9, 2024; 89 FR 16470, Mar. 7, 2024]

Subpart E—ONC Health IT Certification Program

SOURCE: 76 FR 1325, Dec. 7, 2011, unless otherwise noted.

EDITORIAL NOTE: Nomenclature changes to subpart E of part 170 appear at 80 FR 62755, Oct. 16, 2015.

§170.500 Basis and scope.

This subpart implements section 3001(c)(5) of the Public Health Service Act and sets forth the rules and procedures related to the ONC Health IT Certification Program for health information technology (health IT) administered by the National Coordinator for Health Information Technology.

[76 FR 1325, Dec. 7, 2011, as amended at 77 FR 54291, Sept. 4, 2012]

§170.501 Applicability.

(a) This subpart establishes the processes that applicants for ONC–ACB status must follow to be granted ONC–ACB status by the National Coordinator; the processes the National Coordinator will follow when assessing applicants and granting ONC–ACB status;

the requirements that ONC–ACBs must follow to maintain ONC–ACB status; and the requirements of ONC–ACBs for certifying Health IT Module(s), and other types of health IT in accordance with the applicable certification criteria adopted by the Secretary in subpart C of this part.

(b) This subpart establishes the processes that applicants for ONC–ATL status must follow to be granted ONC–ATL status by the National Coordinator; the processes the National Coordinator will follow when assessing applicants and granting ONC–ATL status; the requirements that ONC–ATLs must follow to maintain ONC–ATL status; and the requirements of ONC–ATLs for testing Health IT Modules in accordance with the applicable certification criteria adopted by the Secretary in subpart C of this part.

(c) [Reserved]

(d) This subpart establishes the processes the National Coordinator will follow when exercising direct review of certified health IT and related requirements for ONC–ACBs, ONC–ATLs, and developers of health IT certified under the ONC Health IT Certification Program.

[81 FR 72464, Oct. 19, 2016, as amended at 85 FR 25950, May 1, 2020]

§ 170.502 Definitions.

For the purposes of this subpart:

Applicant means a single organization or a consortium of organizations that seeks to become an ONC–ACB or ONC–ATL by submitting an application to the National Coordinator for such status.

Deployment site means the physical location where a Health IT Module(s) or other type of health IT resides or is being or has been implemented.

Development site means the physical location where a Health IT Module(s) or other type of health IT was developed.

Gap certification means the certification of a previously certified Health IT Module(s) to:

(1) All applicable new and/or revised certification criteria adopted by the Secretary at subpart C of this part based on test results issued by a NVLAP-accredited testing laboratory under the ONC Health IT Certification Program or an ONC–ATL; and

(2) All other applicable certification criteria adopted by the Secretary at subpart C of this part based on the test results used to previously certify the Complete EHR or Health IT Module(s) under the ONC Health IT Certification Program.

ONC–Authorized Certification Body or ONC–ACB means an organization or a consortium of organizations that has applied to and been authorized by the National Coordinator pursuant to this subpart to perform the certification of Health IT Module(s), and/or other types of health IT under the ONC Health IT Certification Program.

ONC-Authorized Testing Lab or ONC–ATL means an organization or a consortium of organizations that has applied to and been authorized by the National Coordinator pursuant to this subpart to perform the testing of Health IT Modules to certification criteria adopted by the Secretary at subpart C of this part.

Providing or provide an updated certification means the action taken by an ONC–ACB to ensure that the developer of a previously certified Health IT Module(s) shall update the information required by § 170.523(k)(1)(i), after the ONC–ACB has verified that the certification criterion or criteria to which the Health IT Module(s) was previously certified have not been revised and that no new certification criteria are applicable to the Health IT Module(s).

Remote certification means the use of methods, including the use of web-based tools or secured electronic transmissions, that do not require an ONC–ACB to be physically present at the development or deployment site to conduct certification.

[76 FR 1325, Dec. 7, 2011, as amended at 77 FR 54291, Sept. 4, 2012; 81 FR 72464, Oct. 19, 2016; 85 FR 25950, May 1, 2020]

§§ 170.503–170.504 [Reserved]

§ 170.505 Correspondence.

(a) Correspondence and communication with ONC or the National Coordinator shall be conducted by email, unless otherwise necessary or specified.

(1) Consideration for providing notice beyond email, such as by regular, express, or certified mail, will be based on, but not limited to, whether: The party requests use of correspondence beyond email; the party has responded via email to our communications; we have sufficient information from the party to ensure appropriate delivery of any other method of notice; and the matter involves an alleged violation within ONC's purview under §170.580 that indicates a serious violation under the ONC Health IT Certification Program with potential consequences of suspension, certification termination, or a certification ban.

(2) The official date of receipt of any email between ONC or the National Coordinator and an applicant for ONC–ACB status, an applicant for ONC–ATL status, an ONC–ACB, an ONC–ATL, health IT developer, or a party to any proceeding under this subpart is the date on which the email was sent.

(b) In circumstances where it is necessary for an applicant for ONC–ACB status, an applicant for ONC–ATL status, an ONC–ACB, an ONC–ATL, health IT developer, or a party to any proceeding under this subpart to correspond or communicate with ONC or the National Coordinator by regular, express, or certified mail, the official date of receipt for all parties will be the date of the delivery confirmation to the address on record.

[85 FR 25950, May 1, 2020]

§ 170.510 Authorization scope for ONC–ACB status.

Applicants for ONC–ACB status may seek authorization from the National Coordinator to perform the following types of certification:

(a) Health IT Module certification; and/or

(b) Certification of other types of health IT for which the Secretary has adopted certification criteria under subpart C of this part.

[76 FR 1325, Dec. 7, 2011, as amended at 81 FR 72464, Oct. 19, 2016; 85 FR 25950, May 1, 2020]

§ 170.511 Authorization scope for ONC–ATL status.

Applicants may seek authorization from the National Coordinator to perform the testing of Complete EHRs or Health IT Modules to a portion of a certification criterion, one certification criterion, or many or all certification criteria adopted by the Secretary under subpart C of this part.

[81 FR 72464, Oct. 19, 2016]

§ 170.520 Application.

(a) *ONC–ACB application.* Applicants must include the following information in an application for ONC–ACB status and submit it to the National Coordinator for the application to be considered complete.

(1) The type of authorization sought pursuant to §170.510. For authorization to perform Health IT Module certification, applicants must indicate the specific type(s) of Health IT Module(s) they seek authorization to certify. If qualified, applicants will only be granted authorization to certify the type(s) of Health IT Module(s) for which they seek authorization.

(2) General identifying, information including:

(i) Name, address, city, state, zip code, and Web site of applicant; and

(ii) Designation of an authorized representative, including name, title, phone number, and email address of the person who will serve as the applicant's point of contact.

(3) Documentation that confirms that the applicant has been accredited to ISO/IEC 17065 (for availability, see §170.599), with an appropriate scope, by any accreditation body that is a signatory to the Multilateral Recognition Arrangement (MLA) with the International Accreditation Forum (IAF).

(4) An agreement, properly executed by the applicant's authorized representative, that it will adhere to the Principles of Proper Conduct for ONC–ACBs.

(b) *ONC–ATL application.* Applicants must include the following information in an application for ONC–ATL status and submit it to the National Coordinator for the application to be considered complete.

(1) The authorization scope sought pursuant to §170.511.

(2) General identifying, information including:

(i) Name, address, city, state, zip code, and Web site of applicant; and

(ii) Designation of an authorized representative, including name, title, phone number, and email address of the person who will serve as the applicant's point of contact.

(3) Documentation that confirms that the applicant has been accredited by NVLAP to the ONC Health IT Certification Program, including to ISO/IEC 17025 (incorporated by reference, *see* § 170.599).

(4) An agreement, properly executed by the applicant's authorized representative, that it will adhere to the Principles of Proper Conduct for ONC–ATLs.

[81 FR 72464, Oct. 19, 2016, as amended at 85 FR 25950, May 1, 2020]

§ 170.523 Principles of proper conduct for ONC–ACBs.

An ONC–ACB shall:

(a) *Accreditation.* Maintain its accreditation in good standing to ISO/IEC 17065 (incorporated by reference in § 170.599).

(b) *Mandatory training.* Attend all mandatory ONC training and program update sessions;

(c) *Training program.* Maintain a training program that includes documented procedures and training requirements to ensure its personnel are competent to certify health IT;

(d) *Reporting.* Report to ONC within 15 days any changes that materially affect its:

(1) Legal, commercial, organizational, or ownership status;

(2) Organization and management including key certification personnel;

(3) Policies or procedures;

(4) Location;

(5) Personnel, facilities, working environment or other resources;

(6) ONC authorized representative (point of contact); or

(7) Other such matters that may otherwise materially affect its ability to certify health IT.

