DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Part 170

RIN 0955–AA00

ONC Health IT Certification Program: Enhanced Oversight and Accountability

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

ACTION: Final rule.

SUMMARY: This final rule finalizes modifications and new requirements under the ONC Health IT Certification Program (''Program''), including provisions related to the Office of the National Coordinator for Health Information Technology (ONC)'s role in the Program. The final rule creates a regulatory framework for ONC's direct review of health information technology (health IT) certified under the Program, including, when necessary, requiring the correction of non-conformities found in health IT certified under the Program and suspending and terminating certifications issued to Complete EHRs and Health IT Modules. The final rule also sets forth processes for ONC to authorize and oversee accredited testing laboratories under the Program. In addition, it includes provisions for expanded public availability of certified health IT surveillance results.

DATES: These regulations are effective December 19, 2016.

The incorporation by reference of the publication listed in the rule is approved by the Director of the Federal Register as of December 19, 2016.

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

SUPPLEMENTARY INFORMATION:

Commonly Used Acronyms

CAP	Corrective Action Plan
CEHRT	Certified Electronic Health Record Technology
CFR	Code of Federal Regulations
CHPL	Certified Health IT Product List
EHR	Electronic Health Record
HHS	Department of Health and Human Services
HIT	Health Information Technology
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
NVLAP	National Voluntary Laboratory Accreditation Program
OMB	Office of Management and Budget
ONC	Office of the National Coordinator for Health Information Technology
ONC–ACB	ONC-Authorized Certification Body
ONC–ATCB	ONC-Authorized Testing and Certification Body
ONC–ATL	ONC-Authorized Testing Laboratory
PoPC	Principles of Proper Conduct

Table of Contents

I. Executive Summary

A. Purpose of Regulatory Action

The ONC Health IT Certification Program (''Program'') was first established as the Temporary Certification Program in a final rule published on June 24, 2010 (''Temporary Certification Program final rule'' (75 FR 36158)). It was later transitioned to the Permanent Certification Program in a final rule published on January 7, 2011 (''Permanent Certification Program final rule'' (76 FR 1262)). Since that time, we have updated the Program and made modifications to the Program through subsequent rules as discussed below.

In November 2011, a final rule established a process for ONC to address instances where the ONC-Approved Accreditor (ONC–AA) has engaged in improper conduct or has failed to perform its responsibilities under the Program (76 FR 72636). In September 2012, a final rule (''2014 Edition final rule'' (77 FR 54163)) established an edition of certification criteria and modified the Program to, among other things, provide clear implementation direction to ONC-Authorized Certification Bodies (ONC–ACBs) for certifying Health IT Modules to new certification criteria. On September 11, 2014, a final rule provided certification flexibility through the adoption of new certification criteria and further improvements to the Program (''2014 Edition Release 2 final rule'' (79 FR 54430)). On October 16, 2015, the Department of Health and Human Services (HHS) published a final rule that identified how health IT certification can support the establishment of an interoperable nationwide health information infrastructure through the certification and adoption of new and updated vocabulary and content standards for the structured recording and exchange of health information (''2015 Edition final rule'' (80 FR 62602)). The 2015 Edition final rule modified the Program to make it open and accessible to more types of health IT, and health IT that supports various care and practice settings. It also included enhanced surveillance, disclosure, and other requirements. These requirements were designed to support the reliability of health IT certified under the Program and increase the transparency of information about such health IT (referred to as ''certified health IT'' throughout this final rule).

With each Program modification and rule, we continue to address stakeholder concerns, provide additional guidance, and improve oversight. In keeping with this approach, in the ''ONC Health IT Certification Program: Enhanced Oversight and Accountability'' proposed rule (81 FR 11056) (''Proposed Rule'') we put forth several new proposals for comment, based on feedback from stakeholders and our own experience administering the Program. Importantly, we explained that the adoption and use of certified health IT has increased significantly since the Program was established, and that this trend will continue, including for settings and use cases beyond the Medicare and Medicaid EHR Incentive Programs (''EHR Incentive Programs''). As certified health IT becomes more integral to the delivery of care, and as certified capabilities increasingly interact with other capabilities in certified health IT and with other products, we seek to strengthen oversight of the performance of certified health IT capabilities and ensure that concerns within the scope of the Program continue to be appropriately addressed.

We explained in the Proposed Rule that we had delegated authority to ONC–ACBs to issue certifications for health IT on our behalf through the Permanent Certification Program final rule (81 FR 11057). In addition to issuing and administering certifications, ONC–ACBs are responsible for conducting ongoing surveillance to assess whether certified health IT continues to conform to the requirements of the Program. An ONC–ACB's surveillance encompasses conformity assessments based on adopted certification criteria as well as certain other regulatory requirements (*e.g.,* §§ 170.523(k) and (l)). However, under this approach, which is consistent with customary certification programs and International Organization for Standardization/International Electrotechnical Commission 17065:2012 (ISO/IEC 17065),[1] ONC–ACBs do not have the responsibility to address the full range of requirements applicable to health IT certified under the Program. For example, an ONC–ACB's conformity assessment may not encompass certain interactions among certified capabilities and other capabilities or products that are not certified under the Program. Similarly, an ONC–ACB's assessment of certified capabilities may be limited to certain functional outcomes and may not encompass the combined or overall performance of certified health IT in accordance with Program requirements. Separately, in some instances an ONC–ACB may be responsible for administering Program requirements but may be unable to do so effectively due to practical challenges. In contrast, ONC is well-positioned to review certified health IT against the full range of requirements under the Program. Therefore, to enhance Program oversight and the reliability and safety of certified health IT, we have finalized provisions of the Proposed Rule that set forth a regulatory framework for ONC to directly review certified health IT and take appropriate responsive actions to address potential non-conformities and non-conformities.

The direct review processes included in this final rule will enhance the National Coordinator's ability to discharge his or her responsibilities under the Health Information Technology for Economic and Clinical Health (HITECH) Act. The HITECH Act amended the Public Health Service Act (PHSA) and created ''Title XXX—Health Information Technology and Quality'' (Title XXX) to improve health care quality, safety, and efficiency through the promotion of health IT and electronic health information exchange. Section 3001(b) of the PHSA requires that the National Coordinator for Health Information Technology (National Coordinator) perform specified statutory duties, including keeping or recognizing a program or programs for the voluntary certification of health information technology (section 3001(c)(5) of the PHSA), in a manner consistent with the development of a nationwide health information technology infrastructure that allows for the electronic use and exchange of information and that: (1) Ensures that each patient's health information is secure and protected, in accordance with applicable law; (2) improves health care quality, reduces medical errors, reduces health disparities, and advances the delivery of patient-centered medical care; (3) reduces health care costs resulting from inefficiency, medical errors, inappropriate care, duplicative care, and incomplete information; (4) provides appropriate information to help guide medical decisions at the time and place of care; (5) ensures the inclusion of meaningful public input in such development of such infrastructure; (6) improves the coordination of care and information among hospitals, laboratories, physician offices, and other entities through an effective infrastructure for the secure and authorized exchange of health care information; (7) improves public health activities and facilitates the early identification and rapid response to public health threats and emergencies, including bioterror events and infectious disease outbreaks; (8) facilitates health and clinical research and health care quality; (9) promotes early detection, prevention, and management of chronic diseases; (10) promotes a more effective marketplace, greater competition, greater systems analysis, increased consumer choice, and improved outcomes in health care services; and (11) improves efforts to reduce health disparities. Consistent with these statutory requirements, this final rule establishes a regulatory framework for ONC's direct review of health IT certified under the Program.

This final rule also sets forth processes for ONC to timely and directly

[1] The international standard to which ONC–ACBs are accredited (*see also* 45 CFR 170.599(b)(3)).

address testing issues. These processes do not currently exist under the Program structure and would serve to align the testing structure with ONC's authorization and oversight of ONC–ACBs. In addition, this final rule would increase the transparency and availability of information about certified health IT through the publication of identifiable surveillance results. The publication of identifiable surveillance results will support further accountability of health IT developers to their customers and users of certified health IT.

B. Summary of Major Provisions

1. ONC Direct Review of Certified Health IT

This final rule provides a regulatory framework for ONC to directly review certified health IT to determine whether it conforms to the requirements of the Program. Under this framework, ONC's review of certified health IT will be independent of, and may be in addition to, ONC–ACBs' surveillance and other functions under the Program. ONC's review will focus on capabilities and aspects of health IT that are certified under the Program (referred to throughout this final rule as ''certified capabilities''), taking into consideration other relevant functionalities or products to the extent necessary to determine whether certified health IT is functioning in a manner consistent with Program requirements.

While the PHSA provides authority for ONC to directly review certified health IT in a broad range of circumstances, at this time we have finalized a regulatory framework for the exercise of such review in a more limited set of circumstances. This scope of review reflects the need to focus ONC's resources in areas that, at this time, are most vital to ensuring the integrity and effectiveness of the Program. It also complements the existing oversight and enforcement responsibilities of other government departments, agencies, and offices (referred to throughout this final rule as ''agencies'' or ''agency,'' as the context requires) that encourage compliance with Program requirements and promote accountability for the reliability and performance of health IT.

Specifically, this final rule establishes regulatory processes for ONC to exercise direct review of certified health IT, and take appropriate responsive actions, in two distinct sets of circumstances.

First, ONC may elect to directly review certified health IT when it has reason to believe that the certified health IT may not conform to the requirements of the Program because the certified health IT is causing or contributing to serious risks to public health or safety. Addressing the full range of these suspected non-conformities is beyond the scope of an ONC–ACB's expertise and responsibilities under the Program. In contrast, ONC has the authority to address the full range of requirements under the Program and, as we explained in the Proposed Rule, can effectively respond to these issues, quickly bringing to bear needed expertise and resources and coordinating activities with federal counterparts and other relevant entities to ensure a coordinated review and response (81 FR 11061).

Second, in addition to serious risks to public health or safety, ONC may elect to directly review certified health IT on the basis of other suspected non-conformities that, while within the scope of an ONC–ACB's responsibilities, present practical challenges that may prevent the ONC–ACB from effectively investigating the suspected non-conformity or providing an appropriate response. In particular, ONC may directly review certified health IT if a suspected non-conformity presents issues that may require access to certain confidential or other information that is unavailable to an ONC–ACB; may require concurrent or overlapping reviews by multiple ONC–ACBs; or may exceed the scope of an ONC–ACB's resources or expertise. We believe that ONC's review of certified health IT in these situations will help ensure the continued effective oversight and administration of the Program.

In response to comments received on the Proposed Rule, we have not at this time finalized regulatory processes by which ONC would directly review certified health IT solely on the basis of circumstances distinct from public health or safety concerns or in cases where practical challenges prevent an ONC–ACB from effectively investigating the suspected non-conformity or providing an appropriate response, as discussed above (*compare* 81 FR 11061). For example, at this time, the processes set forth in this rule do not establish that ONC will directly review certified health IT solely on the basis of a threat to the security or protection of patients' health information in violation of applicable law (*see* section 3001(b)(1) of the PHSA) or the risk of increasing health care costs resulting from, for example, inefficiency or incomplete information (*see* section 3001(b)(3) of the PHSA). We believe that other agencies are currently in the best position to provide effective oversight and enforcement with respect to such potential exigencies. We will continue to assess the need to exercise direct review in these additional circumstances, as necessary.

As mentioned above, in this final rule, we seek to align ONC's direct review of certified health IT with oversight and enforcement responsibilities of other agencies. We therefore clarify that ONC may decline to exercise review of certified health IT for any reason, including if it believes that other agencies may be better situated to respond to a suspected non-conformity. Additionally, to the extent permitted by law, ONC may coordinate and share information with other agencies, including agencies with applicable oversight or enforcement responsibilities, and may engage other persons and entities, as appropriate, to effectively respond to suspected problems or issues with certified health IT. We note that to the extent ONC engages in any efforts to identify or address non-conformities, such efforts and any resulting remediation (or the absence of such efforts or remediation) are not intended to impact the materiality of any non-conformity in a matter addressed by another agency; and nothing in this final rule is intended to supplant, delay, or in any way limit oversight or enforcement by other agencies, including any investigation, decision, legal action, or proceeding.

The final rule addresses actions ONC will take and procedures it will follow in the event that ONC's direct review of certified health IT substantiates a non-conformity. ONC will require corrective action for non-conformities and, when necessary, suspend, or terminate a certification issued to a Complete EHR or Health IT Module. Health IT developers will have the opportunity to appeal determinations by ONC to suspend or terminate certifications issued to health IT under the Program. Further, to protect the integrity of the Program and users of certified health IT, we have finalized a Certification Ban on the future certification of any of a health IT developer's health IT when the certification of one or more of the health IT developer's current Complete EHRs or Health IT Modules is: (1) Terminated by ONC; (2) withdrawn by an ONC–ACB because the health IT developer requested it to be withdrawn when the health IT developer's health IT was the subject of a potential non-conformity or non-conformity as determined by ONC; (3) withdrawn by an ONC–ACB because of a non-conformity with any of the certification criteria adopted by the Secretary at subpart C of this part; or (4) withdrawn by an ONC–ACB because the health IT developer requested it to be withdrawn when the health IT developer's health IT was the subject of surveillance for a certification criterion or criteria adopted by the Secretary at subpart C of this part, including pending surveillance (*e.g.,* the health IT developer received notice of pending randomized surveillance).

We emphasize that ONC's role in reviewing certified health IT will support greater accountability for health IT developers under the Program and provide greater confidence that health IT conforms to Program requirements when it is implemented, maintained, and used. We further emphasize that our first and foremost goal is to work with health IT developers to remedy any identified non-conformities of certified health IT in a timely manner.

2. ONC-Authorized Testing Laboratories

ONC will conduct direct oversight of testing labs under the Program in order to ensure that ONC oversight can be similarly applied at all stages of the Program. Unlike the processes already established for ONC–ACBs, we had not established a similar process for testing labs. Instead, we required in the Principles of Proper Conduct (PoPC) for ONC–ACBs that ONC–ACBs only accept test results from National Voluntary Laboratory Accreditation Program (NVLAP)-accredited testing labs. This requirement for ONC–ACBs has had the effect of requiring testing labs to be accredited by NVLAP to International Organization for Standardization/International Electrotechnical Commission 17025:2005 (General requirements for the competence of testing and calibration laboratories) (ISO/IEC 17025). As a result, there has effectively been no direct ONC oversight of NVLAP-accredited testing labs like there is for ONC–ACBs.

This final rule establishes means for ONC to have direct oversight of NVLAP-accredited testing labs by having them apply to become ONC-Authorized Testing Labs (ONC–ATLs). Specifically, the final rule establishes processes for authorizing, retaining, suspending, and revoking ONC-Authorized Testing Lab (ONC–ATL) status under the Program. These processes are similar to current ONC–ACB processes. The finalized changes will enable ONC to oversee and address testing and certification performance issues throughout the entire continuum of the Program in a precise and direct manner.

3. Transparency and Availability of Identifiable Surveillance Results

In furtherance of our efforts to increase the transparency and availability of information related to certified health IT, we have finalized an approach that will now require ONC–ACBs to make identifiable surveillance results publicly available on the Certified Health IT Product List (CHPL) on a quarterly basis. Posting identifiable surveillance results on the CHPL provides stakeholders with a more readily available means for accessing the results. The information required to be reported for identifiable surveillance results includes information specified in the Proposed Rule and the relevant information already required to be posted on the CHPL, when appropriate, as part of a corrective action plan (CAP).

The publication of identifiable surveillance results will enhance transparency and the accountability of health IT developers to their customers. The public availability of identifiable surveillance results will provide customers and users with valuable information about the continued conformity of certified health IT. While we expect that the prospect of publicly available identifiable surveillance results will motivate some health IT developers to improve their maintenance efforts, we believe that most published results will reassure customers and users of certified health IT. This is because, based on ONC–ACB surveillance results to date, certified health IT and health IT developers are maintaining conformity with certification criteria and Program requirements. The publishing of identifiable surveillance results will also provide more complete information by illuminating good performance and continued conformity; rather than only sharing non-conforming results, and when applicable, CAPs.

C. Costs and Benefits

Executive Orders 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). A regulatory impact analysis (RIA) must be prepared for major rules with economically significant effects ($100 million or more in any one year). It has been determined that this final rule is an economically significant rule as the potential costs associated with this final rule could be greater than $100 million per year. Accordingly, we have prepared an RIA that to the best of our ability presents the costs and benefits of the final rule.

1. Costs

We have identified and estimated the potential monetary costs of this final rule for health IT developers, ONC–ATLs, the federal government (*i.e.,* ONC), and health care providers. We have categorized and addressed costs as follows: (1) Costs for health IT developers to correct non-conformities identified by ONC; (2) costs for ONC and health IT developers related to an ONC inquiry into certified health IT non-conformities and ONC direct review, including costs for the new ''proposed termination'' step; (3) costs for health IT developers and ONC associated with the appeal process following a suspension/termination of a Complete EHR's or Health IT Module's certification; (4) costs for health care providers to transition to another certified health IT product when the certification of a Complete EHR or Health IT Module that they currently use is terminated; (5) costs for ONC–ATLs and ONC associated with ONC–ATL accreditation, application, renewal, and reporting requirements; (6) costs for ONC–ATLs and ONC related to revoking ONC–ATL status; and (7) costs for ONC–ACBs to publicly report (submit) identifiable surveillance results to the CHPL. We also provide an overall annual monetary cost estimate for this final rule. We note that we have rounded all estimates to the nearest dollar and all estimates are expressed in 2016 dollars.