(e) *Onsite observation.* Allow ONC, or its authorized agent(s), to periodically observe on site (unannounced or scheduled), during normal business hours, any certifications performed to demonstrate compliance with the requirements of the ONC Health IT Certification Program;

(f) *Certified product listing.* Provide ONC, no less frequently than weekly, a current list of Health IT Modules, and/or EHR Modules that have been certified that includes, at a minimum:

(1) For the ONC Certification Criteria for Health IT:

(i) The Health IT Module developer name; product name; product version; developer Web site, physical address, email, phone number, and contact name;

(ii) The ONC–ACB Web site, physical address, email, phone number, and contact name, contact function/title;

(iii) The ATL Web site, physical address, email, phone number, and contact name, contact function/title;

(iv) Location and means by which the testing was conducted (*e.g.*, remotely with health IT developer at its headquarters location);

(v) The date(s) the Health IT Module was tested;

(vi) The date the Health IT Module was certified;

(vii) The unique certification number or other specific product identification;

(viii) The certification criterion or criteria to which the Health IT Module has been certified, including the test procedure and test data versions used, test tool version used, and whether any test data was altered (*i.e.*, a yes/no) and for what purpose;

(ix) The way in which each privacy and security criterion was addressed for the purposes of certification;

(x) The standard or mapping used to meet the quality management system certification criterion;

(xi) The standard(s) or lack thereof used to meet the accessibility-centered design certification criterion;

(xii) *Where applicable,* the hyperlink to access an application programming interface (API)'s documentation and terms of use;

(xiii) *Where applicable,* which certification criteria were gap certified;

(xiv) *Where applicable,* if a certification issued was a result of an inherited certified status request;

(xv) *Where applicable,* the clinical quality measures to which the Health IT Module has been certified;

(xvi) *Where applicable,* any additional software a Health IT Module relied upon to demonstrate its compliance

with a certification criterion or criteria adopted by the Secretary;

(xvii) *Where applicable*, the standard(s) used to meet a certification criterion where more than one is permitted;

(xviii) *Where applicable*, any optional capabilities within a certification criterion to which the Health IT Module was tested and certified;

(xix) *Where applicable*, and for each applicable certification criterion, all of the information required to be submitted by Health IT Module developers to meet the safety-enhanced design certification criterion. Each user-centered design element required to be reported must be at a granular level (*e.g.*, task success/failure));

(xx) A hyperlink to the disclosures required by §170.523(k)(1) for the Health IT Module;

(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.

(xxii) *When applicable*, for each instance in which a Health IT Module failed to conform to its certification and for which corrective action was instituted under §170.556 (provided no provider or practice site is identified):

(A) The specific certification requirements to which the technology failed to conform, as determined by the ONC–ACB;

(B) A summary of the deficiency or deficiencies identified by the ONC–ACB as the basis for its determination of non-conformity;

(C) When available, the health IT developer's explanation of the deficiency or deficiencies;

(D) The dates surveillance was initiated and completed;

(E) The results of randomized surveillance, including pass rate for each criterion in instances where the Health IT Module is evaluated at more than one location;

(F) The number of sites that were used in randomized surveillance;

(G) The date of the ONC–ACB's determination of non-conformity;

(H) The date on which the ONC–ACB approved a corrective action plan;

(I) The date corrective action began (effective date of approved corrective action plan);

(J) The date by which corrective action must be completed (as specified by the approved corrective action plan);

(K) The date corrective action was completed; and

(L) A description of the resolution of the non-conformity or non-conformities.

(2) [Reserved]

(g) *Records retention*. (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

(2) Make the records available to HHS upon request during the retention period described in paragraph (g)(1) of this section;

(h) *Certification decision*. Only certify Health IT Modules that have been:

(1) Tested, using test tools and test procedures approved by the National Coordinator, by an:

(i) ONC–ATL;

(ii) ONC–ATL, National Voluntary Laboratory Accreditation Program-accredited testing laboratory under the ONC Health IT Certification Program, and/or an ONC–ATCB for the purposes of performing gap certification; or

(2) Evaluated by it for compliance with a conformance method approved by the National Coordinator.

(i) *Surveillance*. Conduct surveillance of certified health IT in accordance with its accreditation, §170.556, and the following requirements:

(1) Submit an annual surveillance plan to the National Coordinator.

(2) Report, at a minimum, on a quarterly basis to the National Coordinator the results of its surveillance, including surveillance results that identify:

(i) The names of health IT developers;

(ii) Names of products and versions;

(iii) Certification criteria and ONC Health IT Certification Program requirements surveilled;

(iv) The type of surveillance (*i.e.*, reactive or randomized);

(v) The dates surveillance was initiated and completed; and

(vi) As applicable, the number of sites that were used in randomized surveillance.

(3) Annually submit a summative report of surveillance results to the National Coordinator.

(j) *Refunds.* Promptly refund any and all fees received for:

(1) Requests for certification that are withdrawn while its operations are suspended by the National Coordinator;

(2) Certifications that will not be completed as a result of its conduct; and

(3) Previous certifications that it performed if its conduct necessitates the recertification of Complete EHRs and/or Health IT Module(s);

(k) *Disclosures.* Ensure adherence to the following requirements when issuing any certification and during surveillance of Health IT Modules the ONC–ACB has certified.

(1) *Mandatory Disclosures.* A health IT developer must conspicuously include the following on its website and in all marketing materials, communications statements, and other assertions related to the Health IT Module's certification:

(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.

(iii) In plain language, a detailed description of all known material information concerning additional types of costs or fees that a user may be required to pay to implement or use the Health IT Module's capabilities, whether to meet provisions of HHS programs requiring the use of certified health IT or to achieve any other use within the scope of the health IT's certification. The additional types of costs or fees required to be disclosed include but are not limited to costs or fees (whether fixed, recurring, transaction-based, or otherwise) imposed by a health IT developer (or any third party from whom the developer purchases, licenses, or obtains any technology, products, or services in connection with its certified health IT) to purchase, license, implement, maintain, upgrade, use, or otherwise enable and support the use of capabilities to which health IT is certified; or in connection with any data generated in the course of using any capability to which health IT is certified.

(iv) The types of information required to be disclosed under paragraph (k)(iii) of this section include but are not limited to:

(A) Additional types of costs or fees (whether fixed, recurring, transaction-based, or otherwise) imposed by a health IT developer (or any third-party from whom the developer purchases, licenses, or obtains any technology, products, or services in connection with its certified health IT) to purchase, license, implement, maintain, upgrade, use, or otherwise enable and support the use of capabilities to which health IT is certified; or in connection with any data generated in the course of using any capability to which health IT is certified.

(B)–(C) [Reserved]

(v) Health IT self-developers are excluded from the requirements of paragraph (k)(1)(iii) of this section.

(2)–(3) [Reserved]

(4) A certification issued to a Health IT Module based solely on the applicable certification criteria adopted by the ONC Health IT Certification Program must be separate and distinct from any other certification(s) based on other criteria or requirements.

(l) *Certification and Design Mark.* Display the ONC Certified health IT Certification and Design Mark on all certifications issued under the ONC Health IT Certification Program in a manner that complies with the Criteria and Terms of Use for the ONC Certified

health IT Certification and Design Mark, and ensure that use of the mark by health IT developers whose products are certified under the ONC Health IT Certification Program is compliant with the Criteria and Terms of Use for the ONC Certified health IT Certification and Design Mark.

(m) *Adaptations and updates.* On a quarterly basis each calendar year, obtain a record of:

(1) All adaptations of certified Health IT Modules;

(2) All updates made to certified Health IT Modules affecting the capabilities in certification criteria to which the ''safety-enhanced design'' criteria apply;

(3) All uses cases for §170.315(d)(13);

(4) All updates made to certified Health IT Modules in compliance with §170.405(b)(3); and

(5) All updates to certified Health IT Modules and all certifications of Health IT Modules issued including voluntary use of newer standards versions per §170.405(b)(8) or (9). Record of these updates may be obtained by aggregation of ONC–ACB documentation of certification activity.

(n) *Complaints reporting.* Submit a list of complaints received to the National Coordinator on a quarterly basis each calendar year that includes the number of complaints received, the nature/substance of each complaint, and the type of complainant for each complaint.

(o) *Scope reduction.* Be prohibited from reducing the scope of a Health IT Module's certification when it is under surveillance or under a corrective action plan.

(p) *Real world testing.* (1) Review and confirm that applicable health IT developers submit real world testing plans in accordance with §170.405(b)(1).

(2) Review and confirm that applicable health IT developers submit real world testing results in accordance with §170.405(b)(2).

(3) Submit real world testing plans by December 15 of each calendar year and results by March 15 of each calendar year to ONC for public availability.

(q) *Attestations.* Review and submit health IT developer Conditions and Maintenance of Certification requirements attestations made in accordance with §170.406 to ONC for public availability.

(r) *Test results from ONC–ATLs.* Accept test results from any ONC–ATL that is:

(1) In good standing under the ONC Health IT Certification Program, and

(2) Compliant with its ISO/IEC 17025 accreditation requirements as required by 170.524(a).

(s) *Information for direct review.* Report to ONC, no later than a week after becoming aware of, any information that could inform whether ONC should exercise direct review under §170.580(a).

(t) *Health IT Module voluntary standards and implementation specifications updates notices.* Ensure health IT developers opting to take advantage of the flexibility for voluntary updates of standards and implementation specifications in certified Health IT Modules per §170.405(b)(8) provide timely advance written notice to the ONC–ACB and all affected customers.

(1) Maintain a record of the date of issuance and the content of developers' §170.405(b)(8) notices; and

(2) Timely post content or make publicly accessible via the CHPL each §170.405(b)(8) notice received, publicly on the CHPL attributed to the certified Health IT Module(s) to which it applies.

(u) *Insights.* Confirm that developers of certified health IT submit responses for Insights Conditions and Maintenance of Certification requirements in accordance with §170.407.