This final rule may: (1) Lead health IT developers to reassess whether their certified health IT is in conformity with Program requirements; and (2) require health IT developers to correct non-conformities found by ONC in their certified health IT. If ONC were to find a non-conformity with a certified capability under the direct review processes outlined in this final rule, then the costs to correct the non-conformity are a result of this final rule. However, due to the difficulty of projecting such instances given the underlying need to correct non-conformities, we have not been able to include these costs in our quantitative cost estimates, as discussed in greater detail in section VI.C.1.a.(1) of this final rule.

We have estimated the costs for ONC and health IT developers related to an ONC inquiry into certified health IT non-conformities and ONC direct review. We estimate the cost for a health IT developer to cooperate with an ONC review and inquiry into certified health IT would, on average, range from $9,819 to $98,192. We estimate the cost for ONC to review and conduct an inquiry into certified health IT would, on average, range from $2,455 to $147,288.

We have estimated the costs for health IT developers and ONC associated with the appeal process following a suspension/termination of a Complete EHR's or Health IT Module's certification. We estimate the cost for a health IT developer to appeal a suspension or termination would, on average, range from $9,819 to $29,458. We estimate the cost for ONC to conduct an appeal would, on average, range from $24,548 to $98,192.

We have estimated the costs for health care providers to transition to another certified health IT product if the certification of a Complete EHR or Health IT Module that they currently use is terminated. Specifically, we estimate the cost impact of certification termination on health care providers would range from $33,000 to $649,836,000 with a median cost of $792,000 and a mean cost of $6,270,000. We note, however, that it is very unlikely that the high end of our estimated costs would ever be realized. To date, there have been only a few terminations of certified health IT under the Program, which have only affected a small number of providers. Further, we have stated in this final rule our intent to work with health IT developers to correct non-conformities ONC finds in a developer's certified health IT under the provisions in this final rule. We provide a more detailed discussion of past certification terminations and the potential impacts of certification termination on providers in section VI.C.1.a.(4) of this final rule.

We have estimated the costs for ONC–ATLs and ONC associated with ONC–ATL accreditation, application, renewal, and reporting requirements. We estimate the annualized cost for ONC–ATL accreditation, application, and the first proposed three-year authorization period to be approximately $48,832. We estimate the annualized cost for an ONC–ATL to renew its accreditation, application, and authorization during the first three-year ONC–ATL authorization period to be approximately $73,053. In addition, we estimate the total annual cost for ONC–ATLs to meet the reporting requirements of proposed § 170.524(d) to be approximately $3,276.

We estimate ONC's annualized cost for administering the entire application process to be approximately $992. This cost will be the same for a new applicant or ONC–ATL renewal. We would also post the names of applicants granted ONC–ATL status on our Web site. We estimate the potential cost for posting and maintaining the information on our Web site to be approximately $446 annually. We estimate an annual cost to the federal government of $743 to record and maintain updates and changes reported by ONC–ATLs.

We have estimated the costs for ONC–ATLs and ONC related to revoking ONC–ATL status. We estimate the costs for an ONC–ATL to comply with ONC requests per § 170.565 would, on average, range from $2,455 to $19,638. We estimate the cost for ONC would, on average, range from $4,910 to $39,277.

We have estimated the costs for ONC–ACBs to submit identifiable surveillance results to the CHPL on a quarterly basis. We estimate the annual cost for each ONC–ACB to report surveillance results to the CHPL to be $1,024 and the total cost for all three ONC–ACBs to be $3,072.

We estimate the overall annual cost for this final rule, based on the cost estimates outlined above, will range from $171,011 to $650,352,050 with an average annual cost of $6,597,033. For a more detailed explanation of our methodology and estimated costs, please see section VI.C.1.a of this final rule.

2. Benefits

While we do not have available means to quantify the benefits of this final rule, we believe there are many qualitative benefits. This final rule's provisions for ONC direct review of certified health IT promote health IT developers' accountability for the performance, reliability, and safety of certified health IT; and facilitate the use of safer and reliable health IT by health care providers and patients. Specifically, ONC's direct review of certified health IT will facilitate ONC's assessment of non-conformities and ability to require comprehensive corrective actions for health IT developers to address non-conformities determined by ONC, including notifying affected customers. As previously stated, our first and foremost goal is to work with health IT developers to remedy any non-conformities with certified health IT in a timely manner and across all customers. If ONC ultimately suspends and/or terminates a certification issued to a Complete EHR or Health IT Module under the processes established in this final rule, such action will serve to protect the integrity of the Program, patients, and users of health IT. In sum, ONC's direct review of certified health IT supports the National Coordinator in fulfilling his or her responsibilities under the HITECH Act, instills public confidence in the Program, and protects public health and safety.

This final rule's provisions will also provide other benefits. ONC's authorization and oversight of testing labs (ONC–ATLs) will promote further public confidence in testing and certification by facilitating ONC's ability to timely and directly address testing issues for health IT. The public availability of identifiable surveillance results will enhance transparency and the accountability of health IT developers to their customers. It will provide customers and users of certified health IT with valuable information about the continued conformity of certified health IT. Further, the public availability of identifiable surveillance results will likely benefit health IT developers by providing a more complete context of surveillance in the certified health IT industry by illuminating good performance and the continued conformity of certified health IT with Program requirements. Overall, we believe this final rule will improve Program conformity as well as further public confidence in certified health IT.

II. Provisions of the Final Rule

A. ONC's Role Under the ONC Health IT Certification Program

In initially developing the Program, ONC consulted with the National Institute of Standards and Technology (NIST) and created the Program structure based on industry best practice. This structure includes the use of two separate accreditation bodies: (1) An accreditor that evaluates the competency of a health IT testing laboratory to operate a testing program in accordance with international standards; and (2) an accreditor that evaluates the competency of a health IT certification body to operate a certification program in accordance with international standards (*see* the Permanent Certification Program final rule).

This final rule updates the structure of the Program to provide enhanced Program oversight, accountability, and transparency. The rule establishes a regulatory framework that will help facilitate ONC's direct review of certified health IT in current priority areas, including by setting forth processes for such review and describing certain actions ONC may take to enforce Program requirements in appropriate circumstances. The rule also provides for direct ONC oversight of testing laboratories. These and other related provisions of the final rule are described in detail below.

1. Review of Certified Health IT

a. Authority and Scope

We proposed to adopt a regulatory framework that would help facilitate ONC's direct review of certified health IT in certain circumstances and enhance oversight and accountability in the Program (81 FR 11058). This review would be independent of, and could be in addition to, an ONC–ACB's surveillance and other functions under the Program and would complement the role of ONC–ACBs.

In the Proposed Rule, we explained that under the current structure of the Program, ONC–ACBs are responsible for issuing and administering certifications for health IT on behalf of ONC (81 FR 11057). In addition, ONC–ACBs are responsible for conducting ongoing surveillance to assess whether certified health IT continues to conform to the requirements of the Program. An ONC–ACB's surveillance encompasses conformity assessments based on adopted certification criteria as well as certain other regulatory requirements (*e.g.,* § 170.523(k) and (l)). However, under this approach, which is consistent with other certification programs and ISO/IEC 17065,[2] ONC–ACBs do not have the responsibility to address the full range of requirements applicable to health IT certified under the Program. For example, an ONC–ACB's conformity assessments may not encompass certain interactions among certified capabilities and other capabilities or products that are not certified under the Program. Similarly, an ONC–ACB's assessment of certified capabilities may address certain functional outcomes and may not encompass the combined or overall performance of certified health IT in accordance with Program requirements. Separately, in some instances an ONC–ACB may be responsible for administering Program requirements but ONC may be better suited to do so due to practical challenges.[3]

In the Proposed Rule, we outlined several situations in which, for these reasons, an ONC–ACB may be unable to provide oversight necessary to ensure that certified health IT meets Program requirements. We stated, for example, that ONC may be better situated to respond to certain types of non-conformities arising from interactions of certified and uncertified capabilities or from systemic, widespread, or complex issues that could quickly consume or exceed an ONC–ACB's resources or capacity (81 FR 11061). We also observed that in some instances ONC may have access to information about a putative non-conformity that is confidential and cannot be shared with an ONC–ACB (81 FR 11061). We explained that in some cases non-conformities with certified health IT may arise that pose risks to public health or safety or present other exigencies that may warrant ONC's direct review and action (81 FR 11061). Additionally, we noted that a suspected non-conformity may involve health IT or capabilities that have been certified by more than one ONC–ACB. In such a situation, we stated that ONC would be better suited to handle the review of the certified health IT as ONC–ACBs only have oversight of the health IT they certify, while ONC could ensure a more coordinated review and consistent determination. We explained that ONC is well-placed to effectively respond to these potential issues because of its broad authority to administer the full range of requirements under the Program, its ability to quickly marshal and deploy resources and specialized expertise, and its ability to provide a coordinated review and response that may involve other agencies. Therefore, to support ONC's oversight in these areas, we proposed to establish a framework and processes in rulemaking under which ONC may exercise its discretion to directly review certified health IT and take appropriate responsive action.

In the Proposed Rule, we stated that ONC's review of certified health IT could be based on any applicable Program requirements and as such would not be limited to requirements that ONC–ACBs are responsible for enforcing. We proposed that, while ONC would have broad discretion, it would consider the following factors in determining whether to initiate direct review of certified health IT:

- The potential nature, severity, and extent of the suspected non-conformity or non-conformities, including the likelihood of systemic or widespread issues and impact.
- The potential risk to public health or safety or other exigent circumstances.
- The need for an immediate and coordinated governmental response.
- Whether investigating, evaluating, or addressing the suspected non-conformity would require access to confidential or other information that is unavailable to an ONC–ACB; would present issues outside the scope of an ONC–ACB's accreditation; would exceed the resources or capacity of an ONC–ACB; or would involve novel or complex interpretations or application of certification criteria or other requirements.
- The potential for inconsistent application of certification requirements in the absence of direct review.

(*see* 81 FR 11061). We anticipated that ONC's direct review of certified health IT would be relatively infrequent and would focus on situations that pose a risk to public health or safety as well as other situations that present unique challenges or issues that ONC–ACBs may be unable to effectively address without ONC's assistance or intervention (based on consideration of the factors listed above). We stressed that our first and foremost desire would be to work with developers to address any non-conformities identified as a result of ONC's review.

Comments. We received mixed comments on our proposal to establish regulatory processes that would help facilitate ONC's direct review of certified health IT. Some commenters supported the proposal, emphasizing that direct review would address potential gaps in the Program, improve the safety and performance of health IT, and improve the effectiveness of the Program. Other commenters supported ONC's direct review of certified health IT, but within a narrower or more defined scope.

A significant number of commenters were opposed to the proposal or voiced strong concerns. Many of these commenters were opposed to ONC's reviewing the interaction of certified capabilities and uncertified capabilities. Commenters also stated that our proposal would create uncertainty by providing ONC with discretion to review certified health IT in a broad range of circumstances, without clear and predictable rules for assessing conformity to Program requirements. Commenters expressed fear that this broad discretion could lead to inconsistent or arbitrary application of requirements, create uncertainty for developers and other stakeholders, and impede progress and innovation in health IT. Some commenters also contested the authority for ONC to directly review certified health IT in the manner proposed.

Response. We thank commenters for their detailed feedback on this proposal.

[2] The international standard to which ONC–ACBs are accredited (*see also* 45 CFR 170.599(b)(3)).

[3] In certain circumstances, an ONC–ACB may encounter practical challenges that could prevent it from effectively investigating a suspected non-conformity or providing an appropriate response. This may occur where, for example, a suspected non-conformity presents issues that may require access to certain confidential or other information that is unavailable to an ONC–ACB; may require concurrent or overlapping reviews by multiple ONC–ACBs; or may exceed the scope of an ONC–ACB's resources or expertise. For a more detailed discussion of these circumstances, we refer readers to section II.A.1.a.(3) of this final rule and to the section II.B (''Summary of Major Provisions'').

We have finalized the proposal subject to the changes and clarifications summarized here for the convenience of the reader and described in more detail in our responses to the specific comments that follow.

The policy and approach we have finalized respond to emerging challenges identified by stakeholders, through consultation with NIST, and as a result of our experience administering the Program. In the more than six years since the Program was established, certified health IT has become widely adopted and is now integral to the delivery of patient care. At the same time, in response to growing market and regulatory demands for the exchange and use of electronic health information, the capabilities of certified health IT have become more varied, more advanced, and more interdependent with other health IT products and capabilities. These developments are encouraging and signal progress towards a more connected health system that can help transform health and care; yet for that to occur, the public must trust and have confidence in the nation's health IT infrastructure.

To effectively respond to these challenges, and for the National Coordinator to continue to meet his or her responsibilities under section 3001 of the PHSA, we are adopting a regulatory framework in this final rule to enhance the Program. As noted in the Proposed Rule, there are several areas in which ONC–ACBs may lack the responsibility, expertise, or resources to provide effective oversight of certified health IT. Importantly, certain kinds of non-conformities may be difficult to substantiate through technical conformity assessments of the kind ONC–ACBs are currently responsible for administering under the Program. In addition, practical challenges may arise for ONC–ACBs when non-conformities span multiple health IT products whose certifications are administered by more than one ONC–ACB; or where a failure of certified capabilities to perform in an acceptable manner occurs only in the context of the capabilities' interaction with other capabilities or products that are not certified under the Program. For example, some non-conformities may be so systemic, complex, or widespread that to isolate or effectively address them would quickly exceed an ONC–ACB's resources or expertise. In some cases, an ONC–ACB may be unaware of a non-conformity or may be unable to obtain the information necessary to effectively investigate and respond to a suspected non-conformity, such as when doing so would require access to certain confidential information that may be known to ONC but cannot be disclosed to the ONC–ACB.

These reasons support the need for ONC to directly administer Program requirements in appropriate circumstances. Further, the need is all the more compelling when one considers that certified capabilities may be impaired by failures or deficiencies that are not only beyond the reach of ONC–ACBs, but could cause or contribute to serious risks to public health or safety or lead to other outcomes that could significantly undermine public confidence in the health IT infrastructure, the successful development of which is the overriding purpose of the Program itself and of the duties of the National Coordinator under section 3001(c) of the PHSA.

For all of these reasons, we have finalized a regulatory framework that will facilitate ONC's direct review of certified health IT to determine whether it conforms to the requirements of the Program. In doing so, however, we have carefully considered and, where appropriate, accommodated concerns raised by commenters. In particular, while the PHSA provides authority for ONC to directly review certified health IT in a broad range of circumstances, the direct review processes finalized in this rule apply to a more limited set of circumstances in which ONC intends to focus its oversight at this time. This approach will concentrate ONC's resources in areas that at this time are most vital to ensuring the integrity and effectiveness of the Program. In addition, it will complement the existing oversight and enforcement responsibilities of other agencies, provide guidelines that will encourage compliance with Program requirements, and provide accountability for the performance and reliability of health IT. Specifically, this final rule establishes regulatory processes for ONC to exercise direct review of certified health IT, and take appropriate responsive actions, in two distinct sets of circumstances.

First, ONC may elect to directly review certified health IT when it has reason to believe that the certified health IT may not conform to the requirements of the Program because the certified health IT is causing or contributing to conditions that pose a serious risk to public health or safety. Addressing the full range of these suspected non-conformities is beyond the scope of an ONC–ACB's expertise and responsibilities under the Program. In contrast, ONC has the authority to address the full range of requirements under the Program and, as we explained in the Proposed Rule, can effectively respond to these issues, quickly bringing to bear needed expertise and resources and coordinating activities with federal counterparts and other relevant entities to ensure a coordinated review and response (81 FR 11061).

Second, in addition to serious risks to public health or safety, ONC may elect to directly review certified health IT on the basis of other suspected non-conformities that, while they are within the scope of an ONC–ACB's responsibilities, present practical challenges that may prevent the ONC–ACB from effectively investigating the suspected non-conformity or providing an appropriate response. In particular, ONC may directly review certified health IT if a suspected non-conformity presents issues that may require access to certain confidential or other information that is unavailable to an ONC–ACB; may require concurrent or overlapping reviews by multiple ONC–ACBs; or may exceed the scope of an ONC–ACB's resources or expertise. We believe that ONC's review of certified health IT in these circumstances is integral to ensuring the effective oversight and administration of the Program.

In response to comments received on the Proposed Rule, we have not at this time finalized a regulatory framework under which ONC would directly review certified health IT in circumstances other than those that raise public health or safety concerns, or those in which practical challenges prevent an ONC–ACB from effectively investigating a suspected non-conformity or providing an appropriate response, as discussed above (*compare* 81 FR 11061). For example, at this time, the regulatory framework set forth in this rule does not provide that ONC will directly review certified health IT solely on the basis of a threat to the security or protection of patients' health information in violation of applicable law (*see* section 3001(b)(1) of the PHSA) or the risk of increasing health care costs resulting from, for example, inefficiency or incomplete information (*see* section 3001(b)(3) of the PHSA). We believe that other agencies are currently in the best position to provide effective oversight and enforcement with respect to such potential exigencies. We will continue to assess the need to exercise direct review in these additional circumstances, as necessary.