[76 FR 1325, Dec. 7, 2011, as amended at 76 FR 72642, Nov. 25, 2011; 77 FR 54291, Sept. 4, 2012; 79 FR 54479, Sept. 11, 2014; 80 FR 62755, Oct. 16, 2015; 80 FR 76872, Dec. 11, 2015; 81 FR 72465, Oct. 19, 2016; 85 FR 25950, May 1, 2020; 85 FR 70084, Nov. 4, 2020; 89 FR 1435, Jan. 9, 2024]

§170.524 Principles of proper conduct for ONC–ATLs.

An ONC–ATL shall:

(a) *Accreditation.* Maintain its NVLAP accreditation for the ONC Health IT Certification Program, including accreditation to ISO/IEC 17025 (incorporated by reference, *see* §170.599);

(b) *Mandatory training.* Attend all mandatory ONC training and program update sessions;

(c) *Training program.* Maintain a training program that includes documented procedures and training requirements to ensure its personnel are competent to test health IT;

(d) *Reporting.* Report to ONC within 15 days any changes that materially affect its:

(1) Legal, commercial, organizational, or ownership status;

(2) Organization and management including key testing personnel;

(3) Policies or procedures;

(4) Location;

(5) Personnel, facilities, working environment or other resources;

(6) ONC authorized representative (point of contact); or

(7) Other such matters that may otherwise materially affect its ability to test health IT.

(e) *Onsite observation.* Allow ONC, or its authorized agent(s), to periodically observe on site (unannounced or scheduled), during normal business hours, any testing performed pursuant to the ONC Health IT Certification Program;

(f) *Records retention.* (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

(2) Make the records available to HHS upon request during the retention period described in paragraph (f)(1) of this section;

(g) *Approved testing methods.* Only test health IT using test tools and test procedures approved by the National Coordinator; and

(h) *Refunds.* Promptly refund any and all fees received for:

(1) Requests for testing that are withdrawn while its operations are suspended by the National Coordinator;

(2) Testing that will not be completed as a result of its conduct; and

(3) Previous testing that it performed if its conduct necessitates the retesting of Health IT Modules.

[81 FR 72465, Oct. 19, 2016, as amended at 85 FR 25951, May 1, 2020; 89 FR 1435, Jan. 9, 2024]

§ 170.525 Application submission.

(a) An applicant for ONC–ACB or ONC–ATL status must submit its application either electronically via email (or Web site submission if available), or by regular or express mail.

(b) An application for ONC–ACB or ONC–ATL status may be submitted to the National Coordinator at any time.

[81 FR 72465, Oct. 19, 2016]

§ 170.530 Review of application.

(a) *Method of review and review timeframe.* (1) Applications will be reviewed in the order they are received.

(2) The National Coordinator is permitted up to 30 days from receipt to review an application that is submitted for the first time.

(b) *Application deficiencies.* (1) If the National Coordinator identifies an area in an application that requires the applicant to clarify a statement or correct an error or omission, the National Coordinator may contact the applicant to make such clarification or correction without issuing a deficiency notice. If the National Coordinator has not received the requested information after five days, the National Coordinator may issue a deficiency notice to the applicant.

(2) If the National Coordinator determines that deficiencies in the application exist, the National Coordinator will issue a deficiency notice to the applicant and return the application. The deficiency notice will identify the areas of the application that require additional information or correction.

(c) *Revised application.* (1) An applicant is permitted to submit a revised application in response to a deficiency notice. An applicant may request from the National Coordinator an extension for good cause of the 15-day period provided in paragraph (c)(2) of this section to submit a revised application.

(2) In order for an applicant to continue to be considered for ONC–ACB or ONC–ATL status, the applicant's revised application must address the specified deficiencies and be received by the National Coordinator within 15 days of the applicant's receipt of the deficiency notice, unless the National

Coordinator grants an applicant's request for an extension of the 15-day period based on a finding of good cause. If a good cause extension is granted, then the revised application must be received by the end of the extension period.

(3) The National Coordinator is permitted up to 15 days to review a revised application once it has been received and may request clarification of statements and the correction of errors or omissions in a revised application during this time period.

(4) If the National Coordinator determines that a revised application still contains deficiencies, the applicant will be issued a denial notice indicating that the applicant cannot reapply for ONC–ACB or ONC–ATL status for a period of six months from the date of the denial notice. An applicant may request reconsideration of this decision in accordance with §170.535.

(d) *Satisfactory application.* (1) An application will be deemed satisfactory if it meets all the application requirements, as determined by the National Coordinator.

(2) The National Coordinator will notify the applicant's authorized representative of its satisfactory application and its successful achievement of ONC–ACB or ONC–ATL status.

(3) Once notified by the National Coordinator of its successful achievement of ONC–ACB or ONC–ATL status, the applicant may represent itself as an ONC–ACB or ONC–ATL (as applicable) and begin certifying or testing (as applicable) health information technology consistent with its authorization.

[76 FR 1325, Dec. 7, 2011, as amended at 81 FR 72465, Oct. 19, 2016]

§ 170.535 ONC–ACB and ONC–ATL application reconsideration.

(a) *Basis for reconsideration request.* An applicant may request that the National Coordinator reconsider a denial notice only if the applicant can demonstrate that clear, factual errors were made in the review of its application and that the errors' correction could lead to the applicant obtaining ONC–ACB or ONC–ATL status.

(b) *Submission requirement.* An applicant is required to submit, within 15 days of receipt of a denial notice, a written statement to the National Coordinator contesting the decision to deny its application and explaining with sufficient documentation what factual error(s) it believes can account for the denial. If the National Coordinator does not receive the applicant's reconsideration request within the specified timeframe, its reconsideration request may be rejected.

(c) *Reconsideration request review.* If the National Coordinator receives a timely reconsideration request, the National Coordinator is permitted up to 15 days from the date of receipt to review the information submitted by the applicant and issue a decision.

(d) *Decision.* (1) If the National Coordinator determines that clear, factual errors were made during the review of the application and that correction of the errors would remove all identified deficiencies, the applicant's authorized representative will be notified of the National Coordinator's determination and the applicant's successful achievement of ONC–ACB or ONC–ATL status.

(2) If, after reviewing an applicant's reconsideration request, the National Coordinator determines that the applicant did not identify factual errors or that the correction of the factual errors would not remove all identified deficiencies in the application, the National Coordinator may reject the applicant's reconsideration request.

(3) *Final decision.* A reconsideration decision issued by the National Coordinator is final and not subject to further review.

[76 FR 1325, Dec. 7, 2011, as amended at 81 FR 72466, Oct. 19, 2016]

§ 170.540 ONC–ACB and ONC–ATL status.

(a) *Acknowledgement and publication.* The National Coordinator will acknowledge and make publicly available the names of ONC–ACBs and ONC–ATLs, including the date each was authorized and the type(s) of certification or scope of testing, respectively, each has been authorized to perform.

(b) *Representation.* Each ONC–ACB or ONC–ATL must prominently and unambiguously identify the scope of its authorization on its Web site and in all

marketing and communications statements (written and oral) pertaining to its activities under the ONC Health IT Certification Program.

(c) *Renewal.* An ONC–ACB or ONC–ATL is required to renew its status every three years. An ONC–ACB or ONC–ATL is required to submit a renewal request, containing any updates to the information requested in § 170.520, to the National Coordinator 60 days prior to the expiration of its status.

(d) *Expiration.* An ONC–ACB's or ONC–ATL's status will expire three years from the date it was granted by the National Coordinator unless it is renewed in accordance with paragraph (c) of this section.

[81 FR 72466, Oct. 19, 2016]

§ 170.545 [Reserved]

§ 170.550 Health IT Module certification.

(a) *Certification scope.* When certifying Health IT Module(s), an ONC–ACB must certify in accordance with the applicable certification criteria adopted by the Secretary at subpart C of this part.

(b) *Health IT product scope options.* An ONC–ACB must provide the option for an Health IT Module(s) to be certified solely to the applicable certification criteria adopted by the Secretary at subpart C of this part.

(c) *Gap certification.* An ONC–ACB may provide the option for and perform gap certification of previously certified Health IT Module(s).

(d) *Upgrades and enhancements.* An ONC–ACB may provide an updated certification to a previously certified Health IT Module(s).

(e) *Standards updates.* ONC–ACBs must provide an option for certification of Health IT Modules consistent with § 171.405(b)(7) or (8) to any one or more of the criteria referenced in § 170.405(a) based on newer versions of standards included in the criteria which have been approved by the National Coordinator for use in certification.

(f) [Reserved]

(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:

(1) Section 170.315(g)(3) if the Health IT Module is presented for certification to one or more listed certification criteria in § 170.315(g)(3);

(2) Section 170.315(g)(4);

(3) Section 170.315(g)(5); and

(4) Section 170.315(g)(6) if the Health IT Module is presented for certification with C–CDA creation capabilities within its scope. If the scope of certification sought includes multiple certification criteria that require C–CDA creation, § 170.315(g)(6) need only be tested in association with one of those certification criteria and would not be expected or required to be tested for each. If the scope of certification sought includes multiple certification criteria that require C–CDA creation, § 170.315(g)(6) need only be tested in association with one of those certification criteria and would not be expected or required to be tested for each so long as all applicable C–CDA document templates have been evaluated as part of § 170.315(g)(6) for the scope of the certification sought.