Finally, in response to commenters' requests for additional clarity on certain provisions of the Proposed Rule, this final rule explains three key principles ONC will apply when deciding whether to initiate direct review of certified health IT and in determining whether certified health IT conforms to the requirements of the Program.

First, ONC's direct review of certified health IT—and any subsequent determination of non-conformity by ONC—would be based on a reasonable belief that health IT may be or is in violation of Program requirements. Contrary to the assertions of some commenters, these requirements have been clearly and consistently communicated to developers and do not impose new obligations under the Program. Indeed, in the 2015 Edition final rule, we explained that to comply with applicable certification criteria, developers must not only demonstrate required capabilities in a controlled testing environment but must also make those capabilities available in ways that enable them to be implemented and used in production environments for their intended purposes (80 FR 62711). That includes making certified capabilities available in a manner that does not cause or contribute to serious risks to public health or safety or to other outcomes that are inconsistent with the National Coordinator's responsibilities under section 3001(b) of the PHSA.

Second, while several commenters objected to our proposal to review uncertified capabilities, we believe that many of these commenters misunderstood the scope of what was proposed. We proposed and have finalized regulatory processes for ONC to review capabilities and aspects of health IT that are certified under the Program. Our consideration of uncertified capabilities would be ancillary to our review of certified capabilities and would be limited to the extent necessary to determine whether certified capabilities are functioning in a manner consistent with Program requirements.

Last, as we have previously explained in the context of an ONC–ACB's surveillance of certified health IT, a developer of certified health IT cannot be held responsible under the Program for putative non-conformities that are not reasonably within its ability to influence or control. This limiting principle applies with equal force to ONC's direct review of certified health IT under the Program.

The foregoing principles are consistent with those that have previously been established under the Program and ensure that ONC's review of certified health IT is consistent, follows clear and predictable guidelines, and is limited to issues that are within the scope of the Program. These principles and other aspects of ONC's direct review under this final rule are explained in greater detail in the responses to specific comments below. We also have included numerous examples to assist readers in understanding these concepts and the manner in which ONC would apply them in various circumstances.

(1) Requirements of the Program

Comments. Some commenters, primarily health IT developers, posited that ONC may lack the requisite authority to directly review or enforce Program requirements, or to do so in the manner proposed. Several of these commenters criticized our invocation of section 3001(b) of the PHSA, which expressly enumerates the core principles and requirements inherent to the purpose of ONC. Some commenters suggested that the provisions of section 3001(b) are general and aspirational and that Congress did not intend for them to have any operative effect. Alternatively, some commenters supposed that these provisions operate ''in the aggregate'' or on the performance of ONC's functions on the whole but are not relevant to the National Coordinator's responsibility to oversee the Program or to perform other specific duties enumerated in section 3001(c). In support of this view, commenters asserted that other sections of the PHSA speak directly to the scope of the Program and the rules by which it should operate. In particular, section 3001(c)(5)(A) directs the National Coordinator to keep or recognize a program or programs for the voluntary certification of health IT as being in compliance with applicable certification criteria; and sections 3002 through 3004 establish the HIT Policy Committee (HITPC) and HIT Standards Committee (HITSC) and a consultative process for developing, endorsing, and adopting standards, implementation specifications, and certification criteria for inclusion in the Program. According to some of these commenters, this statutory design precludes ONC from enforcing requirements under the Program unless those requirements are expressed in certification criteria adopted through the processes noted above.

In contrast to these comments, several commenters recognized ONC's authority to directly review certified health IT in the manner proposed. Multiple commenters explicitly recognized ONC's broad authority to establish certification programs and to directly review certified health IT against a wide range of requirements. One commenter stated that our proposal was an appropriate exercise of this authority because it did not take a broad brush approach and limited oversight to areas where there is a potential risk to health or safety or a gap in oversight that could result in harm.

Response. We agree that ONC's role under the Program must comport with the National Coordinator's statutory authority under the HITECH Act. As we stated in the Proposed Rule, direct review helps enable the National Coordinator to fulfill the statutory duties specified in section 3001(b) and (c)(5) of the PHSA as they relate to keeping a certification program for the voluntary certification of health IT that allows for the electronic use and exchange of information consistent with ONC's purposes. This includes ensuring that each patient's health information is secure and protected, in accordance with applicable law; improving health care quality; reducing medical errors; reducing health care costs resulting from inefficiency, medical errors, inappropriate care, duplicative care, and incomplete information; and promoting a more effective marketplace, greater competition, greater systems analysis, increased consumer choice, and improved outcomes in health care services (*see* section 3001(b) of the PHSA).

We respectfully disagree with the interpretation advanced by some commenters that the National Coordinator is not bound to observe these statutory dictates in the administration and oversight of the Program. By its plain language, section 3001(b) is an express mandate to the National Coordinator to perform the duties delegated to him or her in a manner consistent with the core principles and requirements enumerated in that section.

It is true that some of the core principles and requirements in section 3001(b) are more relevant to the performance of some of the National Coordinator's duties than others, and that not every one of them is relevant to the performance of all of the National Coordinator's duties at all times or in the same way. It is also true that many of the core principles are stated broadly and permit substantial latitude in determining how corresponding requirements are to be met. But neither of these observations indicates that section 3001(b) was intended to be inoperative, as some commenters have suggested. To the contrary, section 3001(b) is a logical and expedient way to give effect to the purpose of ONC, by enumerating the core principles and requirements that in turn provide the basic parameters by which the National Coordinator must perform his or her duties and functions.

Even were that premise open to question, there is another reason to doubt that Congress would have intended the National Coordinator to administer and oversee the Program in a manner divorced from section 3001(b) of the PHSA. The purpose of ONC and the core principles and requirements expressed in section 3001(b), and the language and structure of the HITECH Act as a whole, leave no doubt that Congress intended a critical role for health IT and the use and exchange of electronic health information in improving health, transforming care, and enabling new frontiers in research and scientific discovery. To achieve these ends, Congress, through the HITECH Act, established the EHR Incentive Programs to encourage the meaningful use of EHR technology certified by ONC. As commenters point out, Congress also specified formal processes and an advisory committee apparatus to assist the National Coordinator in endorsing and adopting certification criteria for use in the Program. Having placed the Program and the certification of health IT at the center of this plan for developing and advancing the goals of a nationwide health IT infrastructure, Congress would have expected the National Coordinator to ensure that the Program furthers those goals and does not permit certified health IT to perform in ways that subvert them.

Finally, we reject the assertion that ONC is precluded from enforcing requirements of the Program other than those expressed in certification criteria adopted under section 3004 of the PHSA. As we explained most recently in the 2015 Edition final rule, the established requirements of the Program are not limited to compliance with certification criteria (80 FR 62710). For example, developers must disclose known material information about limitations and additional types of costs associated with their certified health IT (§ 170.523(k)(1)); comply with rules governing the use of the ONC Certification and Design Mark (§ 170.523(l)); submit user complaints to ONC–ACBs (§ 170.523(n)); make certified capabilities available in ways that enable them to be implemented and used in production environments for their intended purposes (80 FR 62710); cooperate with an ONC–ACB's surveillance of their certified health IT (80 FR 62716); and cooperate with and not seek to prevent or discourage an ONC–ACB from reporting the results of its surveillance activities (80 FR 62718). We have also explained that certification under the Program is conditioned on a health IT developer's compliance with certain Program requirements—independent of any particular certification criteria—that are necessary to the basic integrity and effectiveness of the Program (80 FR 62710, n.170). We discuss these requirements and their regulatory history immediately below in response to requests from commenters for additional clarification of the Program's requirements.

The foregoing considerations and our experience implementing the statutory provisions at issue leave no question that the National Coordinator has a duty to ensure that the certification of health IT under the Program furthers and does not subvert the core principles and requirements directly applicable to the National Coordinator's duties as enumerated in section 3001(b) of the PHSA. At a minimum, that includes updating the Program as necessary to provide effective oversight over problems or deficiencies with certified health IT that could lead to risks to public health or safety or to other outcomes that are inconsistent with the National Coordinator's responsibilities. We believe that the regulatory approach to direct review set forth in this rule is integral to fulfilling that duty.

Comments. Many commenters stated that there is a need for greater clarity and consistency concerning the requirements to which developers will be held under the Program. Several commenters asked us to define the requirements of the Program more explicitly, including by providing a clear definition of non-conformity. Commenters noted that unpublished or generalized Program requirements could be a source of confusion for developers or of capricious application by ONC. This could have unintended consequences such as discouraging investment and innovation in health IT because developers and investors may be reluctant to pursue innovative technologies if regulatory requirements are unclear.

Response. We agree that it is important to clearly communicate the requirements of the Program so that developers can design and make their certified health IT available in a manner that consistently meets Program requirements and the expectations of purchasers and users of certified health IT. In response to the comments, we explain in greater detail the sources of those requirements and the principles that ONC and ONC–ACBs apply when assessing whether they have been met.

In the 2015 Edition Final Rule, we explained that a non-conformity arises when certified health IT fails to conform to the requirements of its certification under the Program (80 FR 62710). Those requirements take various forms and may apply to aspects of the design and performance of the health IT, the ability of the health IT to support required capabilities and uses, and the responsibility of developers to make certified capabilities available in ways that enable them to be implemented and used in production environments for their intended purposes (80 FR 62710).

The certification criteria adopted under section 3004 of the PHSA form the core of the Program. In the 2010 interim final rule entitled Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology (75 FR 2013) (''Interim Final Rule''), we defined certification criteria as criteria to establish that health IT meets applicable standards and implementation specifications adopted by the Secretary or that are used to test and certify that health IT includes required capabilities (75 FR 2021–22; *see also* § 170.102). To meet these certification criteria, health IT must be able to perform required specifications and capabilities and, more generally, to do so in an accurate and reliable manner. For example, health IT certified to § 170.315(a)(1) (Computerized provider order entry—medications) must ''[e]nable a user to record, change, and access medication orders.'' Satisfying this criterion also plainly requires that the health IT perform this function accurately and reliably. For example, when a user enters a medication order for a patient, the health IT must accurately record the medication ordered and associate it with the patient selected by the user. Similarly, when a user accesses a list of medication orders for a particular patient, the health IT must not display medication orders for a different patient.

While certification criteria define the required capabilities of certified health IT, ensuring that health IT can perform certified capabilities is not the only requirement of the Program. In the 2015 Edition final rule, we adopted Program requirements under which developers must disclose on an ongoing basis any known material information about limitations and additional types of costs associated with any certified capabilities of their health IT (80 FR 62720). We have also adopted other Program requirements such as those related to the use of the ONC Certification and Design Mark and the submission of complaints to ONC–ACBs (§ 170.523(l) and (n), respectively). Developers must also submit information that is required to be included on the CHPL (80 FR 62725).

Finally, in previous rulemakings we have highlighted that there are certain overarching requirements of the Program, in addition to those described above, that are necessary to ensuring its basic integrity and effectiveness (*see, e.g.,* 80 FR 62710 n.170), thereby ensuring that the National Coordinator can meet his or her responsibilities under section 3001(b) of the PHSA. These requirements are part of the bases on which other requirements of the Program are understood and assessed.

A prime example is the duty of developers who participate in the Program to cooperate with the surveillance of their certified health IT. The Permanent Certification Program final rule incorporated requirements for ONC–ACBs to conduct surveillance to ensure that certified health IT continues to conform to the requirements of certification when it is implemented ''in the field'' (76 FR 1282). More recently, in the 2015 Edition final rule, we expanded these surveillance requirements and also stated our expectations for the performance of certified health IT in production environments. We explained that health IT developers have a responsibility to make their certified capabilities available to purchasers and users in a manner that allows them to be used for their intended purposes, including any uses reasonably within the scope of the health IT's certification (80 FR 62710). We stated that health IT would no longer conform to the requirements of its certification if customers or users were restricted from successfully implementing and using the technology for any purpose contemplated by the certification criteria to which the technology was certified (80 FR 62711). As an illustration, we said that a developer's failure to supply training materials and instructions necessary to access and successfully use data export capabilities described by § 170.315(b)(6) would constitute a non-conformity (80 FR 62711). Similarly, technical or other limitations that substantially interfere with the ability to access or use certified capabilities (or any aspect or intended uses of such capabilities) would give rise to a non-conformity (80 FR 62711). Further, even in the absence of any actual impairment, if a developer's actions would be likely to substantially impair the ability of one or more users (or prospective users) to implement or use certified capabilities for any purpose within the scope of applicable certification criteria, the technology would no longer conform to the requirements of its certification (80 FR 62711). Thus, we explained that the failure to disclose known material information about limitations or types of costs associated with certified health IT not only violates the express disclosure requirements at § 170.523(k)(1), but also constitutes a non-conformity to the certification criteria associated with the potentially affected capabilities (80 FR 62711).

Consistent with these established principles under the Program, certified health IT must be designed and made available to users in ways that allow certified capabilities to be used in an accurate and reliable manner, including in a manner that does not cause or contribute to serious risks to public health or safety or to other outcomes that are inconsistent with the National Coordinator's responsibilities under section 3001(b) of the PHSA. This requirement applies to the use of certified capabilities individually and in combination with other certified and uncertified capabilities of health IT. Just as the failure to disclose known material limitations or types of costs may impair the use of certified capabilities, the failure to design and make certified capabilities available so that they perform in an accurate and reliable manner impairs the safe and effective use of certified capabilities and is a non-conformity under the Program.

It is important to note that the foregoing examples and analysis assume that the putative non-conformity is a result of the actions of the developer or factors that are reasonably within the developer's ability to influence or control. As we have explained on prior occasions, a non-conformity does not arise when certified health IT fails to perform in an acceptable manner but where the failure is the result of factors that are far removed from the control or responsibility of the developer (80 FR 62710).

These principles are further elaborated and applied in the responses to specific comments throughout the remainder of this section (II.A.1.a) of the final rule. We have also included numerous examples to assist readers in understanding these principles and how ONC would apply them in particular circumstances.

Comments. Many commenters believed that ONC should review certified health IT against specific standards, implementation specifications, certification criteria, or other express requirements, preferably developed through formal rulemaking; otherwise, developers would have insufficient guidance to design and implement their products in a manner that complies with Program requirements, and any determinations made by ONC could be ad hoc and have the potential to be unfairly applied. For these reasons, several commenters urged us to initiate separate rulemaking to identify and adopt new certification criteria that would prescribe specific requirements that ONC would apply when reviewing certified health IT and determining whether it conforms to Program requirements.

Response. These comments raise many of the same concerns expressed in comments on the 2015 Edition proposed rule regarding then-proposed requirements for ONC–ACBs to conduct in-the-field surveillance of certified health IT. As we explained in finalizing those requirements, we understand the desire for bright-line rules; yet experience suggests that the fast-paced nature of technological change in the health IT landscape makes it impracticable to anticipate and prescribe detailed rules for every conceivable situation in which health IT may not conform to Program requirements (*see* 80 FR 62709). In practice, certified health IT may be integrated with a wide range of other systems, processes, and workflows and may be customized and used in many different ways. These circumstances, which are inherent to the production environment, are too numerous and varied to anticipate or to reduce to simple rules of universal application.

For the same reasons, we do not believe that adopting certification criteria would provide the clarity or certainty sought by advocates of that approach. We believe that clarity and predictability are best achieved by articulating and explaining the basic principles that govern our review of certified health IT, as we have done in our previous response above and in the examples and discussion of potential non-conformities throughout this section of the preamble. These principles are consistent with those that govern an ONC–ACB's surveillance of certified health IT in the field (80 FR 62709). As such, they will ensure that ONC's review of certified health IT is consistent and based on clear and predictable principles.

Comments. Multiple commenters stated that a non-conformity should be defined as occurring only when certified health IT can no longer complete or repeat the certification test procedures against which it was previously tested and on the basis of which the health IT was certified.

Response. We expressly rejected these arguments in the preamble to the 2015 Edition final rule (80 FR 62709). There, we explained that an ONC–ACB's assessment of certified health IT in the field is not limited to aspects of the technology that were tested in a controlled environment. Rather, an ONC–ACB must consider the unique circumstances and context in which the certified health IT is implemented and used in order to properly assess whether it continues to perform in a manner that complies with its certification.

Testing is an important part of an ONC–ACB's overall analysis of health IT under the Program. For practical reasons, however, testing focuses on particular use cases and necessarily reflects assumptions about how capabilities will be implemented and used in practice. Thus, while test results provide a preliminary indication that health IT meets the requirements of its certification and can support the capabilities required by the certification criteria to which the technology was certified, that determination is always subject to an ONC–ACB's ongoing surveillance, including the ONC–ACB's evaluation of certified capabilities in the field. Indeed, a fundamental purpose of in-the-field surveillance is to identify deficiencies that may be difficult to anticipate or that may not become apparent until after certified health IT is implemented and used in a production environment. That purpose would be entirely frustrated if an ONC–ACB's assessment of technology in the field were confined to those aspects of the technology's performance specifically delineated in test procedures.

For these same reasons, we again reject the position that Program requirements should be rigidly defined by test procedures instead of more meaningful performance outcomes. In assessing putative non-conformities in the course of ONC direct review, we consider the unique circumstances and context in which the certified health IT is implemented and used in order to properly assess whether it continues to perform in a manner that complies with the Program (*see,* 80 FR 62709).

Comments. Several commenters observed that the performance of health IT may be impacted by providers' implementation choices or other factors that the developer of the health IT may be unable to reasonably anticipate or control. One commenter explained that health IT developers do not necessarily control which third-party products their customers may deploy in conjunction with the developer's certified health IT and that it is not unusual for interface issues to arise because of updates to these unsupported products or uses. Commenters noted that developers may find it particularly difficult to anticipate and address interactions of their certified health IT with third-party products that are not certified under the Program or with capabilities or aspects of certified health IT that are not directly governed by certification criteria.

Response. In the 2015 Edition final rule, we recognized there may be instances in which the failure of certified health IT to perform required capabilities in the field may be due to factors that are beyond the ability of the health IT's developer to reasonably influence or control (80 FR 62710). Because the requirements of the Program focus on the responsibilities of health IT developers and those aspects of their technology that they can reasonably influence or control, we explained that the failure of health IT to perform in an acceptable manner would not constitute a non-conformity if the failure was caused exclusively by factors far removed from the control or responsibility of the developer.[4] We also explained that, in evaluating non-conformities in the field, ONC–ACBs are required to determine the reasons for the failure of health IT to function in an acceptable manner, taking into account the roles of the technology as well as the health IT developer, users, and other parties. If an ONC–ACB finds that the developer or its technology were a substantial cause of the failure, the ONC–ACB would conclude that the health IT does not meet the requirements of its certification. By contrast, if the ONC–ACB finds that the failure was caused exclusively by factors far removed from the control or responsibility of the developer, the ONC–ACB would regard those factors as beyond the scope of the health IT's certification and would not find a non-conformity.

These same principles apply equally to ONC's review of certified health IT. If in the course of reviewing certified health IT, ONC determines that the failure of the health IT to perform in an acceptable manner is the result of factors that, because they are far removed from the control or responsibility of the developer, were not within its ability to reasonably influence or control, ONC would not conclude that the certified health IT is non-conforming.

(2) Review of Uncertified Capabilities

In the Proposed Rule, we proposed that ONC could review the interaction of certified capabilities of health IT with uncertified capabilities. As defined earlier in section II.A.1.a of this final rule, we use the term ''certified capabilities'' to refer to any capabilities or other aspects of health IT that are certified under the Program. In contrast, other aspects of health IT are referred to as ''uncertified capabilities'' throughout this final rule. Uncertified capabilities may be integrated with certified capabilities within a single certified health IT product (*i.e.,* a certified Complete EHR or certified Health IT Module) or may be part of other health IT products or services that are not certified under the Program.

Comments. Several commenters supported our proposal to review certified health IT in a manner that recognizes that, in practice, certified capabilities frequently interact with uncertified capabilities, whether because a developer of certified health IT includes additional capabilities in its certified health IT product or because the developer's certified health IT product is deployed with or configured to work with other health IT products that are not certified under the Program. One commenter stated that a significant limitation of the Program to date has been the lack of an effective means to evaluate how certified capabilities of health IT are performing once they are deployed in the field and interact with other capabilities or products that are not certified under the Program.

In contrast, some commenters, including one health IT developer, suggested that it would be appropriate for ONC to review uncertified capabilities, but only in certain limited circumstances. One commenter recommended that such review be limited to situations in which a developer integrates uncertified ''components'' with its certified health IT in a manner that directly causes a material adverse impact on the ability of the certified health IT to function in accordance with certification requirements.

Other commenters categorically opposed this aspect of our proposal. Some of these commenters assumed, however, that ONC would review and make determinations about the performance of capabilities or products

[4] For example, in the 2015 Edition final rule we provided a hypothetical scenario in which a health IT developer's certified health IT could not demonstrate required capabilities in the field due to factors that were far removed from the developer's control or responsibility (80 FR 62710). In the scenario, a customer had instructed the developer to configure the certified health IT to use clinical decision support content from a third-party vendor with whom the developer had no sublicensing agreement. The customer agreed that it would be responsible for maintaining the necessary licenses for access to the third-party vendor's content. Despite the developer's warning, the customer failed to maintain the necessary licenses and access to the content was suspended, which prevented the certified health IT from functioning as expected.

that the commenters regarded as clearly beyond the scope of the Program. Some commenters even assumed that ONC would review health IT products that are not certified under the Program at all. According to these commenters, ONC's review of uncertified capabilities or other products would be inconsistent with the voluntary nature of the Program and would be a significant overstep of ONC's authority. One commenter, for example, stated that ONC had no authority to investigate uncertified ''components'' of certified health IT or to dictate how a developer builds and modifies a product in response to market mandates.

Response. It appears that many commenters interpreted this aspect of our proposal in a manner that was more far-reaching than we had either contemplated or proposed. The confusion appears to have resulted from our summary of the major provisions of the Proposed Rule, which stated that ONC's direct review ''may include certified capabilities and non-certified capabilities of the certified health IT'' and ''would extend to the interaction of certified and uncertified capabilities within the certified health IT and to the interaction of a certified health IT's capabilities with other products'' (81 FR 11058).

In explaining the purpose of the Proposed Rule, we stated that as certified capabilities of health IT interact with other capabilities in certified health IT and with other products, ONC's direct review would ensure that concerns *within the scope of the Program* can be appropriately addressed (81 FR 11057). As this statement suggests, the purpose of direct review is to evaluate and determine whether capabilities and other aspects of health IT that are certified under the Program conform to the Program's requirements. Nevertheless, because certified capabilities are frequently integrated or deployed with uncertified capabilities, evaluating whether a certified capability under review (the ''target capability'') conforms to the requirements of the Program may require understanding how the target capability is interacting with other capabilities of health IT. Those other capabilities may be certified under the Program or they may be uncertified capabilities. In the case of an uncertified capability, the capability may be part of the same ''product'' as the target capability or it may be part of a different product, which may or may not be certified under the Program. Whatever the case, to ensure that ONC can properly evaluate whether the target capability is functioning in an acceptable manner, we proposed that ONC may have to consider the interaction of the target capability with other capabilities that affect its performance, which could include uncertified capabilities, as discussed above. We did *not* propose, however, that uncertified capabilities would themselves become a target of ONC's review. In this sense, our statement that ONC's ''review'' would extend to the uncertified capabilities was somewhat inexact because ONC would be concerned with only the effects of the uncertified capabilities on the target capability, not with the performance of the uncertified capabilities in isolation. In other words, ONC's consideration of uncertified capabilities would be ancillary to its review of certified capabilities and limited to the extent necessary to determine whether those certified capabilities are functioning in a manner consistent with Program requirements.

As an illustration, consider a Health IT Module designed for ambulatory settings and that is certified to, among other criteria, § 170.314(b)(5) (Incorporate laboratory tests and values/results). Under the process established by this final rule, ONC could initiate direct review if, for example, it had reliable information that the Health IT Module were receiving and incorporating lab results incorrectly in a manner that was causing or contributing to missed diagnoses or improper management of serious medical conditions. ONC's review of the Health IT Module would be based on the Health IT Module's certified capabilities, which include the capability to incorporate lab results according to the standard specified in § 170.205(j) and, at a minimum, the version of the standard specified in § 170.207(c)(2). However, it may be that the lab results are being corrupted before they are received by the certified capability. To determine whether that is the case, it may be necessary for ONC to examine the capabilities of upstream health IT systems from which the Health IT Module receives lab results. This may include examining certified capabilities or uncertified capabilities of the upstream systems to the extent that those capabilities could be causing or contributing to incorrect data being transmitted to the receiving Health IT Module.

We reiterate that ONC does not intend to review the functioning of uncertified capabilities except to the extent that an uncertified capability interacts with and affects the performance of a certified capability that is under review. If ONC commenced review of certified health IT based on a reasonable belief that the certified health IT may not conform to the requirements of the Program, but subsequently determined that the problem or deficiency was related solely to the functioning of uncertified capabilities in isolation, ONC would cease its review of the certified health IT. We note that, as discussed subsequently in section II.A.1.a.(3) of this preamble, ONC may share any information obtained in connection with its review with other relevant agencies, to the extent permitted by law, including agencies with applicable federal oversight or enforcement authority.

With these clarifications, we believe the concerns raised in connection with this aspect of our proposal are misplaced. Contrary to those concerns, this final rule does not establish a process for ONC to make determinations about uncertified capabilities, nor to dictate how developers design uncertified capabilities within certified health IT or other technologies. ONC's consideration of uncertified capabilities will be ancillary to ONC's review of certified capabilities and limited to aspects of uncertified capabilities that interact with certified capabilities and are relevant to evaluating the performance of those certified capabilities. Further, we reiterate our expectation that direct review will occur relatively infrequently and will focus on situations that pose a risk to public health or safety or where ONC–ACBs may be unable to respond effectively.

Comments. A number of commenters raised concerns that the application of direct review to uncertified capabilities would be contrary to ONC's policy of encouraging flexibility in the way that health IT systems are configured and used. Commenters also expressed concern that direct review of uncertified capabilities could create regulatory uncertainty and would diminish innovation. Noting that developers regard the uncertified aspects of their health IT as a key area of differentiation from their competitors, commenters expressed fear that direct review of uncertified capabilities would crowd out innovation in this important area and diminish overall incentives to innovate and improve health IT capabilities.

Response. We are sensitive to the competition and innovation concerns raised by commenters. We believe that those concerns can be effectively addressed by clearly communicating the scope of ONC's direct review under this final rule and the limited extent to which it will impact developers of uncertified capabilities. We have explained the potential scope of ONC's review under the processes established by this final rule, including the extent to which ONC would consider the impact of uncertified capabilities on the performance of certified capabilities. In addition, section II.A.1.a.(3) of this preamble describes the types of circumstances in which ONC may invoke the processes for direct review set forth in this final rule.

To further communicate our intent and address the concerns raised by commenters, we reiterate that the purpose of direct review is to ensure that certified health IT functions in a manner that is consistent with the requirements of the Program. In the event that ONC determines that an uncertified capability is causing a certified capability to function in a manner inconsistent with Program requirements, ONC's determination would relate to the functioning of the certified capability at issue. Even in the event that an uncertified capability is identified as the cause of, or a contributing factor toward, certified health IT functioning in a manner inconsistent with Program requirements, direct review would not dictate whether or in what manner the uncertified capability should be modified. Any corrective action to be taken by the developer in response to a determination of non-conformity by ONC would relate to bringing the certified capability or capabilities into conformity. For example, appropriate corrective action might involve the developer taking steps to ensure that the certified capability does not interact with the uncertified capability that is causing it to function in an unsafe manner.

Comments. A number of commenters expressed concern that extending ONC's review to uncertified capabilities or to uncertified products would conflict with or duplicate oversight of health IT by other federal agencies.

Response. We acknowledge that the investigatory and enforcement authorities of other federal agencies might apply, in certain circumstances, to the performance and functioning of certified health IT. For several reasons, however, we disagree that ONC's review will conflict with or duplicate other oversight of health IT.

First, as discussed above, while ONC's review may encompass uncertified capabilities, ONC would only be concerned with aspects of the uncertified capabilities that interact with the certified capabilities that are the subject of ONC's review, and only to the extent necessary to assess whether the certified capabilities are functioning in accordance with Program requirements. This limited and ancillary consideration of uncertified capabilities would be unlikely to create any significant conflict with or duplication of any other agency's authority. Moreover, to the extent that ONC's review does uncover issues that fall within the purview of other agencies with relevant oversight or enforcement responsibilities, ONC could coordinate with and share any information or evidence it has obtained with such agencies, to the extent permitted by federal law, and, if appropriate, could pause or end its review.

Second, as discussed below in section II.A.1.a.(3) of this preamble, we have narrowed the scope of direct review under this final rule based in part on the ability of other agencies to provide appropriate oversight of certain types of non-conformities that would otherwise warrant ONC's review. For example, at this time, we have not finalized in this rule processes for ONC direct review of a suspected non-conformity solely on the basis that certified health IT may be compromising the security or protection of patients' health information (*see* section 3001(b)(1) of the PHSA) or increasing health care costs as a result of, for example, inefficiency or incomplete information (*see* section 3001(b)(3) of the PHSA). Our decision not to establish regulatory processes for such oversight at this time is based in part on the recognition that other agencies have the ability to investigate and respond to these types of issues and our desire to make the most efficient use of limited federal resources.

Third, far from conflicting with or duplicating the efforts of other agencies, we expect direct review to promote greater alignment in the oversight of health IT. Direct review allows ONC to coordinate with and provide expertise to other agencies, and to share any information or evidence ONC has obtained, as permitted by federal law. For example, ONC could quickly marshal and deploy resources and specialized expertise while working with federal counterparts to ensure a coordinated review and response to potential non-conformities. This approach is consistent with our inter-agency efforts to avoid regulatory duplication and promote appropriate, risk-based oversight of health IT, including efforts described in the Draft Food and Drug Administration Safety and Innovation Act (FDASIA) Health IT Report,[5] published jointly with the Food and Drug Administration (FDA) and the Federal Communications Commission (FCC). Indeed, the need for effective coordination could be especially important in responding to serious risks to public health or safety that arise from the complex interaction of health IT products that may include certified capabilities regulated by ONC as well as uncertified capabilities that may be subject to FDA, FCC, or another agency's oversight.

Finally, we note that ONC may elect to not initiate direct review (or, if it has initiated direct review, to cease such review) at any time and for any reason, including if ONC believes that another agency is better situated to investigate or address a suspected non-conformity, or if ONC believes that direct review could duplicate or interfere with the oversight or enforcement activities of other agencies. ONC may also coordinate with and share any information or evidence it has obtained, through its direct review or otherwise, with other agencies, to the extent permitted by federal law. We also anticipate that ONC may coordinate with ONC–ACBs, ONC–ATLs, the ONC–AA, and other entities in appropriate circumstances and consistent with applicable federal law.

(3) Scope of Review

We proposed that ONC may exercise direct review of certified health IT when there is reason to believe that the certified health IT may not conform to the requirements of the Program. We explained that ONC's review could be in response to concerns that certified health IT may be leading to medical errors or other outcomes that are inconsistent with the National Coordinator's responsibilities under section 3001 of the PHSA. We also stated there could also be other exigencies, distinct from public health or safety concerns, that for similar reasons would warrant ONC's direct review and action. In addition, we proposed that ONC may directly review certified health IT in situations that present unique challenges or issues that ONC–ACBs may be unable to effectively address without ONC's assistance or intervention. We listed a variety of factors in this regard that could help inform ONC's decision whether to initiate direct review in individual cases, specifically:

- The potential nature, severity, and extent of the suspected non-conformity or non-conformities, including the likelihood of systemic or widespread issues and impact.

[5] Draft FDASIA Health IT Report: Proposed Strategy and Recommendations for a Risk-Based Framework (April 2014), available at *https://www.healthit.gov/sites/default/files/fdasia_healthitreport_final.pdf.*

- The potential risk to public health or safety or other exigent circumstances.
- The need for an immediate and coordinated governmental response.
- Whether investigating, evaluating, or addressing the suspected non-conformity would require access to confidential or other information that is unavailable to an ONC–ACB; would present issues outside the scope of an ONC–ACB's accreditation; would exceed the resources or capacity of an ONC–ACB; or would involve novel or complex interpretations or application of certification criteria or other requirements.
- The potential for inconsistent application of certification requirements in the absence of direct review.

(*see* 81 FR 11061). We anticipated that ONC's direct review of certified health IT would be relatively infrequent and would focus on situations that pose a risk to public health or safety as well as other situations that present unique challenges or issues that ONC–ACBs may be unable to effectively address without ONC's assistance or intervention (based on consideration of the factors listed above). We stressed that our first and foremost desire would be to work with developers to address any non-conformities identified as a result of ONC's review.

Comments. A majority of commenters agreed that ONC should directly review certified health IT that could be leading to medical errors or other risks to public health or safety. One commenter representing health care professionals noted a strong need for ONC to adjust the Program to focus on the safety, usability, and interoperability of certified health IT, citing widespread concerns among the medical community about these issues. The commenter stated that ONC could play a valuable role in ensuring that the appropriate parties are identifying, analyzing, and correcting health IT safety concerns by quickly resolving non-conformity issues.

Several commenters who otherwise opposed direct review, including health IT developers, stated that it may be reasonable for ONC to review non-conformities as a "true last resort" when risks to patient safety are sufficiently compelling or when there is a gap or overlap in the ability of ONC–ACBs to effectively address the risk.