(5) Section 170.315(b)(10) when a health IT developer presents a Health IT Module for certification that can store electronic health information at the time of certification by the product, of which the Health IT Module is a part.

(h) *Privacy and security certification framework*—(1) *General rule.* When certifying a Health IT Module to the ONC Certification Criteria for Health IT, an ONC–ACB can only issue a certification to a Health IT Module if the privacy and security certification criteria in paragraphs (h)(3)(i) through (ix) of this section have also been met (and are included within the scope of the certification).

(2) *Testing.* In order to be issued a certification, a Health IT Module would only need to be tested once to each applicable privacy and security criterion in paragraphs (h)(3)(i) through (ix) of this section so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification, except for the following:

(i) A Health IT Module presented for certification to §170.315(e)(1) must be separately tested to §170.315(d)(9); and

(ii) A Health IT Module presented for certification to §170.315(e)(2) must be separately tested to §170.315(d)(9).

(3) *Applicability.* (i) Section 170.315(a)(1) through (3), (5), (12), (14), and (15) are also certified to the certification criteria specified in §170.315(d)(1) through (7), (d)(12), and (13).

(ii) Section 170.315(a)(4), (9), (10), and (13) are also certified to the certification criteria specified in §170.315(d)(1) through (3), and (d)(5) through (7), (d)(12), and (13).

(iii) Section 170.315(b)(1) through (3) and (6) through (9) are also certified to the certification criteria specified in §170.315(d)(1) through (3) and (d)(5) through (8), (12), and (13);

(iv) Section 170.315(c) is also certified to the certification criteria specified in §170.315(d)(1), (d)(2)(i)(A), (B), (d)(2)(ii) through (v), (d)(3), (5), (12), and (13);

(v) Section 170.315(e)(1) is also certified to the certification criteria specified in §170.315(d)(1) through (3), (5), (7), (9), (12), and (13);

(vi) Section 170.315(e)(2) and (3) is also certified to the certification criteria specified in §170.315(d)(1), (d)(2)(i)(A) and (B), (d)(2)(ii) through (v), (d)(3), (5), (9), (12), and (13);

(vii) Section 170.315(f) is also certified to the certification criteria specified in §170.315(d)(1) through (3), (7), (12), and (13);

(viii) Section 170.315(g)(7) through (10) is also certified to the certification criteria specified in §170.315(d)(1), (9), (12), and (13); and (d)(2)(i)(A) and (B), (d)(2)(ii) through (v), or (d)(10);

(ix) Section 170.315(h) is also certified to the certification criteria specified in §170.315(d)(1), (d)(2)(i)(A) and (B), (d)(2)(ii) through (v), (d)(3), (12), and (13); and

(i) [Reserved]

(j) *Direct Project transport method.* An ONC–ACB can only issue a certification to a Health IT Module for §170.315(h)(1) if the Health IT Module's certification also includes §170.315(b)(1).

(k) *Inherited certified status.* An ONC–ACB must accept requests for a newer version of a previously certified Health IT Module(s) to inherit the certified status of the previously certified Health IT Module(s) without requiring the newer version to be recertified.

(1) Before granting certified status to a newer version of a previously certified Health IT Module(s), an ONC–ACB must review an attestation submitted by the developer(s) of the Health IT Module(s) to determine whether any change in the newer version has adversely affected the Health IT Module(s)' capabilities for which certification criteria have been adopted.

(2) An ONC–ACB may grant certified status to a newer version of a previously certified Health IT Module(s) if it determines that the capabilities for which certification criteria have been adopted have not been adversely affected.

(l) *Conditions of certification attestations.* Ensure that the health IT developer of the Health IT Module has met its responsibilities under subpart D of this part.

(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:

(1) Section 170.315(a)(10) and (13) and §170.315(e)(2) for the period before January 1, 2022.

(2) Section 170.315(b)(6) for the period before December 31, 2023.

(3) Section 170.315(g)(8) for the period before December 31, 2022.

[76 FR 1325, Dec. 7, 2011, as amended at 77 FR 54291, Sept. 4, 2012; 79 FR 54480, Sept. 11, 2014; 80 FR 62757, Oct. 16, 2015; 85 FR 25952, May 1, 2020; 85 FR 70085, Nov. 4, 2020; 89 FR 1435, Jan. 9, 2024; 89 FR 8549, Feb. 8, 2024]

§170.553 [Reserved]

§170.555 Certification to newer versions of certain standards.

(a) ONC–ACBs may certify Health IT Module(s) to a newer version of certain identified minimum standards specified at subpart B of this part, unless the Secretary prohibits the use of a newer version for certification.

(b) *Applicability of a newer version of a minimum standard.* (1) ONC–ACBs are not required to certify Health IT Module(s) according to newer versions of

standards adopted and named in subpart B of this part, unless:

(i) The National Coordinator approves a newer version for use in certification and a health IT developer voluntarily elects to seek certification of its health IT in accordance with §170.405(b)(9) or update its certified health IT to the newer version in accordance with §170.405(b)(8); or

(ii) The new version is incorporated by reference in §170.299.

(2) A certified Complete EHR or certified Health IT Module may be upgraded to comply with newer versions of standards identified as minimum standards in subpart B of this part without adversely affecting its certification status, unless the Secretary prohibits the use of a newer version for certification.

[77 FR 54291, Sept. 4, 2012, as amended at 85 FR 25952, May 1, 2020]

§ 170.556 In-the-field surveillance and maintenance of certification for Health IT.

(a) *In-the-field surveillance.* Consistent with its accreditation under 170.523(a) to ISO/IEC 17065 and the requirements of this subpart, an ONC–ACB must initiate surveillance ''in the field'' as necessary to assess whether a certified Health IT Module continues to conform to the requirements in subparts A, B, C and E of this part once the certified Health IT Module has been implemented and is in use in a production environment.

(1) *Production environment.* An ONC–ACB's assessment of a certified capability in the field must be based on the use of the capability in a production environment, which means a live environment in which the capability has been implemented and is in use.

(2) *Production data.* An ONC–ACB's assessment of a certified capability in the field must be based on the use of the capability with production data unless the use of test data is specifically approved by the National Coordinator.

(b) *Reactive surveillance.* An ONC–ACB must initiate surveillance (including, as necessary, in-the-field surveillance required by paragraph (a) of this section) whenever it becomes aware of facts or circumstances that would cause a reasonable person to question a certified Health IT Module's continued conformity to the requirements of its certification.

(1) *Review of required disclosures.* When an ONC–ACB performs reactive surveillance under this paragraph, it must verify that the requirements of §170.523(k)(1) have been followed as applicable to the issued certification.

(2) [Reserved]

(c) *Randomized surveillance.* During each calendar year surveillance period, an ONC–ACB may conduct in-the-field surveillance for certain randomly selected Health IT Modules to which it has issued a certification.

(1) *Scope.* When an ONC–ACB selects a certified Health IT Module for randomized surveillance under this paragraph, its evaluation of the certified Health IT Module must include all certification criteria prioritized by the National Coordinator that are part of the scope of the certification issued to the Health IT Module.

(2) [Reserved]

(3) *Selection method.* An ONC–ACB must randomly select (subject to appropriate weighting and sampling considerations) and certified Health IT Modules for surveillance under this paragraph.

(4) *Number and types of locations for in-the-field surveillance.* For each certified Health IT Module selected for randomized surveillance under this paragraph, an ONC–ACB must:

(i) Evaluate the certified Health IT Module's capabilities at one or more locations where the certified Health IT Module is implemented and in use in the field.

(ii) Ensure that the locations are selected at random (subject to appropriate weighting and sampling considerations) from among all locations where the certified Health IT Module is implemented and in use in the field.

(d) *Corrective action plan and procedures.* (1) When an ONC–ACB determines, through surveillance under this section or otherwise, that a Health IT Module does not conform to the requirements of its certification, the ONC–ACB must notify the developer of its findings and require the developer to submit a proposed corrective action plan for the applicable certification

criterion, certification criteria, or certification requirement.

(2) The ONC–ACB shall provide direction to the developer as to the required elements of the corrective action plan.

(3) The ONC–ACB shall verify the required elements of the corrective action plan, consistent with its accreditation and any elements specified by the National Coordinator. At a minimum, any corrective action plan submitted by a developer to an ONC–ACB must include:

(i) A description of the identified non-conformities or deficiencies;

(ii) An assessment of how widespread or isolated the identified non-conformities or deficiencies may be across all of the developer's customers and users of the certified Health IT Module;

(iii) How the developer will address the identified non-conformities or deficiencies, both at the locations under which surveillance occurred and for all other potentially affected customers and users;

(iv) How the developer will ensure that all affected and potentially affected customers and users are alerted to the identified non-conformities or deficiencies, including a detailed description of how the developer will assess the scope and impact of the problem, including identifying all potentially affected customers; how the developer will promptly ensure that all potentially affected customers are notified of the problem and plan for resolution; how and when the developer will resolve issues for individual affected customers; and how the developer will ensure that all issues are in fact resolved.

(v) The timeframe under which corrective action will be completed.

(vi) An attestation by the developer that it has completed all elements of the approved corrective action plan.