A small number of commenters categorically opposed this aspect of our proposal and stated that whether certified health IT is leading to medical errors or other risks to public health or safety is either beyond the scope of current certification criteria, other Program requirements, or section 3001(c)(5) of the PHSA. A few commenters, including one ONC–ACB, stated that health IT-related safety risks should not be addressed through the Program because there might be other channels, such as the proposed Health IT Safety Collaborative,[6] through which these issues could be more effectively dealt with, including by identifying health IT safety-related issues, defining appropriate best practices and criteria, and making objective assessments. Commenters also urged ONC to continue to support existing private-public initiatives that are developing a framework for the identification of health IT safety incidents to expand knowledge for all stakeholders.

Response. We thank commenters for their feedback and suggestions on this aspect of our proposal. Based on the comments, and consistent with the focus of the Proposed Rule, we continue to believe that direct review by ONC is necessary to address potential non-conformities and non-conformities in certified health IT that may be leading to medical errors or contributing to other risks to public health or safety. As we have explained, although ONC–ACBs play an important role in the Program, addressing the full range of these suspected non-conformities is beyond the scope of their responsibilities under the Program. In addition, ONC–ACBs may as a practical matter lack the expertise and resources to effectively respond to certain types of non-conformities, such as widespread or systemic problems with certified capabilities. Other agencies may similarly be unable to effectively respond to these issues, especially when the underlying causes are unclear or involve complex interactions among multiple health IT capabilities or products. As the capabilities of certified health IT evolve and become ubiquitous in the delivery of care, the National Coordinator has a responsibility to continually update and enhance oversight of the Program so that certified health IT continues to improve, and does not compromise, patient safety.

Addressing these types of issues will promote greater confidence in the safety of certified health IT and protect the integrity and effectiveness of the Program. Accordingly, § 170.580(a)(2) addresses the process for ONC to directly review certified health IT when the health IT may be causing or contributing to conditions that pose a serious risk to public health or safety. We note that the policy we have finalized is consistent with the general sentiment expressed by commenters, as we understand it, that ONC should exercise direct review judiciously, focusing on risks to public health or safety that are serious and on non-conformities that cannot be effectively addressed by ONC–ACBs. As we stated in the Proposed Rule, we expect that ONC's exercise of direct review will be relatively infrequent. We discuss these considerations in detail in our responses to the comments summarized immediately below.

We agree with commenters that advancing health IT safety is a shared responsibility and will require a concerted commitment by all relevant stakeholders, including through current public-private efforts and proposed initiatives such as the Health IT Safety Collaborative. We continue to strongly support these efforts and recognize the vital role they play in promoting the safety of health IT and the use of health IT to improve the safety and quality of care. We regard ONC's direct review as complementary to these efforts.

We disagree with the view expressed by some commenters that concerns related to the safety of certified health IT are beyond the scope of current certification criteria, other Program requirements, or section 3001(c)(5) of the PHSA. We refer commenters to our discussion of these issues in section II.A.1.a.(1) of this preamble.

Comments. We received relatively broad support for our proposal to enhance oversight of non-conformities that pose a risk to public health or safety, including through the direct review of such issues by ONC. A significant number of commenters urged us to prioritize public health and safety over other concerns by narrowing the scope of ONC's review to focus exclusively or primarily on non-conformities that pose serious risks to public health or safety. Commenters stated that this narrower focus would

[6] *See* Department of Health and Human Services, *Justification of Estimates for Appropriations Committee (Office of the National Coordinator for Health Information Technology),* app. IV, *https://www.healthit.gov/sites/default/files/final_onc_cj_fy_2017_clean.pdf* (2016) (proposing that Congress provide ONC with authority to establish a Health IT Safety Collaborative and provide adequate confidentiality protections). *See also* ONC, *Health IT Safety Center Roadmap, http://www.healthitsafety.org/uploads/4/3/6/4/43647387/roadmap.pdf* (2015) (containing task force recommendations for the development of a national Health IT Safety Center); Food and Drug Administration, *Draft FDASIA Health IT Report, https://www.healthit.gov/sites/default/files/fdasia_healthitreport_final.pdf* (2014) (recommending establishment of a Health IT Safety Center as a key component of a risk-based approach to health IT safety oversight and efforts to create a sustainable, integrated health IT learning system that avoids regulatory duplication and leverages and complements existing public and private sector activities to improve the safety and safe use of health IT).

allow ONC to concentrate its resources and provide more effective oversight of safety issues.

Many commenters also recognized the need for and supported ONC's review of non-conformities that, for other reasons, would be difficult for ONC–ACBs to effectively address.

Commenters were less supportive of applying ONC oversight of the Program to the other areas we had proposed, such as widespread non-conformities that could compromise the security or protection of patients' health information in violation of applicable law, or that could lead to inappropriate claims for reimbursement under federal health care programs. A substantial majority of commenters urged us to significantly narrow and more clearly define the types of non-conformities that ONC could potentially review. Commenters were concerned that, as proposed, ONC could conceivably review non-conformities that implicate any of a wide and diverse range of potential subjects, from security breaches, to anti-competitive practices, to conditions giving rise to health disparities. This could lead to regulatory uncertainty or arbitrary enforcement, and could discourage innovation in health IT.

For many of the same reasons, commenters urged us to clarify the specific types of circumstances or situations in which ONC would be likely to initiate direct review of certified health IT. While we had proposed several factors that ONC would consider in determining whether to initiate direct review, a number of commenters stated that these factors were too numerous or open-ended to provide useful guidance to stakeholders. Several commenters urged us to provide guidelines or examples explaining when ONC would be likely to initiate direct review. One commenter explained that by clarifying our methodology we could make the direct review process fairer and more equitable and establish confidence both in the process and its outcomes.

Response. We agree with commenters that the types of non-conformities ONC may review and, equally important, the types of circumstances in which ONC will take action to enforce Program requirements should be made as clear as possible and should be applied in a consistent and judicious manner. Such clarity and consistency help enable developers to design and make their certified health IT available in a manner that consistently meets Program requirements and the expectations of purchasers, licensees, and users of certified health IT. We also appreciate that uncertain or unnecessary regulation can have unintended consequences, including reducing incentives to invest in and to innovate the technologies that will make it possible to use health IT and health information to improve health and the delivery of care.

In light of these and other considerations described below, we have reconsidered and revised our proposal in several key respects. Importantly, while the PHSA provides the National Coordinator the authority to directly review certified health IT in the broad range of circumstances we proposed, at this time we have finalized a regulatory framework for the exercise of such review in a more limited set of circumstances. This scope of review is consistent with our expectation stated in the Proposed Rule that direct review will be relatively infrequent and will focus primarily on issues that pose a risk to public health or safety (81 FR 11058) or that ONC–ACBs may be unable to effectively address without ONC's assistance or intervention (81 FR 11061). While we stated that there could be other exigencies in addition to risks to public health and safety that could also warrant ONC's review, we agree with commenters that the need for additional ONC oversight in these areas is less pronounced at this time. In particular, we note the active oversight in these areas by other agencies, as discussed below. In light of this existing oversight and the limited resources at ONC's disposal, we agree with commenters that it is advisable to focus ONC's resources in areas in which, at this time, additional and direct oversight by ONC is most vital to ensuring the integrity and effectiveness of the Program. We believe that focusing ONC's review in these areas will help foster alignment and coordination with other agencies and promote confidence in the performance of certified health IT and the nation's health IT infrastructure, which will in turn support innovations and investments in health IT.

For all of these reasons, we have finalized processes in this rule for ONC to exercise direct review of certified health IT in two distinct sets of circumstances.

First, ONC may elect to directly review certified health IT when there is reason to believe that the certified health IT may be causing or contributing to serious risks to public health or safety. In these circumstances, ONC's direct review of certified health IT may be necessary to protect the public from certified health IT that is unsafe and to ensure the basic integrity and effectiveness of the Program. As explained in section II.A.1.a.(1) of this preamble, it is a requirement of the Program that certified health IT be made available in a manner that does not cause or contribute to serious risks to public health or safety. However, responding to the full range of these suspected non-conformities is beyond the scope of an ONC–ACB's expertise and responsibilities under the Program. In contrast, ONC is well-placed to respond to these issues, through the direct review processes established by this final rule, bringing to bear needed expertise and resources and coordinating activities with federal counterparts and other relevant entities to ensure a coordinated review and response to public health and safety concerns (81 FR 11061).

Second, in addition to serious risks to public health or safety, ONC may elect to directly review certified health IT on the basis of other suspected non-conformities that, while within the scope of an ONC–ACB's responsibilities, present practical challenges that may prevent the ONC–ACB from effectively investigating the suspected non-conformity or providing an appropriate response. In particular, ONC may directly review certified health IT if a suspected non-conformity presents issues that may require access to certain confidential or other information that is unavailable to an ONC–ACB; may require concurrent or overlapping reviews by multiple ONC–ACBs; or may exceed the scope of an ONC–ACB's resources or expertise. We believe that ONC's review of certified health IT in these situations will help ensure the continued effective oversight and administration of the Program.

The circumstances described above do not encompass all possible non-conformities of certified health IT. For example, certified health IT may not conform to the requirements of the Program if it is causing or contributing to other outcomes—distinct from risks to public health or safety—that are inconsistent with the National Coordinator's responsibilities, such as compromising the security or protection of patients' health information in violation of applicable law (*see* section 3001(b)(1) of the PHSA) or increasing health care costs resulting from, for example, inefficiency or incomplete documentation (*see* section 3001(b)(3) of the PHSA). At this time, however, we believe that other agencies are in the best position to provide effective federal oversight and enforcement in these areas. For example, within HHS, the Office for Civil Rights' (OCR) enforces the Privacy, Security, and Breach Notification Rules promulgated under the Health Insurance Portability and

Accountability Act of 1996 (HIPAA) and amended by the HITECH Act, and the Office of Inspector General (OIG) enforces a range of federal laws related to fraud, waste, and abuse. Therefore, we have not at this time finalized regulatory processes by which ONC would directly review certified health IT solely on the basis of circumstances distinct from public health or safety concerns or in cases where practical challenges prevent an ONC–ACB from effectively investigating the suspected non-conformity or providing an appropriate response, as discussed above (*compare* 81 FR 11061). We will continue to assess the need to exercise direct review in these additional circumstances, as necessary

As mentioned above, in this final rule, we seek to align ONC's direct review of certified health IT with oversight and enforcement responsibilities of other agencies. We therefore clarify that ONC may decline to exercise review of certified health IT for any reason, including if it believes that other agencies may be better situated to respond to a suspected non-conformity. Additionally, to the extent permitted by law, ONC may coordinate and share information with other agencies, including agencies with applicable oversight or enforcement responsibilities, and may engage other persons and entities, as appropriate, to effectively respond to suspected problems or issues with certified health IT.[7] Such agencies could include, for example, the Centers for Medicare and Medicaid Services, the Food and Drug Administration, the HHS Office for Civil Rights, the HHS Office of Inspector General, the Department of Veterans Affairs, the Federal Communications Commission, or state Medicaid agencies. We note that to the extent ONC exercises its discretion to engage in any efforts to identify or address non-conformities, such efforts and any resulting remediation (or the absence of such efforts or remediation) are not intended to impact the materiality of any non-conformity in a matter addressed by another agency; and nothing in this final rule is intended to supplant, delay, or in any way limit oversight or enforcement by other agencies, including any investigation, decision, legal action, or proceeding.

Finally, our decision to focus ONC's review, at this time, on the types of non-conformities described above allows us to provide a more structured decision-making regulatory framework to support the exercise of ONC's discretion to initiate review of certified health IT in the circumstances we have described. In contrast to the framework set forth in the Proposed Rule, we have simplified and defined with greater specificity the factors ONC will consider in determining whether to initiate direct review of a suspected non-conformity. The updated regulatory framework, which we have finalized at § 170.580(a)(2), provides a more sequential and targeted set of factors that ONC will consider when determining whether to initiate direct review. We have also eliminated duplicative or redundant factors included in the Proposed Rule, as discussed in more detail in our responses to comments on those factors below. These revisions will provide clear and predictable guidelines that will promote compliance with Program requirements while preserving incentives to develop and adopt new and innovative technologies.

Comments. Several commenters suggested that ONC should focus its oversight on risks to public health or safety that are ''clear,'' ''severe,'' ''immediate,'' ''extreme,'' or otherwise compelling. A few commenters stated that ONC should not exercise direct review unless the risk to patient safety or public health poses imminent risks to public health or safety. Commenters stated that focusing on these types of risks would ensure that ONC's limited resources are used to mitigate the problems or issues with certified health IT that pose the most serious risks of harm to patients and the public. Separately, some commenters stated that exercising direct review of all potential risks could be counter-productive in that it may discourage efforts to implement and use health IT to improve patient safety and care.

Relatedly, commenters requested additional specificity regarding the types of risks to public health or safety that could trigger ONC's review or give rise to a non-conformity. One commenter requested that ONC provide examples to illustrate how certified health IT might contribute to risks to patient safety and public health.

Response. We agree that not every risk to public health or safety necessitates ONC's direct review. We are also cognizant of the need to prioritize ONC's limited resources by focusing on the kinds of problems and other issues that, if not addressed through ONC's direct review, are most likely to lead to harm to patients or the public and undermine confidence in health IT and the integrity of the Program.

As described in section II.A.1.a.(1) of this preamble, to conform to the requirements of the Program certified health IT must be designed and made available to users in a way that allows certified capabilities to be used in an accurate and reliable manner. This includes making capabilities available in a manner that does not cause or contribute to medical errors or other conditions that give rise to serious risks to public health or safety. Direct review would be appropriate if ONC had reason to believe that certified health IT were causing or contributing to conditions that present a serious risk to public health or safety, including conditions that could result in serious injury or death, whether to a patient or to any other person.

Our focus on risks to public health or safety that are ''serious'' is consistent with the Proposed Rule, in which we suggested that ONC's direct review would be appropriate in response to certified health IT causing or contributing to medical errors or other exigent circumstances that call for an immediate or coordinated governmental response (81 FR 11058; *compare* proposed § 170.580(a)(1)(ii) through (iii) at 81 FR 11082). This focus also aligns with the general sentiment expressed by commenters that ONC's review of matters involving public health or safety should focus on risks that are ''clear,'' ''severe,'' ''immediate,'' ''extreme,'' or otherwise compelling. We note that these terms are not self-defining and that assessing whether certified health IT poses serious risks to public health or safety will necessarily involve a careful consideration of the relevant facts and circumstances in each case. To this end, ONC would consider the nature, extent, and severity of the risk and the conditions giving rise to it, in light of the information available to ONC at the time. In addition to any other factors that may be relevant, ONC would consider the apparent severity of the harm that might result, or has resulted, from the suspected unsafe conditions, including the likelihood of death or serious injury; the number of persons who may be harmed in the event that the harm were to materialize; and the likelihood that harm will in fact materialize if appropriate action is not taken. ONC would also consider the extent to which the risk of harm may be imminent such that an immediate or coordinated governmental response is necessary to significantly reduce the likelihood of actual harm occurring or recurring (§ 170.580(a)(2)(i)(B)). In evaluating whether the risk of harm may be imminent, ONC would also take into

[7] Example E in section II.A.1.a.(3) of this preamble illustrates the complementary roles of ONC's direct review and the activities of other agencies.

account any actions being taken to mitigate the risk, to the extent that ONC is aware of those actions. We have declined to adopt commenters' suggestions that ONC should focus exclusively on the ''imminence'' of a potential risk to public health or safety when determining whether to exercise direct review. While the nature of public health or safety risks dictates that in most cases they will be imminent, we can envision scenarios in which a risk might not be strictly ''imminent'' at the time ONC determines that it will initiate its review but might nonetheless lead to serious harm if not addressed. For example, ONC might decide to exercise direct review if it became aware of information about a serious safety risk that a developer, in concert with its healthcare provider customers, is managing by way of a complex series of manual ''work-arounds'' until the scheduled release of the developer's next software update. While the developer may assert that the risk to patients is not imminent because of the existence of the manual work-arounds, it may be necessary—both to protect patients and the integrity and effectiveness of the Program—for ONC to review the safety risk at issue immediately and not have to wait until such time as the manual work-arounds fail. ONC may, as part of direct review in this instance, determine that the risk to patient safety is such that, for the health IT to remain certified, the developer must rectify the deficiency by way of a patch and not wait until the developer's next scheduled software release.

Separate from information about unsafe conditions in particular, ONC could conclude that certified health IT poses a serious risk to public health or safety were it aware of information calling into question the validity of the health IT's certification. Such information might include, for example, credible allegations that a health IT developer obtained or maintained any part of the certification of its health IT by means of false or misleading statements or representations to an ONC–ACB; misrepresented or made false or misleading statements to customers or users about the certification or certified capabilities of the health IT; concealed problems, deficiencies, or potential non-conformities; or took other actions that would be likely either to compromise or to circumvent processes under the Program for testing, certifying, and conducting ongoing surveillance and review of certified health IT. These circumstances present a serious risk to public health or safety because obtaining and maintaining a valid certification is fundamental to ensuring that health IT meets Program requirements, including requirements essential to providing basic assurance that health IT is able to perform required capabilities in an accurate and reliable manner. Indeed, customers, implementers, and users rely on the certifications issued on behalf of ONC to provide this basic assurance so that they can select appropriate technologies and capabilities, identify potential implementation or performance issues, and implement certified health IT in a predictable, reliable, and successful manner (80 FR 62709). Where the validity of a certification is called into question, these and other persons are unknowingly deprived of this basic assurance upon which they rely.

To further illustrate these principles and how they would be applied in practice, we offer the following contrasting examples.

Example A: ONC receives multiple, detailed reports that a cloud-based EHR system (certified to the 2015 Edition) has become so slow that it may take up to five minutes to load a patient's record or to display information within a patient's record, such as the patient's medication and medication allergy lists. When providing emergency treatment, clinicians cannot wait five minutes for this information and must order medications with incomplete information about patients' current medications and medication allergies. Even when treatment is not urgent, the system's delays in responding lead many clinicians to assume that the EHR is not working and to order medications based on their best recollection of patients' current medications and allergies.

Clinicians at several hospitals in multiple states are experiencing these problems. There is no indication that these hospitals are maintaining substandard hardware or network infrastructure below the recommendations from the health IT developer, nor that they have customized their health IT in a way that would adversely affect system performance. The health IT did not behave this way when it was installed, but as the clinical data and number of records has grown the speed of the EHR's responsiveness has decreased.

In this example, ONC may initiate direct review of the certified health IT. The facts suggest that several capabilities of the certified health IT are implicated, including § 170.315(a)(6) (Problem list) and § 170.315(a)(7) (Medication list). The capabilities as implemented appear to be performing or interacting in a way that is causing or contributing to a serious risk of harm to public health or safety. The risk of harm is serious for several reasons. First, clinicians are abandoning use of the capabilities and resorting to memory to order medications for patients, which could result in severe harm to patients, including serious injury or death. Moreover, the risk is imminent because it is likely that harm will occur soon unless immediate action is taken to address the unsafe conditions. Further, the extent of the risk is large because the unsafe conditions have been reported at several hospitals in multiple states and may therefore put at risk a large number of patients.

Assuming ONC were to initiate direct review, it would examine the certified capabilities to determine why they are not performing in an accurate and reliable manner and whether the cause of the problem was within the ability of the health IT developer to reasonably influence or control. The facts suggest that the problem is common across multiple customers and is not the result of any actions of the developer's customers or users. Because the problem developed over time, the developer would have been aware of the problem and could have prevented it by employing best software practices to prevent a system related slow-down under load. If this were established, ONC would find a non-conformity.

Example B: ONC receives credible information from multiple sources that a large hospital's EHR system, which is certified to the 2015 Edition, is dropping medication orders. While the cause of the dropped orders is not yet clear, data in patients' records is not being recorded in a consistent and reliable manner, which is leading to patients not receiving medications.

Based on the information it has received, ONC believes that the EHR system's computerized provider order entry (CPOE) capability for medications (§ 170.315(a)(1)) may be interacting with other capabilities within the EHR or within other health IT in a way that is causing or contributing to orders not arriving when they are needed. This poses a serious risk to public health or safety because there is an imminent risk that patients will not receive needed or even life-saving medications that have been ordered for them, which could result in severe harm.

Accordingly, ONC initiates review of the certified health IT. However, during the course of its review, ONC determines that the hospital had chosen not to install and maintain the minimum specified hardware and network requirements published by the developer of the certified health IT. As a direct result of the substandard hardware and network connectivity, the certified health IT is suffering system timeouts, losing network packets, and not operating correctly. Based on these findings, ONC finds that while the certified capability is not performing in an acceptable manner, the reason for the substandard performance is that the hospital has chosen not to follow the developer's minimum hardware and network recommendations. The hospital's decision to intentionally disregard the developer's clear instructions regarding the safe use of its technology is a factor that is beyond the ability of the developer to reasonably influence or control. Therefore, ONC would not find a non-conformity and would cease its review. ONC may, however, refer the matter (and information or evidence obtained as a result of its review) to other agencies with applicable oversight or enforcement responsibilities, as discussed above in this section of the preamble.

Example C: ONC receives multiple reports from a large hospital concerning a potential problem with its EHR. Over the past week, several patients with congestive heart failure (CHF) had to be readmitted because of CHF exacerbations. Clinical and IT staff at the hospital have investigated the problem and believe that it is due to an error in the hospital's EHR, which is certified to the 2015 Edition. The hospital reports that its CHF patients are all given electronic scales that record their weight and automatically transmit the daily weight back to the hospital's EHR. The weight can be tracked and the patients can be alerted if they are gaining too much weight (from excess fluid, one of the signs of a CHF exacerbation) and need to adjust their CHF medications accordingly. The readmissions happened due to inaccurate weight data being presented to clinicians, which caused the clinicians to not adjust diuretic medication to manage patients' fluid status appropriately.

Based on these facts, ONC may initiate direct review of the certified health IT. ONC could form a reasonable belief that the certified health IT may be causing or contributing to serious risks to public health or safety, in violation of Program requirements. A number of certified capabilities appear to be implicated, including § 170.315(e)(3) (Patient Health Information Capture) and certified capabilities that interact with vital signs data (which is part of the Common Clinical Data Set (§ 170.102)). Although the cause of the problem is not yet clear, it is reasonable to believe that it may be a result of one or more of these certified capabilities or of their interaction with other uncertified capabilities or products. Meanwhile, the occurrence of multiple readmissions in the past week suggests that, if the certified health IT is causing or contributing to these risks to public health or safety, the risks are sufficiently serious as to constitute a non-conformity and to warrant ONC's review.

Example D: ONC becomes aware of a patient safety hazard at a large area hospital. In one reported case, a patient with chest pain entered the emergency department (ED) of the hospital. In the ED, nurses enter protocol orders for patients with chest pain on behalf of the attending physician. On this occasion, an attending physician accessed the patient's record in the EHR and, observing that no blood tests had been ordered, proceeded to order the tests from the standard order set. Contemporaneously, a nurse was in the process of entering the same tests from the same order set. The nurse completed her order a few seconds before the physician completed hers. Neither the nurse nor physician recall any duplicate order alerts, although hospital IT staff state that clinical decision support (CDS) was active in the EHR system and had been configured to intercept and display alerts when duplicate orders are entered. The duplicate orders were noticed later when the physician was reviewing the patient's record in the EHR. At that time, the physician cancelled the nurse's order, which thereafter was no longer displayed in the EHR. The EHR continued to display the physician's order with a status of ''pending collection.'' The lab system assumed that the identical lab requests for the same patient were duplicates and cancelled the physician's request because the nurse's request had arrived first. The lab system, however, did not create an outgoing interface message to the ordering EHR indicating that the physician's ''duplicate'' request had been cancelled. As a result, the physician's order continued to be displayed in the EHR with a status of ''pending collection.''

Back in the ED, alert staff noticed that the labs had not been drawn within the expected time frame, and reordered the tests. Fortunately no harm resulted to the patient. However, the hospital's clinical staff and leadership believe the EHR presents a serious patient safety hazard. The clinicians report the incident to ONC and note that in a large and busy ED it is not uncommon for clinicians to enter contemporaneous orders; and that they expect the EHR to alert them when this occurs and to intercept duplicate orders before they are transmitted. The hospital's IT staff and the EHR developer, with whom the IT staff have been working to analyze this incident, believe that the EHR was configured to provide these CDS interventions. Neither the hospital's IT staff nor the EHR developer has been able to ascertain why these safeguards appear to have failed in this case. Based on these facts, ONC could form a reasonable belief that the certified health IT may be causing or contributing to a serious risk to public health or safety. As noted by the hospital's clinical staff and leadership, duplicate orders are not uncommon, especially in a large and busy ED. If not detected, the duplicate orders may lead to a wide range of serious hazards, such as administration of unnecessary tests or excessive medication dosages. And as illustrated by this example, the failure to detect and intercept duplicate orders may also have downstream effects that could prevent the fulfillment of orders and result in patients not receiving timely test results and treatment. The severity and extent of the harm that could occur is significant and is likely to materialize unless the cause of the problem is isolated and resolved. That the hospital's IT staff and the EHR developer are cooperating and yet have been unable to ascertain the cause of the problem is also relevant to ONC's consideration because it suggests that the problem could reoccur and that the full extent of the problem, including for other hospitals or facilities that use the developer's EHR, is not known.

While the risk to public health or safety is clear, to initiate direct review, ONC must have a reasonable belief that the certified health IT may be causing or contributing to that risk. Here, there are at least two certified capabilities that are potentially implicated: CPOE (§ 170.315(a)(3)) and CDS (§ 170.315(a)(9)). This nexus to certified capabilities is sufficient for ONC to initiate direct review.

Concurrently, ONC might direct the responsible ONC–ACB to perform surveillance of issues that are within the scope of its responsibilities and expertise. Here, an ONC–ACB could conduct in-the-field surveillance of the CPOE and CDS capabilities to determine whether there is a non-conformity to the requirements of § 170.315(a)(3) or (a)(9). For example, the ONC–ACB would be well-positioned to determine through in-the-field surveillance whether the certified CDS capability, when properly configured to intercept and alert users to duplicate orders, consistently triggers those interventions in a reliable manner in a production environment.

On the other hand, an ONC–ACB may be unable to analyze other possible non-conformities. For example, it may be that the CDS reliably displays alerts as intended but that the alerts are designed in a way that makes them susceptible to being inadvertently overridden. These usability considerations are within the scope of the Program's requirements but may be best suited for ONC to review. ONC could also examine the interaction of the certified capabilities with the receiving lab system (which may or may not be certified under the Program), which in this example is critical to isolating and understanding the nature of the problem and assessing whether the certified health IT conforms to Program requirements. In reaching that determination, ONC would consider whether the EHR developer could have reasonably anticipated that the lab system would cancel the orders without sending a notification of the cancellation and whether it could have taken reasonable steps to mitigate this risk (such as warning users to manually confirm the orders or providing a bi-directional interface that ensures that users are able to view when orders are in fact received and filled). This may require analyzing the EHR developer's interfaces and contractual agreements with the lab system as well as the EHR developer's field testing and quality assurance procedures. Again, these factors may be beyond the expertise of the ONC–ACB and better suited for ONC's review.

As the foregoing examples illustrate, the particular facts and circumstances that may trigger ONC's review of certified health IT will be unique to each case, as will be the analysis of the issues relevant to determining whether the certified health IT conforms to Program requirements. Nevertheless, we believe the examples above will help stakeholders understand the types of risks to public health or safety that may prompt ONC's review and that may lead to a finding of non-conformity. We anticipate issuing additional guidance on these and other aspects of this final rule as appropriate.

Comments. A small number of commenters distinguished between risks to patient safety and those related to broader public safety or public health. Some commenters stated that direct review would not be appropriate in circumstances that pose a risk of harm to public health but not specifically to patient safety. In contrast, one commenter posited that public health considerations may justify or weigh in favor of direct review in certain situations, such as where problems with certified health IT may adversely impact socially or medically vulnerable populations.

Response. We intend the term public health or safety to encompass risks to both patients and other persons. Given the central role of health IT in delivering care, it is likely that ONC's oversight will focus on risks of harm to patients. However, we would be no less concerned if certified health IT were causing or contributing to risks of harm to persons other than patients, and we believe that the National Coordinator's responsibility to provide for effective oversight of certified health IT so that it does not create unreasonable risks of harm to patient safety applies with equal force to risks involving public health.

We note that under the approach we have finalized, ONC would consider the potential nature of a public health or safety risk when reaching a determination whether to initiate direct review. Thus ONC's determination would take into account the impact that the potential risk is having, or might have, on a patient(s). This determination would necessarily involve an analysis of the risk as it relates to the affected patient population.

Comments. A number of commenters voiced concerns about the factors that ONC would consider when determining whether to initiate direct review, characterizing those factors as overly broad and creating a risk of arbitrary application. Commenters noted in particular that the phrase ''other exigent circumstances'' was ambiguous. Some commenters suggested that ONC's potential reliance on such an open ended factor would enable ONC to exercise direct review in an unaccountable manner. Commenters requested clarification or reconsideration of the inclusion of ''other exigent circumstances'' as a factor to be considered by ONC when initiating direct review.

Response. We identified a number of factors in the Proposed Rule that ONC might consider when determining whether to exercise its discretion to initiate direct review. These factors were included to provide health IT developers with some comfort that while ONC's authority to initiate direct review is broad, ONC's use of direct review would be guided by principles that focus ONC's limited resources on the oversight of non-conformities that pose substantial risks to the integrity and effectiveness of the Program. Indeed, the inclusion in the proposal of the phrase ''other exigent circumstances'' was intended to narrow ONC's discretion rather than, as suggested by commenters, provide ONC with a degree of flexibility that would make ONC's exercise of direct review unaccountable. Notwithstanding this, we acknowledge commenters' concerns regarding the open-ended nature of the phrase ''other exigent circumstances.'' We maintain that there could be other exigencies, distinct from public health or safety concerns, that pose risks to the integrity and effectiveness of the Program and warrant ONC's direct review and action. However, at this time, our decision to focus on public health and safety risks (in addition to non-conformities over which, for practical or other reasons, ONC–ACBs may be unable to provide effective oversight) at this stage of our administration of the Program has enabled us to omit any reference in the final rule to ONC considering ''other exigent circumstances'' when determining whether to exercise direct review.

We clarify that while under the processes established by this final rule ONC would not, at this time, initiate direct review solely on the basis of exigencies other than serious risks to public health or safety, and while ONC's review would focus on aspects of health IT that are certified under the Program, ONC would not be precluded from sharing, to the extent permitted by federal law, any information or evidence (including about other exigent circumstances or problems with uncertified capabilities of health IT) with other relevant agencies, including law enforcement or other agencies who may be able to address such matters. Conversely, ONC may receive information about potential non-conformities or non-conformities from other agencies in the course of their oversight, enforcement, or other activities. As an illustration, consider the following example.

Example E: A Health IT Module certified to the 2015 Edition (''the EHR'') is the subject of a ''ransomware'' attack. The attacker gained unauthorized access to the EHR at multiple health care facilities and deployed malicious software that rendered patients' electronic health information completely inaccessible to clinicians and other users of the EHR. Several of these facilities have reverted to backup systems, including in some cases paper records and manual workflows that significantly increase the risks of medical errors and harm to patients. Several federal agencies (''the Agencies'') are currently investigating the attack. The Agencies request the assistance and expertise of ONC's Chief Privacy Officer to better understand the role of the EHR in contributing to the incident. The investigation quickly reveals that the attacker exploited a vulnerability in the operating system software (OS) used in conjunction with the EHR. The OS was out of date and no longer receiving security updates. The Agencies, concerned about the prospect of additional security breaches, share this information confidentially with ONC.

For the reasons stated earlier in section II.A.1.a.(3) of this preamble, ONC would not initiate direct review of the certified health IT solely on the basis of security incidents or other exigencies that are distinct from risks to public health or safety. At this time, we believe that other agencies are currently best positioned to provide effective oversight and enforcement of health IT with respect to these potential exigencies. Nevertheless, as the facts of this example make clear, these exigencies may also give rise to serious risks to public health or safety. Where certified health IT may be causing or contributing to risks of this kind, ONC may initiate direct review to protect the public and the integrity and effectiveness of the Program.

Here, ONC initiates direct review based on the information received from the Agencies. To ensure that ONC's review assists and does not in any way hinder the ongoing investigation, ONC carefully coordinates with the Agencies and shares information and evidence it obtains during its review. ONC's review confirms that the developer of the EHR requires users to install and use a version of the OS that is no longer supported by the OS manufacturer and is not receiving security updates. All certified capabilities of the EHR are affected by this requirement, which exposes users to vulnerabilities and attacks that could compromise patient data and result in serious harm to patients. At the same time, ONC finds that the developer could have reasonably anticipated, and avoided, these risks because the OS manufacturer had published many notices that the version of the OS was being retired and would no longer receive security updates. Based on these findings, ONC issues a notice of non-conformity to the developer.

By contrast, if ONC had found that the health IT developer offers an upgrade path to the latest versions of the operating system software, and encourages its users to upgrade, ONC would not find a non-conformity if users decided to not install the upgrade.

Comments. Commenters suggested that we clarify our proposed methodology for assessing the ''nature, severity, and extent'' of a suspected non-conformity and the significance of this factor to ONC's determination whether to initiate direct review.

Response. In response to the concerns raised by commenters, we have made a number of adjustments in the final rule that will create greater predictability for the process that ONC will use to determine when to initiate direct review.

The proposals in the Proposed Rule outlined a direct review process in which ONC would exercise wide latitude to consider and weigh factors when determining whether to initiate direct review. As proposed, ONC might evaluate a number of factors that could be relevant to the particular circumstances at issue at the same time. However, at this time, we have chosen to narrow the scope of potential non-conformities and non-conformities ONC will review as described above. Given this narrower scope, we are able to delineate the specific factors that ONC will consider and apply when determining whether to initiate direct review of certified health IT.

Under the final rule, the nature, severity, and extent of a non-conformity would be relevant if ONC were to initiate review of a suspected non-conformity on the basis of public health or safety concerns. In that instance, ONC would have a reasonable belief that certified health IT may be causing or contributing to conditions that pose a serious risk to public health or safety. The potential nature, severity, and extent of the suspected conditions giving rise to that risk would be directly relevant to this determination, as would the need for an immediate or coordinated governmental response. These considerations are described in greater detail earlier in section II.A.1.a.(3) of this preamble. We have expressly included these considerations as factors that ONC will consider when determining whether certified health IT may be causing or contributing to risks that are sufficiently serious as to suspect that the certified health IT does not conform to the requirements of the Program and ONC's direct review.