(4) When the ONC–ACB receives a proposed corrective action plan (or a revised proposed corrective action plan), the ONC–ACB shall either approve the corrective action plan or, if the plan does not adequately address the elements described by paragraph (d)(3) of this section and other elements required by the ONC–ACB, instruct the developer to submit a revised proposed corrective action plan.

(5) *Suspension.* Consistent with its accreditation to ISO/IEC 17065 and procedures for suspending a certification, an ONC–ACB shall initiate suspension procedures for a Health IT Module:

(i) 30 days after notifying the developer of a non-conformity pursuant to paragraph (d)(1) of this section, if the developer has not submitted a proposed corrective action plan;

(ii) 90 days after notifying the developer of a non-conformity pursuant to paragraph (d)(1) of this section, if the ONC–ACB cannot approve a corrective action plan because the developer has not submitted a revised proposed corrective action plan in accordance with paragraph (d)(4) of this section; and

(iii) Immediately, if the developer has not completed the corrective actions specified by an approved corrective action plan within the time specified therein.

(6) *Withdrawal.* If a or certified Health IT Module's certification has been suspended, an ONC–ACB is permitted to initiate certification withdrawal procedures for the Health IT Module (consistent with its accreditation to ISO/IEC 17065 and procedures for withdrawing a certification) when the health IT developer has not completed the actions necessary to reinstate the suspended certification.

(e) *Reporting of surveillance results requirements*—(1) *Rolling submission of in-the-field surveillance results.* The results of in-the-field surveillance under this section must be submitted to the National Coordinator, at a minimum, on a quarterly basis in accordance with §170.523(i)(2).

(2) *Confidentiality of locations evaluated.* The contents of an ONC–ACB's surveillance results submitted to the National Coordinator must not include any information that would identify any user or location that participated in or was subject to surveillance.

(3) *Reporting of corrective action plans.* When a corrective action plan is initiated for a Health IT Module, an ONC–ACB must report the Health IT Module and associated product and corrective action information to the National Coordinator in accordance with

§ 170.523(f)(1)(xxii) or (f)(2)(xi), as applicable.

(f) *Relationship to other surveillance requirements.* Nothing in this section shall be construed to limit or constrain an ONC–ACB's duty or ability to perform surveillance, including in-the-field surveillance, or to suspend or terminate the certification, of any certified Health IT Module as required or permitted by this subpart and the ONC–ACB's accreditation to ISO/IEC 17065.

[80 FR 62758, Oct. 16, 2015, as amended at 80 FR 76872, Dec. 11, 2015; 81 FR 72466, Oct. 19, 2016; 85 FR 25952, May 1, 2020]

§ 170.557 Authorized testing and certification methods.

(a) *ONC–ATL applicability.* An ONC–ATL must provide remote testing for both development and deployment sites.

(b) *ONC–ACB applicability.* An ONC–ACB must provide remote certification for both development and deployment sites.

[81 FR 72466, Oct. 19, 2016]

§ 170.560 Good standing as an ONC–ACB or ONC–ATL.

(a) *ONC–ACB good standing.* An ONC–ACB must maintain good standing by:

(1) Adhering to the Principles of Proper Conduct for ONC–ACBs;

(2) Refraining from engaging in other types of inappropriate behavior, including an ONC–ACB misrepresenting the scope of its authorization, as well as an ONC–ACB certifying Health IT Module(s) for which it does not have authorization; and

(3) Following all other applicable federal and state laws.

(b) *ONC–ATL good standing.* An ONC–ATL must maintain good standing by:

(1) Adhering to the Principles of Proper Conduct for ONC–ATLs;

(2) Refraining from engaging in other types of inappropriate behavior, including an ONC–ATL misrepresenting the scope of its authorization, as well as an ONC–ATL testing health IT for which it does not have authorization; and

(3) Following all other applicable federal and state laws.

[81 FR 72466, Oct. 19, 2016; 85 FR 25953, May 1, 2020]

§ 170.565 Revocation of ONC–ACB or ONC–ATL status.

(a) *Type-1 violations.* The National Coordinator may revoke an ONC–ATL or ONC–ACB's status for committing a Type-1 violation. Type-1 violations include violations of law or ONC Health IT Certification Program policies that threaten or significantly undermine the integrity of the ONC Health IT Certification Program. These violations include, but are not limited to: False, fraudulent, or abusive activities that affect the ONC Health IT Certification Program, a program administered by HHS or any program administered by the federal government.

(b) *Type-2 violations.* The National Coordinator may revoke an ONC–ATL or ONC–ACB's status for failing to timely or adequately correct a Type-2 violation. Type-2 violations constitute noncompliance with § 170.560.

(1) *Noncompliance notification.* If the National Coordinator obtains reliable evidence that an ONC–ATL or ONC–ACB may no longer be in compliance with § 170.560, the National Coordinator will issue a noncompliance notification with reasons for the notification to the ONC–ATL or ONC–ACB requesting that the ONC–ATL or ONC–ACB respond to the alleged violation and correct the violation, if applicable.

(2) *Opportunity to become compliant.* After receipt of a noncompliance notification, an ONC–ATL or ONC–ACB is permitted up to 30 days to submit a written response and accompanying documentation that demonstrates that no violation occurred or that the alleged violation has been corrected.

(i) If the ONC–ATL or ONC–ACB submits a response, the National Coordinator is permitted up to 30 days from the time the response is received to evaluate the response and reach a decision. The National Coordinator may, if necessary, request additional information from the ONC–ATL or ONC–ACB during this time period.

(ii) If the National Coordinator determines that no violation occurred or that the violation has been sufficiently corrected, the National Coordinator will issue a memo to the ONC–ATL or ONC–ACB confirming this determination.

(iii) If the National Coordinator determines that the ONC–ATL or ONC–ACB failed to demonstrate that no violation occurred or to correct the area(s) of non-compliance identified under paragraph (b)(1) of this section within 30 days of receipt of the non-compliance notification, then the National Coordinator may propose to revoke the ONC–ATL or ONC–ACB's status.

(c) *Proposed revocation.* (1) The National Coordinator may propose to revoke an ONC–ATL or ONC–ACB's status if the National Coordinator has reliable evidence that the ONC–ATL or ONC–ACB has committed a Type-1 violation; or

(2) The National Coordinator may propose to revoke an ONC–ATL or ONC–ACB's status if, after the ONC–ATL or ONC–ACB has been notified of a Type-2 violation, the ONC–ATL or ONC–ACB fails to:

(i) Rebut the finding of a violation with sufficient evidence showing that the violation did not occur or that the violation has been corrected; or

(ii) Submit to the National Coordinator a written response to the non-compliance notification within the specified timeframe under paragraph (b)(2) of this section.

(d) *Suspension of an ONC–ATL or ONC–ACB's operations.* (1) The National Coordinator may suspend the operations of an ONC–ATL or ONC–ACB under the ONC Health IT Certification Program based on reliable evidence indicating that:

(i) *Applicable to both ONC–ACBs and ONC–ATLs.* The ONC–ATL or ONC–ACB committed a Type-1 or Type-2 violation;

(ii) *Applicable to ONC–ACBs.* The continued certification of Health IT Modules by the ONC–ACB could have an adverse impact on the health or safety of patients.

(iii) *Applicable to ONC–ATLs.* The continued testing of Health IT Modules by the ONC–ATL could have an adverse impact on the health or safety of patients.

(2) If the National Coordinator determines that the conditions of paragraph (d)(1) of this section have been met, an ONC–ATL or ONC–ACB will be issued a notice of proposed suspension.

(3) Upon receipt of a notice of proposed suspension, an ONC–ATL or ONC–ACB will be permitted up to 3 days to submit a written response to the National Coordinator explaining why its operations should not be suspended.

(4) The National Coordinator is permitted up to 5 days from receipt of an ONC–ATL or ONC–ACB's written response to a notice of proposed suspension to review the response and make a determination.

(5) The National Coordinator may make one of the following determinations in response to the ONC–ATL or ONC–ACB's written response or if the ONC–ATL or ONC–ACB fails to submit a written response within the timeframe specified in paragraph (d)(3) of this section:

(i) Rescind the proposed suspension; or

(ii) Suspend the ONC–ATL or ONC–ACB's operations until it has adequately corrected a Type-2 violation; or

(iii) Propose revocation in accordance with paragraph (c) of this section and suspend the ONC–ATL or ONC–ACB's operations for the duration of the revocation process.

(6) A suspension will become effective upon an ONC–ATL or ONC–ACB's receipt of a notice of suspension.

(e) *Opportunity to respond to a proposed revocation notice.* (1) An ONC–ATL or ONC–ACB may respond to a proposed revocation notice, but must do so within 10 days of receiving the proposed revocation notice and include appropriate documentation explaining in writing why its status should not be revoked.

(2) Upon receipt of an ONC–ATL or ONC–ACB's response to a proposed revocation notice, the National Coordinator is permitted up to 30 days to review the information submitted by the ONC–ACB or ONC–ATL and reach a decision.

(f) *Good standing determination.* If the National Coordinator determines that an ONC–ATL or ONC–ACB's status should not be revoked, the National Coordinator will notify the ONC–ATL or ONC–ACB's authorized representative in writing of this determination.

(g) *Revocation.* (1) The National Coordinator may revoke an ONC–ATL or ONC–ACB's status if:

(i) A determination is made that revocation is appropriate after considering the information provided by the ONC–ATL or ONC–ACB in response to the proposed revocation notice; or

(ii) The ONC–ATL or ONC–ACB does not respond to a proposed revocation notice within the specified timeframe in paragraph (e)(1) of this section.