Separately, and as also discussed in section II.A.1.a.(3) of this preamble, ONC may directly review certified health IT when a suspected non-conformity, while based on requirements of the Program that are generally within the scope of an ONC–ACB's responsibilities to administer and enforce, presents issues that may prevent the ONC–ACB from effectively investigating or responding. The nature, severity, and extent of a suspected non-conformity may be relevant to this determination. For example, the suspected non-conformity may be so systemic, complex, or widespread that an ONC–ACB would lack the resources or expertise to effectively investigate or respond to it. On this basis, ONC may directly review the suspected non-conformity.

Comments. One commenter suggested that ONC include additional factors for assessing when to exercise its direct review. This commenter recommended that ONC develop an additional factor that ensures that ONC's decision to initiate direct review takes into account the impact of non-conformities on socially and medically vulnerable populations.

Response. Under the final rule, ONC will consider the potential nature, severity, and extent of a public health or safety risk when reaching a determination as to whether to initiate direct review. This determination would take into account the potential impact the risk is having, or might have, on a patient(s) or the public. We anticipate that an analysis of the affected population could be relevant to that determination. For example, an issue might present a less serious risk of harm to patients at a large tertiary hospital with in-house IT staff and robust quality assurance processes than to patients served by a safety-net provider with no in-house IT expertise and less extensive quality controls and resources than might be available to a large institution.

Comments. Many commenters expressed support for ONC direct review in situations where ONC–ACBs may be unable to effectively investigate or respond to potential non-conformities. Several commenters recognized that there may be a variety of situations in which ONC–ACBs are unable to effectively investigate and respond to non-conformities, such as where doing so would require access to confidential or other information that is unavailable to an ONC–ACB, would exceed the resources or capacity of an ONC–ACB, or would involve novel or complex interpretations or application of certification criteria or other Program requirements. One commenter recommended that ONC invest in and empower ONC–ACBs to enable them to investigate and address non-conformities that are currently beyond the scope of their responsibilities under the Program.

All three ONC–ACBs commented on this aspect of our proposal. One ONC–ACB related that in its own surveillance it had encountered scenarios in which

ONC's direct oversight would have proven beneficial to the situation and its resolution. Another ONC–ACB stated that it had received complaints from users of certified health IT that raised issues (including issues related to patient safety) that were beyond the scope of the ONC–ACBs' accreditation and ability to address but that could be governed by the broader requirements of the Program. The remaining ONC–ACB did not believe that ONC should enforce any Program requirements that ONC–ACBs themselves could not administer in accordance with their accreditation; however, the ONC–ACB did support ONC's direct review of non-conformities whose nature, severity, or extent would be likely to quickly consume or exceed an ONC–ACB's resources or capacity.

Some commenters suggested that ONC should only intervene due to ONC–ACB limitations in very limited circumstances and that ONC should use its discretion in this respect as a ''last resort.'' One commenter suggested that ONC refine the factors that it will consider when determining whether to initiate direct review on this basis. Another commenter suggested that ONC should only initiate direct review on the basis of ONC–ACB limitations when clearly defined criteria are met; the commenter provided the example of a non-conformity involving the interaction of two health IT products certified by separate ONC–ACBs and having a proven and urgent impact on patient safety.

Response. We thank commenters for their support and thoughtful comments on this aspect of our proposal. We have adopted the proposed approach to ONC direct review when ONC–ACBs may lack necessary expertise or resources, with the following clarifications. ONC may exercise direct review on the basis of suspected non-conformities that, while generally within the scope of an ONC–ACB's responsibilities and expertise, may present issues that could prevent an ONC–ACB from effectively investigating or providing an effective response. In these circumstances, ONC's direct review of the certified health IT is appropriate to help ensure consistency in the effective oversight and administration of the Program. Specifically, under the processes established in this final rule, ONC may directly review certified health IT if investigating or responding to a suspected non-conformity may require access to confidential or other information that is unavailable to an ONC–ACB (§ 170.580(a)(ii)(A)); may require concurrent or overlapping reviews by multiple ONC–ACBs (§ 170.580(a)(ii)(B)); or may exceed the scope of an ONC–ACB's resources or expertise (§ 170.580(a)(ii)(C)).

In response to the comments and to provide additional clarity regarding the types of circumstances that may exceed an ONC–ACB's resources or expertise, we provide the following example, which includes three alternative scenarios. The scenarios, which are mutually exclusive, illustrate how variations in facts and circumstances may give rise to different issues that necessitate different levels of involvement and forms of collaboration between ONC and ONC–ACBs.

Example F: An EHR system certified to the 2015 Edition is in use by several major hospitals and health systems, including their ambulatory clinics, in multiple states. During a span of two weeks, over a dozen users at multiple health care facilities report to ONC and to the ONC–ACB that the EHR is displaying inaccurate or missing diagnoses (problems) and that, as a result, patients are not receiving appropriate care. In one reported instance, a patient was diagnosed with renal impairment, and this diagnosis was entered into the patient's active problem list in the EHR by her primary care physician (PCP). The PCP then referred the patient to an orthopedist for an unrelated musculoskeletal issue. The orthopedist is affiliated with the same health system as the PCP and has access to the same instance of the EHR. When the orthopedist accessed the patient's problem list, the diagnosis for renal impairment was missing from any relevant sections as displayed in the EHR. Unaware of this diagnosis, the orthopedist prescribed a medication for musculoskeletal pain that should either be avoided or minimized in patients with renal impairment. As a result, the patient suffered acute renal failure. Similar instances involving other missed or inaccurate diagnoses and resulting harm to patients have also been reported to ONC and the ONC–ACB.

Based on the information described above, the ONC–ACB initiates in-the-field surveillance of the certified health IT, as required by § 170.556(b), to assess whether the problem list capability continues to conform to the requirements of the certification criterion at § 170.315(a)(6) (Problem list). Separately, because the certified health IT may be performing in a manner that is causing or contributing to a serious risk to public or health or safety, ONC also initiates direct review of the certified health IT on this basis. ONC does not exercise exclusive[8] review under the Program at this time.

Scenario 1

The ONC–ACB's in-the-field surveillance reveals that the cause of the issue is a software error that is only found in one EHR ''workflow.'' The EHR presents the user with multiple ways, or screens, to accomplish the same task. In this case, the PCP modified the problem list from a ''quick summary screen,'' which due to a software error did not write the updated diagnosis (problem) back to the database. This led to a situation where the PCP thought the diagnosis had been updated, but in fact on the back end, the list had not been updated. The EHR, when tested for certification, had presented the ''standard office visit'' screen for diagnosis list modification but not the ''quick summary screen,'' which is an alternate workflow available only in production.

The ONC–ACB concludes that the failure of the problem list capability to function in accordance with § 170.315(a)(6) was reasonably within the control of the developer, who should have anticipated the risk during the course of normal software development. Any additional read/write/display functionality may initially contain code errors, and all functions of certified health IT should be subjected to adequate testing. The developer could have reasonably taken actions to avoid the risk by employing an adequate software regression testing methodology.

Based on the surveillance and analysis above, the ONC–ACB finds a non-conformity to § 170.315(a)(6) and requires the developer to take corrective action, pursuant to § 170.556(d), including by submitting a CAP in accordance with §§ 170.556(d)(1)–(4) that addresses how the developer will resolve the identified non-conformity and related deficiencies across all of the developer's customers and users. ONC, in coordination with the ONC–ACB, concurs with the ONC–ACB's finding of non-conformity and, at this time, forbears from taking any action against the developer because the non-conformity involves a straightforward violation of a certification criterion, which is well within the scope of the

[8] Under the final provisions, ONC may assert exclusive review of certified health IT as to any matters under its review and any similar matters under surveillance by an ONC–ACB. In determining if matters are similar, ONC will, as proposed, consider whether the matters are so intrinsically linked that divergent determinations between ONC and an ONC–ACB would be inconsistent with the effective administration or oversight of the Program.

ONC–ACB's responsibilities and does not appear to exceed the ONC–ACB's resources. ONC continues to closely monitor the situation and coordinate with the ONC–ACB. If at any time ONC were to believe that the ONC–ACB could not effectively administer the necessary corrective action or that ONC's direct intervention were necessary to more quickly and effectively mitigate the risk to public health or safety, ONC could immediately issue a notice of non-conformity and notice of suspension, as described in section II.A.1.c of this preamble.

Scenario 2

The ONC–ACB's in-the-field surveillance reveals that the missing diagnosis was due to a system workflow implementation that the healthcare organization had customized. Contrary to the developer's recommendations, the healthcare organization had removed the problem list from the ''quick visit'' EHR workflow that is presented to ambulatory PCPs. This resulted in the PCP not being able to quickly and easily update the problem list properly, resulting in incomplete problem lists.

In contrast to scenario 1, the ONC–ACB finds that there is no non-conformity because these factors are beyond the developer's ability to reasonably influence or control. ONC concurs with the ONC–ACB's determination and ceases its direct review of the certified Health IT Module(s).

Scenario 3

Based on its in-the-field surveillance, the ONC–ACB finds that the problem list capability is functioning in accordance with § 170.315(a)(6). Specifically, the ONC–ACB concludes that the issue is not the result of any technical or functional deficiencies with the problem list capability but rather the manner in which the problem list's user interface has been designed, which is unintuitive and appears to have contributed to problems being recorded incorrectly or not at all. The ONC–ACB shares its findings with ONC and states that these usability issues are beyond the scope of the ONC–ACB's expertise and its responsibilities under the Program because a complete assessment of these issues would appear to require an assessment of the developer's software development processes in light of current software usability and human factors best practices.

ONC agrees that these issues are beyond the scope of the ONC–ACB's expertise and responsibilities under the Program. However, the issues are not beyond the scope of the Program. ONC concludes that the problem list capability was designed in a way that does not adhere to commonly accepted usability guidelines. In this case, ONC finds that in order to add a diagnosis to the problem list, a user is forced to navigate through an excessive series of windows, confirmation dialogues, and an inordinate amount of clicks to properly select the correct diagnosis. This in turn results in incomplete problem lists due to clinicians' difficulty navigating the overly complex workflow, inability to complete the laborious series of steps due to time constraints, or a combination of both factors.

On the basis of these findings, ONC concludes that the certified health IT does not conform to the requirements of the Program. As discussed in section II.A.1.a.(1) of this preamble, certified health IT must be designed and made available to users in ways that allow certified capabilities to be used in an accurate and reliable manner, including in a manner that does not cause or contribute to serious risks to public health or safety. Where certified capabilities do not perform in such a manner due to factors that the developer could have reasonably influenced or controlled, the certified capabilities do not conform to the requirements of the Program. Here, the developer could have reasonably anticipated the risk through an understanding of software usability and human factors best practices, and the developer could have reasonably taken actions to avoid the risk, such as by ensuring adequate usability testing prior to software release. ONC would follow the processes discussed in section II.A.1.c of this preamble to notify the developer of the non-conformity and to work with the developer to expeditiously and comprehensively correct the non-conformity and prevent similar safety risks from recurring. This might include, for example, instituting corrective actions to assist the developer in improving its user-centered design and other quality assurance processes.

The example and scenarios above illustrate our intent that ONC's direct review complement and provide a ''backstop'' to the surveillance and other activities of ONC–ACBs so that suspected non-conformities requiring attention do not go unaddressed. To this end, ONC may consult with the ONC–AA, ONC–ACB(s), and other persons or entities, as appropriate, when determining whether to exercise direct review and in conducting such review. ONC may also share relevant information with the ONC–AA, ONC–ACB(s), and other relevant persons and entities as appropriate to assist ONC–ACB surveillance and other activities to address issues with certified health IT, to the extent that the sharing of such information is permitted by law. We believe that such communication will help ONC–ACBs as well as ONC accurately and effectively assess certain issues with certified health IT products. We continue to maintain that reviews by ONC–ACBs and ONC will be complementary and will support comprehensive and consistent review of certified health IT.

Comments. Multiple commenters stated that ONC should not review certified health IT on the basis that a potential non-conformity raises novel or complex interpretations or applications of certification criteria (*see* proposed § 170.580(a)(1)(iv)(D)) or could lead to inconsistent application of certification requirements in the absence of direct review (*see* proposed § 170.580(a)(1)(v)). The commenters stated that if certification criteria pose issues that are novel, complex, or likely to lead to inconsistent application, these issues should be addressed during the testing and certification process, not by reviewing certified health IT after it has been certified.

Response. Commenters may have misunderstood the purpose of these proposed factors and the situations in which they would be relevant to determining whether ONC should initiate direct review. In the 2015 Edition final rule, we explained that to comply with applicable certification criteria, developers must not only demonstrate required capabilities in a controlled testing environment but must also make those capabilities available in ways that enable them to be implemented and used in production environments for their intended purposes (80 FR 62711). As ONC–ACBs increase their surveillance of the performance of certified health IT in production environments, we anticipate that ONC–ACBs may be presented with performance and functionality that might require the analysis of unfamiliar and difficult problems or deficiencies in certified health IT that require significant resources and expertise to properly investigate and assess under existing certification criteria. In some instances, the resources required to undertake this assessment may exceed the resources available to the ONC–ACB.

The factors proposed at § 170.580(a)(1)(iv)(D) and (a)(1)(v) were not intended to suggest, as some commenters seem to have misunderstood, that ONC could use direct review to engage in novel interpretations of certification criteria. Rather, these factors were intended to cover situations, such as those described above, that could exceed an ONC–ACB's resources or expertise. To avoid any confusion, we have removed these factors from the final rule's regulation text on the basis that they are duplicative of ONC's consideration of whether an ONC–ACB has sufficient ''resources or expertise'' to evaluate a suspected non-conformity.

Comments. A few commenters, including one ONC–ACB, suggested that ONC–ACBs are in the best position to know their own capabilities and as such ONC should not initiate direct review unless invited by an ONC–ACB. One commenter suggested that ONC should be ''on call'' to assist ONC–ACBs to respond to suspected non-conformities that exceed the ONC–ACBs capacity or expertise.

Response. We thank commenters for their comments. In response to commenter concerns, we have adapted the final rule to provide ONC with an opportunity to consult with ONC–ACBs, as well as the ONC–AA and any other persons or entities, as ONC deems appropriate. In order for ONC to exercise direct review under § 170.580(a)(2)(ii)(C), ONC must necessarily make a judgment about the resources and expertise of an ONC–ACB. ONC would only very rarely be in a position to make such a judgment without first consulting with the relevant ONC–ACB. However, because ONC is the Program owner and administrator, it would be inappropriate if an ONC–ACB were able to prevent ONC from initiating direct review if ONC has formed a reasonable belief that the ONC–ACB lacks the resources or expertise to investigate and address the suspected non-conformity at issue.

Comments. Commenters urged us to clarify the types of information that ONC would rely on in deciding whether to initiate direct review, including when ONC would deem information ''reliable and actionable'' so as to warrant further inquiry into certified health IT's conformity to Program requirements (*see* 81 FR 11062).

Response. In the 2015 Edition final rule, we provided guidance on the circumstances that would trigger an ONC–ACB's duty to initiate reactive surveillance (80 FR 62712). We said that in determining whether to initiate reactive surveillance, an ONC–ACB must consider and weigh the volume, substance, and credibility of complaints and other information received against the type and extent of the alleged non-conformity, in light of the ONC–ACB's expertise and experience with the particular capabilities, health IT, and certification requirements at issue. As an example, we supposed that where an ONC–ACB receives a number of anonymous complaints alleging general dissatisfaction with a particular certified health IT, the ONC–ACB would not be required to initiate surveillance (though it would not be precluded from doing so). In contrast, upon receiving several complaints alleging specific non-conformities, the ONC–ACB must initiate surveillance of the certified health IT unless a reasonable person in the ONC–ACB's position would doubt the credibility or accuracy of the complaints. By way of example, we explained that a reasonable basis for doubt might exist if the ONC–ACB had recently responded to the very same issue and determined through in-the-field surveillance of the certified health IT at several different locations that the reported problem was due to a ''bug'' arising from an unsupported use of the certified health IT that the developer had specifically cautioned users about in advance.

We anticipate applying these same principles in determining whether information about a potential non-conformity is sufficiently reliable and actionable to warrant ONC's direct review. We note, however, that in contrast to an ONC–ACB's affirmative duty to initiate surveillance, ONC is not required to initiate direct review. As such, ONC may require additional information before initiating review or may choose not to exercise review for any reason.

Comments. Commenters made a range of suggestions about criteria that ONC could adopt, or indicia ONC could use, to determine the veracity or credibility of information received by ONC when making a determination on whether or not to commence direct review. A number of commenters suggested that ONC should not initiate direct review of an alleged non-conformity unless the complainant has first notified the developer and given the developer an opportunity to rectify the deficiency.