(2) A decision to revoke an ONC–ATL or ONC–ACB's status is final and not subject to further review unless the National Coordinator chooses to reconsider the revocation.

(h) *Extent and duration of revocation*—(1) *Effectuation.* The revocation of an ONC–ATL or ONC–ACB is effective as soon as the ONC–ATL or ONC–ACB receives the revocation notice.

(2) *ONC–ACB provisions.* (i) A certification body that has had its ONC–ACB status revoked is prohibited from accepting new requests for certification and must cease its current certification operations under the ONC Health IT Certification Program.

(ii) A certification body that has had its ONC–ACB status revoked for a Type-1 violation is not permitted to reapply for ONC–ACB status under the ONC Health IT Certification Program for a period of 1 year.

(iii) The failure of a certification body that has had its ONC–ACB status revoked to promptly refund any and all fees for certifications of Health IT Module(s) not completed will be considered a violation of the Principles of Proper Conduct for ONC–ACBs and will be taken into account by the National Coordinator if the certification body reapplies for ONC–ACB status under the ONC Health IT Certification Program.

(3) *ONC–ATL provisions.* (i) A testing lab that has had its ONC–ATL status revoked is prohibited from accepting new requests for testing and must cease its current testing operations under the ONC Health IT Certification Program.

(ii) A testing lab that has had its ONC–ATL status revoked for a Type-1 violation is not permitted to reapply for ONC–ATL status under the ONC Health IT Certification Program for a period of 1 year.

(iii) The failure of a testing lab that has had its ONC–ATL status revoked to promptly refund any and all fees for testing of health IT not completed will be considered a violation of the Principles of Proper Conduct for ONC–ATLs and will be taken into account by the National Coordinator if the testing lab reapplies for ONC–ATL status under the ONC Health IT Certification Program.

[81 FR 72466, Oct. 19, 2016, as amended at 85 FR 25953, May 1, 2020]

§ 170.570 Effect of revocation on the certifications issued to Complete EHRs and EHR Module(s).

(a) The certified status of Health IT Module(s) certified by an ONC–ACB or tested by an ONC–ATL that had its status revoked will remain intact unless a Type-1 violation was committed by the ONC–ACB and/or ONC–ATL that calls into question the legitimacy of the certifications issued.

(b) If the National Coordinator determines that a Type-1 violation was committed by an ONC–ACB and/or ONC–ATL that called into question the legitimacy of certifications issued to health IT, then the National Coordinator would:

(1) Review the facts surrounding the revocation of the ONC–ACB's or ONC–ATL's status; and

(2) Publish a notice on ONC's Web site if the National Coordinator believes that the Health IT Module(s) certifications were based on unreliable testing and/or certification.

(c) If the National Coordinator determines that Health IT Module(s) certifications were based on unreliable testing and/or certification, the certification status of affected Health IT Module(s) would only remain intact for 120 days after the National Coordinator publishes the notice.

(1) The certification status of affected Health IT Module(s) can only be maintained after the 120-day timeframe by being re-tested by an ONC–ATL in good standing, as necessary, and re-certified by an ONC–ACB in good standing.

(2) The National Coordinator may extend the time that the certification

status of affected Health IT Module(s) remains intact as necessary for the proper retesting and recertification of the affected health IT.

[81 FR 72467, Oct. 19, 2016, as amended at 85 FR 25953, May 1, 2020]

§ 170.575 [Reserved]

§ 170.580 ONC review of certified health IT.

(a) *Direct review*—(1) *Purpose.* ONC may directly review certified health IT or a health IT developer's actions or practices to determine whether either conform to the requirements of the ONC Health IT Certification Program.

(2) *Circumstances that may trigger review*—(i) *Certified health IT causing or contributing to unsafe conditions.* ONC may initiate direct review under this section if it has a reasonable belief that certified health IT may not conform to the requirements of the Program because the certified health IT may be causing or contributing to conditions that present a serious risk to public health or safety, taking into consideration—

(A) The potential nature, severity, and extent of the suspected conditions;

(B) The need for an immediate or coordinated governmental response; and

(C) If applicable, information that calls into question the validity of the health IT's certification or maintenance thereof under the Program.

(ii) *Impediments to ONC–ACB oversight of certified health IT.* ONC may initiate direct review under this section if it has a reasonable belief that certified health IT may not conform to requirements of the Program and the suspected non-conformity presents issues that—

(A) May require access to confidential or other information that is not available to an ONC–ACB;

(B) May require concurrent or overlapping review by two or more ONC–ACBs; or

(C) May exceed an ONC–ACB's resources or expertise.

(iii) *Noncompliance with a Condition and Maintenance of Certification requirement.* ONC may initiate direct review under this section if it has a reasonable belief that a health IT developer has not complied with a Condition or Maintenance of Certification requirement under subpart D of this part.

(3) *Relationship to ONC–ACBs and ONC–ATLs.* (i) ONC's review of certified health IT or a health IT developer's actions or practices is independent of, and may be in addition to, any surveillance of certified health IT conducted by an ONC–ACB.

(ii) ONC may assert exclusive review of certified health IT as to any matters under review by ONC and any similar matters under surveillance by an ONC–ACB.

(iii) ONC's determination on matters under its review is controlling and supersedes any determination by an ONC–ACB on the same matters.

(iv) An ONC–ACB and ONC–ATL shall provide ONC with any available information that ONC deems relevant to its review of certified health IT or a health IT developer's actions or practices.

(v) ONC may end all or any part of its review of certified health IT or a health IT developer's actions or practices under this section at any time and refer the applicable part of the review to the relevant ONC–ACB(s) if ONC determines that doing so would serve the effective administration or oversight of the ONC Health IT Certification Program.

(4) *Coordination with the Office of Inspector General.* (i) ONC may coordinate its review of a claim of information blocking with the Office of Inspector General or defer to the Office of Inspector General to lead a review of a claim of information blocking.

(ii) ONC may rely on Office of Inspector General findings to form the basis of a direct review action.

(b) *Notice*—(1) *Notice of potential non-conformity*—(i) *Circumstances that may trigger notice of potential non-conformity.* At any time during its review of certified health IT or a health IT developer's actions or practices under paragraph (a) of this section, ONC may send a notice of potential non-conformity if it has a reasonable belief that certified health IT or a health IT developer's actions or practices may not conform to the requirements of the ONC Health IT Certification Program.

(ii) *Health IT developer response.* (A) The health IT developer must respond

to the notice of potential non-conformity by:

(*1*) Cooperating with ONC and/or a third party acting on behalf of ONC;

(*2*) Providing ONC and/or a third party acting on behalf of ONC access, including in accordance with paragraph (b)(3) of this section, to the certified health IT under review;

(*3*) Providing ONC with a written explanation and all supporting documentation addressing the potential non-conformity within 30 days, or within the adjusted timeframe set in accordance with paragraph (b)(1)(ii)(B) of this section.

(B) ONC may adjust the 30-day timeframe specified in paragraph (b)(1)(ii)(A)(*3*) of this section to be shorter or longer based on factors including, but not limited to:

(*1*) The type of certified health IT and certification in question;

(*2*) The type of potential non-conformity to be corrected;

(*3*) The time required to correct the potential non-conformity; and

(*4*) Issues of public health or safety.

(iii) *ONC determination.* After receiving the health IT developer's written explanation and supporting documentation as required by paragraph (b)(1)(ii)(A)(*3*) of this section, ONC shall do one of the following:

(A) Issue a written determination ending its review.

(B) Request additional information and continue its review in accordance with a new timeframe ONC establishes under (b)(1)(ii)(A)(*3*) and (b)(1)(ii)(B) of this section.

(C) Substantiate a non-conformity and issue a notice of non-conformity.

(D) Issue a notice of proposed termination if the health IT is under review in accordance with paragraph (a)(2)(i) or (ii) of this section.

(2) *Notice of non-conformity*—(i) *Circumstances that may trigger notice of non-conformity.* At any time during its review of certified health IT or a health IT developer's actions or practices under paragraph (a) of this section, ONC may send a notice of non-conformity to the health IT developer if it determines that certified health IT or a health IT developer's actions or practices does not conform to the requirements of the ONC Health IT Certification Program.

(ii) *Health IT developer response.* (A) The health IT developer must respond to the notice of non-conformity by:

(*1*) Cooperating with ONC and/or a third party acting on behalf of ONC;

(*2*) Providing ONC and/or a third party acting on behalf of ONC access, including in accordance with paragraph (b)(3) of this section, to the certified health IT under review;

(*3*) Providing ONC with a written explanation and all supporting documentation addressing the non-conformity within 30 days, or within the adjusted timeframe set in accordance with paragraph (b)(1)(ii)(B) of this section; and

(*4*) Providing a proposed corrective action plan consistent with paragraph (c) of this section.

(B) ONC may adjust the 30-day timeframe specified in paragraph (b)(2)(ii)(A)(*3*) of this section to be shorter or longer based on factors including, but not limited to:

(*1*) The type of certified health IT and certification in question;

(*2*) The type of non-conformity to be corrected;

(*3*) The time required to correct the non-conformity; and

(*4*) Issues of public health or safety.

(iii) *ONC determination.* After receiving the health IT developer's response provided in accordance with paragraph (b)(2)(ii) of this section, ONC shall either issue a written determination ending its review or continue with its review under the provisions of this section.

(3) *Records access.* In response to a notice of potential non-conformity or notice of non-conformity, a health IT developer shall make available to ONC and for sharing within HHS, with other federal departments, agencies, and offices, and with appropriate entities including, but not limited to, third-parties acting on behalf of ONC:

(i) All records related to the development, testing, certification, implementation, maintenance and use of its certified health IT;

(ii) Any complaint records related to the certified health IT;

(iii) All records related to the Condition(s) and Maintenance of Certification requirements, including marketing and distribution records, communications, and contracts; and

(iv) Any other relevant information.

(c) *Corrective action plan and procedures*—(1) *Applicability.* If ONC determines that certified health IT or a health IT developer's action or practice does not conform to requirements of the ONC Health IT Certification Program, ONC shall notify the health IT developer of its determination and require the health IT developer to submit a proposed corrective action plan.

(2) ONC shall provide direction to the health IT developer as to the required elements of the corrective action plan, which shall include such required elements as ONC determines necessary to comprehensively and expeditiously resolve the identified non-conformity(ies). The corrective action plan shall, in all cases, at a minimum include the following required elements:

(i) An assessment and description of the nature, severity, and extent of the non-conformity;

(ii) Identification of all potentially affected customers;

(iii) A detailed description of how the health IT developer will promptly ensure that all potentially affected customers are notified of the non-conformity and plan for resolution;

(iv) A detailed description of how and when the health IT developer will resolve the identified non-conformity and all issues, both at the locations where the non-conformity was identified and for all affected customers;

(v) A detailed description of how the health IT developer will ensure that the identified non-conformity and all issues are resolved;

(vi) A detailed description of the supporting documentation that will be provided to demonstrate that the identified non-conformity and all issues are resolved; and

(vii) The timeframe under which all elements of the corrective action plan will be completed.

(viii) An explanation of, and agreement to execute, the steps that will be prevent the non-conformity from re-occurring.

(3) When ONC receives a proposed corrective action plan (or a revised proposed corrective action plan), it shall either approve the proposed corrective action plan or, if the plan does not adequately address all required elements, instruct the health IT developer to submit a revised proposed corrective action plan within a specified period of time.

(4) The health IT developer is responsible for ensuring that a proposed corrective action plan submitted in accordance with paragraph (b)(2)(ii)(A)(*4*) of this section or a revised corrective action plan submitted in accordance with paragraph (c)(3) of this section adequately addresses all required elements as determined by ONC no later than 90 days after the health IT developer's receipt of a notice of non-conformity.

(5) Health IT developers may request extensions for the submittal and/or completion of corrective action plans. In order to make these requests, health IT developers must submit a written statement to ONC that explains and justifies the extension request. ONC will evaluate each request individually and will make decisions on a case-by-case basis.

(6) Upon fulfilling all of its obligations under the corrective action plan, the health IT developer must submit an attestation to ONC, which serve as a binding official statement by the health IT developer that it has fulfilled all of its obligations under the corrective action plan.

(7) ONC may reinstitute a corrective action plan if it later determines that a health IT developer has not fulfilled all of its obligations under the corrective action plan as attested in accordance with paragraph (c)(6) of this section.

(d) *Suspension.* (1) ONC may suspend the certification of a Health IT Module at any time if ONC has a reasonable belief that the certified health IT may present a serious risk to public health or safety.

(2) When ONC decides to suspend a certification, ONC will notify the health IT developer of its determination through a notice of suspension.

(i) The notice of suspension will include, but may not be limited to:

(A) An explanation for the suspension;

(B) Information supporting the determination;

(C) The consequences of suspension for the health IT developer and the Health IT Module under the ONC Health IT Certification Program; and

(D) Instructions for appealing the suspension.

(ii) A suspension of a certification will become effective upon the date specified in the notice of suspension.

(3) The health IT developer must notify all potentially affected customers of the identified non-conformity(ies) and suspension of certification in a timely manner.

(4) When a certification is suspended, the health IT developer must cease and desist from any marketing, licensing, and sale of the suspended Health IT Module as ''certified'' under the ONC Health IT Certification Program from that point forward until such time ONC cancels the suspension in accordance with paragraph (d)(6) of this section.

(5) The certification of any health IT produced by a health IT developer that has the certification of one of its Health IT Modules suspended under the Program is prohibited, unless ONC cancels a suspension in accordance with paragraph (d)(6) of this section.

(6) ONC may cancel a suspension at any time if ONC no longer has a reasonable belief that the certified health IT presents a serious risk to public health or safety.

(e) *Proposed termination*—(1) *Applicability*. Excluding situations of non-compliance with a Condition or Maintenance of Certification requirement under subpart D of this part, ONC may propose to terminate a certification issued to a Health IT Module if:

(i) The health IT developer fails to timely respond to any communication from ONC, including, but not limited to:

(A) Fact-finding;

(B) A notice of potential non-conformity within the timeframe established in accordance with paragraph (b)(1)(ii)(A)(*3*) of this section;

(C) A notice of non-conformity within the timeframe established in accordance with paragraph (b)(2)(ii)(A)(*3*) of this section; or

(D) A notice of suspension.

(ii) The information or access provided by the health IT developer in response to any ONC communication, including, but not limited to: Fact-finding, a notice of potential non-conformity, or a notice of non-conformity is insufficient or incomplete;

(iii) The health IT developer fails to cooperate with ONC and/or a third party acting on behalf of ONC;

(iv) The health IT developer fails to timely submit in writing a proposed corrective action plan;

(v) The health IT developer fails to timely submit a corrective action plan that adequately addresses the elements required by ONC as described in paragraph (c) of this section;

(vi) The health IT developer does not fulfill its obligations under the corrective action plan developed in accordance with paragraph (c) of this section; or

(vii) ONC concludes that a certified health IT's non-conformity(ies) cannot be cured.

(2) When ONC decides to propose to terminate a certification, ONC will notify the health IT developer of the proposed termination through a notice of proposed termination.

(i) The notice of proposed termination will include, but may not be limited to:

(A) An explanation for the proposed termination;

(B) Information supporting the proposed termination; and

(C) Instructions for responding to the proposed termination.

(3) The health IT developer may respond to a notice of proposed termination, but must do so within 10 days of receiving the notice of proposed termination and must include appropriate documentation explaining in writing why its certification should not be terminated.

(4) Upon receipt of the health IT developer's written response to a notice of proposed termination, ONC has up to 30 days to review the information submitted by the health IT developer and make a determination. ONC may extend this timeframe if the complexity of the case requires additional time for ONC review. ONC will, as applicable:

(i) Notify the health IT developer in writing that it has ceased all or part of its review of the health IT developer's certified health IT.

(ii) Notify the health IT developer in writing of its intent to continue all or part of its review of the certified health IT under the provisions of this section.

(iii) Proceed to terminate the certification of the health IT under review consistent with paragraph (f) of this section.

(f) *Termination*—(1) *Applicability*. The National Coordinator may terminate a certification if:

(i) A determination is made that termination is appropriate after considering the information provided by the health IT developer in response to the proposed termination notice;

(ii) The health IT developer does not respond in writing to a proposed termination notice within the timeframe specified in paragraph (e)(3) of this section; or

(iii) A determination is made that the health IT developer is noncompliant with a Condition or Maintenance of Certification requirement under subpart D of this part or for the following circumstances when ONC exercises direct review under paragraph (a)(2)(iii) of this section:

(A) The health IT developer fails to timely respond to any communication from ONC, including, but not limited to:

(*1*) Fact-finding;

(*2*) A notice of potential non-conformity within the timeframe established in accordance with paragraph (b)(1)(ii)(A)(*3*) of this section; or

(*3*) A notice of non-conformity within the timeframe established in accordance with paragraph (b)(2)(ii)(A)(*3*) of this section.

(B) The information or access provided by the health IT developer in response to any ONC communication, including, but not limited to: Fact-finding, a notice of potential non-conformity, or a notice of non-conformity is insufficient or incomplete;

(C) The health IT developer fails to cooperate with ONC and/or a third party acting on behalf of ONC;

(D) The health IT developer fails to timely submit in writing a proposed corrective action plan;

(E) The health IT developer fails to timely submit a corrective action plan that adequately addresses the elements required by ONC as described in paragraph (c) of this section;

(F) The health IT developer does not fulfill its obligations under the corrective action plan developed in accordance with paragraph (c) of this section; or

(G) ONC concludes that the non-conformity(ies) cannot be cured.

(2) When ONC decides to terminate a certification, ONC will notify the health IT developer of its determination through a notice of termination.

(i) The notice of termination will include, but may not be limited to:

(A) An explanation for the termination;

(B) Information supporting the determination;

(C) The consequences of termination for the health IT developer and the Health IT Module under the ONC Health IT Certification Program; and

(D) Instructions for appealing the termination.

(ii) A termination of a certification will become effective after the following applicable occurrence:

(A) The expiration of the 10-day period for filing a statement of intent to appeal in paragraph (g)(3)(i) of this section if the health IT developer does not file a statement of intent to appeal.

(B) The expiration of the 30-day period for filing an appeal in paragraph (g)(3)(ii) of this section if the health IT developer files a statement of intent to appeal, but does not file a timely appeal.

(C) A final determination to terminate the certification per paragraph (g)(7) of this section if a health IT developer files an appeal.

(3) The health IT developer must notify all potentially affected customers of the identified non-conformity(ies) and termination of certification in a timely manner.

(4) ONC may rescind a termination determination before the termination becomes effective if ONC determines that termination is no longer appropriate.

(g) *Appeal*—(1) *Basis for appeal.* A health IT developer may appeal an ONC determination to suspend or terminate a certification issued to a Health IT Module and/or an ONC determination to issue a certification ban under § 170.581(a)(2) if the health IT developer asserts:

(i) ONC incorrectly applied ONC Health IT Certification Program requirements for a:

(A) Suspension;

(B) Termination; or

(C) Certification ban under § 170.581(a)(2).

(ii) ONC's determination was not sufficiently supported by the information provided by ONC with its determination.

(2) *Method and place for filing an appeal.* A statement of intent to appeal followed by a request for appeal must be submitted to ONC in writing by an authorized representative of the health IT developer subject to the determination being appealed. The statement of intent to appeal and request for appeal must be filed in accordance with the requirements specified in the notice of:

(i) Termination;

(ii) Suspension; or

(iii) Certification ban under § 170.581(a)(2).

(3) *Time for filing a request for appeal.* (i) A statement of intent to appeal must be filed within 10 days of a health IT developer's receipt of the notice of:

(A) Suspension;

(B) Termination; or

(C) Certification ban under § 170.581(a)(2).

(ii) An appeal, including all supporting documentation, must be filed within 30 days of the filing of the intent to appeal.

(4) *Effect of appeal.* (i) A request for appeal stays the termination of a certification issued to a Health IT Module, but the Health IT Module is prohibited from being marketed, licensed, or sold as ''certified'' during the stay.

(ii) A request for appeal does not stay the suspension of a Health IT Module.

(iii) A request for appeal stays a certification ban issued under § 170.581(a)(2).

(5) *Appointment of a hearing officer.* The National Coordinator will assign the case to a hearing officer to adjudicate the appeal on his or her behalf.

(i) The hearing officer may not review an appeal in which he or she participated in the initial suspension, termination, or certification ban determination or has a conflict of interest in the pending matter.

(ii) The hearing officer must be trained in a nationally recognized ethics code that articulates nationally recognized standards of conduct for hearing officers/officials.

(6) *Adjudication.* (i) The hearing officer may make a determination based on:

(A) The written record, which includes the:

(1) ONC determination and supporting information;

(2) Information provided by the health IT developer with the appeal filed in accordance with paragraphs (g)(1) through (3) of this section; and

(3) Information ONC provides in accordance with paragraph (g)(6)(v) of this section; or

(B) All the information provided in accordance with paragraph (g)(6)(i)(A) and any additional information from a hearing conducted in-person, via telephone, or otherwise.

(ii) The hearing officer will have the discretion to conduct a hearing if he/she:

(A) Requires clarification by either party regarding the written record under paragraph (g)(6)(i)(A) of this section;

(B) Requires either party to answer questions regarding the written record under paragraph (g)(6)(i)(A) of this section; or

(C) Otherwise determines a hearing is necessary.

(iii) The hearing officer will neither receive witness testimony nor accept any new information beyond what was provided in accordance with paragraph (g)(6)(i) of this section.

(iv) The default process will be a determination in accordance with paragraph (g)(6)(i)(A) of this section.

(v) ONC will have an opportunity to provide the hearing officer with a written statement and supporting documentation on its behalf that clarifies,

as necessary, its determination to suspend or terminate the certification or issue a certification ban.

(7) *Determination by the hearing officer.* (i) The hearing officer will issue a written determination to the health IT developer within 30 days of receipt of the appeal or within a timeframe agreed to by the health IT developer and ONC and approved by the hearing officer, unless ONC cancels the suspension or rescinds the termination determination.

(ii) The National Coordinator's determination on appeal, as issued by the hearing officer, is final and not subject to further review.

[81 FR 72468, Oct. 19, 2016, as amended at 85 FR 25953, May 1, 2020]

§ 170.581 Certification ban.

(a) *Circumstances that may trigger a certification ban.* The certification of any of a health IT developer's health IT is prohibited when:

(1) The certification of one or more of the health IT developer's Health IT Modules is:

(i) Terminated by ONC under the ONC Health IT Certification Program;

(ii) Withdrawn from the ONC Health IT Certification Program by an ONC–ACB because the health IT developer requested it to be withdrawn (for reasons other than to comply with Program requirements) when the health IT developer's health IT was the subject of a potential non-conformity or non-conformity as determined by ONC;

(iii) Withdrawn by an ONC–ACB because of a non-conformity with any of the certification criteria adopted by the Secretary under subpart C of this part;

(iv) Withdrawn by an ONC–ACB because the health IT developer requested it to be withdrawn (for reasons other than to comply with Program requirements) when the health IT developer's health IT was the subject of surveillance for a certification criterion or criteria adopted by the Secretary under subpart C of this part, including notice of pending surveillance; or

(2) ONC determines a certification ban is appropriate per its review under §170.580(a)(2)(iii).

(b) *Notice of certification ban.* When ONC decides to issue a certification ban to a health IT developer, ONC will notify the health IT developer of the certification ban through a notice of certification ban. The notice of certification ban will include, but may not be limited to:

(1) An explanation of the certification ban;

(2) Information supporting the certification ban;

(3) Instructions for appealing the certification ban if banned in accordance with paragraph (a)(2) of this section; and

(4) Instructions for requesting reinstatement into the ONC Health IT Certification Program, which would lift the certification ban.

(c) *Effective date of certification ban.* (1) A certification ban will be effective immediately if banned under paragraph (a)(1) of this section.

(2) For certification bans issued under paragraph (a)(2) of this section, the ban will be effective immediately after the following applicable occurrence:

(i) The expiration of the 10-day period for filing a statement of intent to appeal in §170.580(g)(3)(i) if the health IT developer does not file a statement of intent to appeal.

(ii) The expiration of the 30-day period for filing an appeal in §170.580(g)(3)(ii) if the health IT developer files a statement of intent to appeal, but does not file a timely appeal.

(iii) A final determination to issue a certification ban per §170.580(g)(7) if a health IT developer files an appeal timely.

(d) *Reinstatement.* The certification of a health IT developer's health IT subject to the prohibition in paragraph (a) of this section may commence once the following conditions are met.

(1) A health IT developer must request ONC's permission in writing to participate in the ONC Health IT Certification Program.

(2) The request must demonstrate that the customers affected by the certificate termination, certificate withdrawal, or noncompliance with a Condition or Maintenance of Certification requirement have been provided appropriate remediation.

(3) For noncompliance with a Condition or Maintenance of Certification

requirement, the noncompliance must be resolved.

(4) ONC is satisfied with the health IT developer's demonstration under paragraph (d)(2) of this section that all affected customers have been provided with appropriate remediation and grants reinstatement into the ONC Health IT Certification Program.

[85 FR 25954, May 1, 2020]

§ 170.599 Incorporation by reference.

(a) Certain material is incorporated by reference into this subpart with the approval of the Director of the Federal Register under 5 U.S.C. 552(a) and 1 CFR part 51. To enforce any edition other than that specified in this section, the Department of Health and Human Services must publish a document in the FEDERAL REGISTER and the material must be available to the public. All approved material is available for inspection 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, and is available from the source listed below. It is also available for inspection at the National Archives and Records Administration (NARA). For information on the availability of this material at NARA, call 202–741–6030 or go to *http://www.archives.gov/federal_register/code_of_federal_regulations/ibr_locations.html*.

(b) International Organization for Standardization, Case postale 56, CH·1211, Geneve 20, Switzerland, telephone +41–22–749–01–11, *http://www.iso.org*.

(1) ISO/IEC GUIDE 65:1996—General Requirements for Bodies Operating Product Certification Systems (First Edition), 1996, ''ISO/IEC Guide 65,'' IBR approved for § 170.503.

(2) ISO/IEC 17011:2004 Conformity Assessment—General Requirements for Accreditation Bodies Accrediting Conformity Assessment Bodies (Corrected Version), February 15, 2005, ''ISO/IEC 17011,'' IBR approved for § 170.503.

(3) ISO/IEC 17025:2005(E)—General requirements for the competence of testing and calibration laboratories (Second Edition), 2005–05–15, ''ISO/IEC 17025,'' IBR approved for §§ 170.520(b) and 170.524(a).

(4) ISO/IEC 17025:2017(E)—General requirements for the competence of testing and calibration laboratories (Third Edition), 2017–11, ''ISO/IEC 17025,'' IBR approved for §§ 170.520(b), and 170.524(a).

(5) ISO/IEC 17065:2012(E)—Conformity assessment—Requirements for bodies certifying products, processes and services (First Edition), 2012, ''ISO/IEC 17065,'' IBR approved for §§ 170.503 and 170.523(a).

[81 FR 72471, Oct. 19, 2016, as amended at 85 FR 25955, May 1, 2020]

PART 171—INFORMATION BLOCKING

Subpart A—General Provisions

Sec.

Subpart B—Exceptions That Involve Not Fulfilling Requests to Access, Exchange, or Use Electronic Health Information