Response. We thank commenters for their constructive suggestions. Because most issues that are the subject of direct review will concern risks to public health or safety, we anticipate that it will be very rare for information about such risks to be reported to ONC without first being brought to the developer's attention. However, we have determined that it would not be appropriate for ONC to be inhibited from initiating direct review on the basis that a health IT user had not first notified the health IT developer of the issue and provided the developer with an opportunity to rectify the deficiency. Consistent with a number of comments received from health IT developers, we note that a large number of health IT users do not have a direct business relationship with the developer of the health IT product they use. This is because many small healthcare practices receive their health IT via a sublicensing arrangement entered into with a large health care network. Similarly, other health IT stakeholders, such as health information exchanges, are positioned to identify deficiencies in certified health IT products they interact with but would not necessarily have a recognized process through which to raise issues or grievances with the developer concerned. Because ONC will weigh the volume, substance, and credibility of any information received, in light of all relevant circumstances, we do not believe it is necessary or appropriate to exclude from consideration any particular types or sources of information or to decide in advance what if any weight should be assigned to them.

Comments. One commenter also suggested that ONC would need to receive a threshold number of complaints by multiple distinct users in respect to the same certified health IT version number before the information in ONC's possession was actionable.

Response. ONC respectfully disagrees that there is a threshold number of complaints that would apply in all circumstances to ensure that direct review was triggered in only appropriate cases. Indeed, we can envision public health or safety risks for which a single complaint supported by detailed information and/or evidence would be sufficiently reliable and actionable to trigger ONC's exercise of discretion to initiate direct review.

Comments. A commenter suggested that a provider's timeliness in implementing all applicable and available releases and ''hot fixes'' for the certified health IT should be taken into consideration by ONC when assessing the veracity and credibility of information ONC has received.

Response. We thank this commenter for their comment. If a health IT developer issued customers with a new release, patch, or ''hot fix'' to address a deficiency in the developer's certified health IT, but their recommendation to implement the update within a specified period is ignored, ONC may determine that the deficiency at issue was caused by factors removed from the control or responsibility of the developer (*see* discussion above in section II.A.1.a.(1) of this preamble).

However, ONC may determine that it may nevertheless initiate review of the affected certified health IT in order to make a proper determination of the cause of any suspected non-conformity and to make an assessment of whether the remedial action implemented by the developer is appropriate in the circumstances.

b. ONC–ACB's Role

We proposed that ONC's review of certified health IT would be independent of, and may be in addition to, any review conducted by an ONC–ACB, even if ONC and the ONC–ACB were to review the same certified health IT, and even if the reviews occurred concurrently. To ensure consistency and clear accountability, we also proposed that ONC, if it deems necessary, could assert exclusive review of certified health IT as to any matters under review by ONC and any other matters that are so intrinsically linked that divergent determinations between ONC and an ONC–ACB would be inconsistent with the effective administration or oversight of the Program. Finally, we proposed that in such instances, ONC's determinations on these matters would take precedent and a health IT developer would be subject to the proposed ONC direct review provisions in the Proposed Rule, including having the opportunity to appeal an ONC determination, as applicable.

We clarified in the Proposed Rule that, in matters where ONC does not assert direct and/or exclusive review or ceases its direct and/or exclusive review, an ONC–ACB would be permitted to issue its own determination on the matter. We further clarified that any resulting determination to suspend or terminate a certification issued to a Complete EHR or Health IT Module by an ONC–ACB would not be subject to ONC review under the provisions proposed in the Proposed Rule. We also stated that in those instances, there would be no opportunity to appeal the ONC–ACB's determination(s) under the provisions proposed in the Proposed Rule. We emphasized that ONC–ACBs are accredited, authorized, and entrusted to issue and administer certifications under the Program consistent with adopted certification criteria and other specified Program requirements. Therefore, they have the necessary expertise and capacity to effectively administer these specific requirements.

We proposed in the Proposed Rule that ONC could initiate review of certified health IT on its own initiative based on information from an ONC–ACB, which could include a specific request from the ONC–ACB to conduct a review. In exercising its review of certified health IT, we proposed that ONC would be entitled to any information it deems relevant to its review that is available to the ONC–ACB responsible for administering the health IT's certification. We proposed that ONC could contract with an ONC–ACB to conduct facets of an ONC direct review within an ONC–ACB's scope of expertise, such as surveillance of certified capabilities.

We proposed that ONC could also share information with an ONC–ACB that may lead the ONC–ACB, at its discretion and consistent with its accreditation, to conduct in-the-field surveillance of the certified health IT at particular locations. We further proposed that ONC could, at any time, end all or any part of its review of certified health IT under the processes proposed and refer the applicable part of the review to the relevant ONC–ACB(s), if doing so would be in the best interests of efficiency or the effective administration and oversight of the Program. We stated that the ONC–ACB would be under no obligation to proceed further, but would have the discretion to review and evaluate the information provided and proceed in a manner it deems appropriate. As noted above, this may include processes and determinations (*e.g.,* suspension or termination) not governed by the proposed review and appeal processes.

We requested comment on our proposed approach and the role of an ONC–ACB.

Comments. Multiple commenters supported our proposals regarding the ONC–ACB's role and responsibilities for reviewing certifications of Complete EHRs and Health IT Modules. Commenters agreed that there are situations when ONC should have authority to independently review or assist an ONC–ACB in reviewing certified health IT. Other commenters questioned our rationale for allowing ONC direct review to be independent of, and in addition to, ONC–ACB review. These commenters contended that ONC–ACBs are qualified to review all non-conformities. A few commenters requested clarification regarding the scope of review responsibilities for ONC and ONC–ACBs, respectively.

Response. We have finalized our proposals regarding the ONC–ACB's role and responsibilities in relation to ONC direct review as proposed with the following clarifications and a revision as discussed in the response below. As stated above, reviews by ONC–ACBs and ONC would be complementary, but independent as well. As discussed in detail under section II.A.1.a, we believe that ONC should exercise direct review over matters outside of an ONC–ACB's resources and expertise as well as matters that pose a serious risk to public health or safety.

We clarify that ONC–ACB review after a certification is issued is limited to surveillance. This clarification is consistent with the requirements of ISO/IEC 17065 [9] and our discussion of ONC–ACB surveillance in the 2015 Edition final rule (*see* 80 FR 62605). Thus, we refer to this ''review'' by the ONC–ACB as surveillance in this final rule.

Comments. Commenters, including an ONC–ACB, expressed agreement with our proposal that as the scheme owner and regulator, ONC's determinations should take precedent. Other commenters were concerned that there could be conflicts between ONC and ONC–ACB determinations and questioned why ONC's determination should take precedent. Commenters also suggested that the proposed approach to review could cause mixed messaging by ONC and ONC–ACBs and duplication of efforts by health IT developers (*e.g.,* document production and interviews). Commenters encouraged ONC and ONC–ACBs to share relevant information and coordinate review in order to avoid duplication.

Response. We believe the final provisions will facilitate sound determinations by the appropriate body and help avoid duplicative review. Under the final provisions, ONC may assert exclusive review of certified health IT as to any matters under its review and any similar matters under surveillance by an ONC–ACB. In determining if matters are similar, ONC will, as proposed, consider whether the matters are so intrinsically linked that divergent determinations between ONC and an ONC–ACB would be inconsistent with the effective administration or oversight of the Program.

A determination by ONC on matters under its review will be controlling and supersede any determination by an ONC–ACB. We believe these steps will help avoid conflicts in determinations and permit ONC, as the administrator of the Program, to reach appropriate outcomes consistent with Program requirements on matters within its review.

Under the final provision in § 170.580(a)(3)(v), ONC may end all or any part of its review of certified health IT and refer the applicable part of the review to the relevant ONC–ACB(s) if

[9] The international standard to which ONC–ACBs are accredited. 45 CFR 170.599(b)(4).

ONC determines that doing so would serve the effective administration or oversight of the Program. The ONC–ACB would be under no obligation to proceed further, but would have the discretion to review and evaluate the information provided and proceed in a manner it deems appropriate.

We are finalizing this provision by revising it for clarity. We had proposed that ONC may end its review based on the best interests of efficiency or the administration and oversight of the Program (81 FR 11083). We have revised that proposal to be that ONC may determine to end its review if that would serve the effective administration or oversight of the Program. We believe the revision eliminates duplicative bases for ending review and remains consistent with the intent of the proposed provision. In addition, for further clarity, we have added that ONC may cease its review at any time. We indicated in the Proposed Rule that we could cease our review, but we did not make clear that it could be at any time during the direct review process (*see also* section II.A.1.a.(2) of this preamble). We further note that in the discussion of the direct review processes, we provide clarity regarding the steps ONC would take throughout direct review, including after receiving health IT developer responses to notices.

We appreciate commenters' suggestion that ONC increase coordination and sharing of information with ONC–ACBs. ONC and ONC–ACBs regularly communicate and we anticipate this communication would continue when ONC initiates direct review of certified health IT. As noted by commenters, such communication will benefit the Program and minimize the possibility of mixed messaging or duplicative review. In furtherance of collaboration between ONC and ONC–ACBs, we have finalized the proposed requirement that ONC–ACBs must provide ONC with any available information that ONC deems relevant to its review of certified health IT. We have also included ONC–ATLs in this information sharing provision as we have finalized the ONC–ATL processes in this final rule. We note that we could share information with an ONC–ACB that may lead the ONC–ACB, at its discretion and consistent with its accreditation, to conduct in-the-field surveillance of the health IT at a particular location.

Comment. A commenter expressed concern that the Proposed Rule did not propose appeal rights for ONC–ACB determinations. The commenter explained that, if there are two different enforcement bodies (ONC and ONC–ACBs) that may make determinations, there should be equal rights for a health IT developer to appeal those determinations.

Response. Health IT developers that have their certifications terminated by an ONC–ACB can appeal that determination to the ONC–ACB, similar to how an ONC termination can be appealed to the National Coordinator under the processes finalized in this final rule. The ONC–ACB will process the appeal in accordance with the requirements of ISO/IEC 17065 and the ONC–ACB's procedures. Appeal procedures may vary among ONC–ACBs, so health IT developers should familiarize themselves with the appeal procedures provided by their ONC–ACB(s). If the health IT developer is not satisfied with the result of the appeal, the health IT developer can submit the matter to the Approved Accreditor for certification under the Program, American National Standards Institute (ANSI), for consideration.

In consideration of the ONC–ACB appeals process outlined above and our belief that ONC–ACBs have the necessary expertise and capacity to effectively administer certifications under the Program consistent with the certification criteria and other specified Program requirements, we have not established a process for health IT developers to appeal ONC–ACB determinations to ONC.

c. Review Processes

We stated in the Proposed Rule that ONC could become aware of information from the general public, interested stakeholders, ONC–ACBs, or by any other means that indicates that certified health IT may not conform to the requirements of its certification or is, for example, leading to medical errors or other outcomes that do not align with the National Coordinator's responsibilities under section 3001 of the PHSA. We proposed that, if ONC deems the information to be reliable and actionable, it would conduct further inquiry into the certified health IT. We further stated that ONC could also initiate an independent inquiry into the certified health IT that could be conducted by ONC or a third party(ies) on behalf of ONC (*e.g.,* contractors or inspection bodies under the certification scheme). If information reveals that there is a potential non-conformity (through substantiation or omission of information to the contrary) or confirms a non-conformity in the certified health IT, we stated that ONC would proceed to notify the health IT developer of its findings, as applicable, and work with the health IT developer to address the matter.

We proposed that correspondence and communication with ONC and/or the National Coordinator for all processes proposed under this section (section II.A.1.c) of the preamble shall be conducted by email, unless otherwise necessary or specified. We proposed to modify § 170.505 accordingly.

Comments. Commenters supported the ONC direct review processes as proposed. A commenter emphasized that the review processes would promote greater accountability of health IT developers for the performance, reliability, and safety of certified health IT. A few commenters, however, expressed concern about frivolous complaints. These commenters and other commenters requested clarification regarding the type of information that would warrant ONC direct review and requested that ONC explain what constitutes ''reliable and actionable'' information. A commenter requested that ONC establish clear requirements for what information must be presented as part of a complaint or allegation of non-conformity and who would be eligible to make such a complaint.

Response. We have finalized the process and criteria for identifying non-conformities that would warrant ONC direct review as proposed with clarifications in response to comments. We clarify that in order to determine the reliability of the information, ONC will consider and weigh the volume, substance, and credibility of complaints and other information received against the type and extent of the alleged non-conformity. We note that this reliability standard aligns with the ONC–ACB standard for initiating surveillance in the 2015 Edition final rule (80 FR 62713). We also clarify that if information ONC receives does not provide adequate detail, specificity, or clarity regarding the suspected non-conformity, ONC will, as necessary, contact the party(ies) who submitted the complaint to gather additional information and make a decision as to whether the complaint is actionable. To avoid confusion, we have removed ''reliable and actionable'' from the relevant provisions of § 170.580. We believe the above clarification is responsive to commenters and clarifies the type of information that would give ONC a ''reasonable belief'' that the certified health IT may not or does not conform to the requirements of the Program.

In section II.A.1.a.(3) of this final rule, we describe factors ONC should consider when deciding whether to exercise direct review. These factors afford ONC discretion to evaluate information on a case-by-case basis. Considering the wide range of information ONC may receive regarding non-conformities in certified health IT, and that ONC has specialized expertise to evaluate the reliability and accuracy of such information, it is essential that ONC have discretion in making direct review decisions.

Comments. Many commenters suggested that correspondence throughout the review processes should be issued by mail.

Response. We have finalized the requirements for correspondence with additional regulation revisions and processes. Section 170.505 states that correspondence and communication with ONC or the National Coordinator shall be conducted by email, unless otherwise necessary or specified. We note that email correspondence and communication of protected health information by HIPAA covered entities and business associates must employ safeguards in compliance with the HIPAA Rules.

Section 170.505 provides the flexibility to use means other than email as ''necessary or specified.'' As stated in the Proposed Rule, we intend to send notice of suspension and termination via certified mail. We also intend to send notices of potential non-conformity, notices of non-conformity, and notices of proposed termination via certified mail. We have, therefore, revised § 170.505 to clearly state the potential use of certified mail in addition to regular and express mail. Section 170.505 specifies that the official date of receipt of any form of mail will be the date of the delivery confirmation. We have revised the language of this provision to clarify that it applies to all parties and that delivery confirmation is to the address on record. The address on record is the most recently provided address to ONC or an ONC–ACB, as applicable. We believe this will clarify the process in situations where an entity, such as a health IT developer, moves its place of business or goes out of business without notifying ONC or the relevant ONC–ACB.

(1) Notice of Potential Non-Conformity or Non-Conformity

We proposed that if information suggests to ONC that certified health IT is not performing consistent with Program requirements and a non-conformity exists with the certified health IT, ONC would send a notice of potential non-conformity or non-conformity to the health IT developer. We explained in the Proposed Rule that the notice would specify ONC's reasons for the notification, explain ONC's findings, and request that the health IT developer respond to the potential/alleged non-conformity (and potentially a corrective action request) or be subject to further action (*e.g.,* corrective action, suspension, and/or the termination of the certification in question, as appropriate).

We proposed that ONC should have the ability to access and share within HHS, with other federal agencies, and with appropriate entities, a health IT developer's relevant records related to the development, testing, certification, implementation, maintenance, and use of its product, as well as any complaint records related to the product. We stated that this proposal would ensure a complete and comprehensive review of the certified health IT product. We noted that much of this information already must be disclosed as required by the Program and described in the 2015 Edition final rule. We proposed, however, that ONC be granted access to, and be able to share within HHS, with other federal agencies, and with appropriate entities (*e.g.,* a contractor or ONC–ACB) any additional records not already disclosed that may be relevant and helpful in ONC's fact-finding and review. If we determined that the health IT developer was not cooperative with the fact-finding process, we proposed that we would have the ability to suspend or terminate the certification of any encompassed Complete EHR or Health IT Module of the certified health IT as outlined later in sections II.A.1.c.(3) and (4) of this final rule.

We stated in the Proposed Rule that we understood that health IT developers may have concerns regarding disclosure of proprietary, trade secret, competitively sensitive, or other confidential information. To address these concerns, we further stated that ONC would implement appropriate safeguards to ensure, to the extent permissible with federal law, that any proprietary business information or trade secrets that ONC might encounter by accessing the health IT developer's records would be kept confidential by ONC.[10] For instance, ONC would ensure that, if it obtains proprietary or trade secret information, that information would not be included in the CHPL. We noted, however, that the safeguards we would adopt would be prophylactic and would not create a substantive basis for a health IT developer to refuse to comply with the proposed requirements. Thus, a health IT developer would not be able to avoid providing ONC access to relevant records by asserting that such access would require it to disclose trade secrets or other proprietary or confidential information.

We proposed that unless otherwise specified in the notice, the health IT developer would be required to respond within 30 days of receipt of the notice and, if necessary, submit a proposed CAP as outlined below in section II.A.1.c.(2) of this final rule. We proposed that ONC may require a health IT developer to respond and/or submit a proposed CAP in more or less time than 30 days based on factors such as, but not limited to: (1) The type of health IT and health IT certification in question; (2) the type of non-conformity to be corrected; (3) the time required to correct the potential non-conformity or non-conformity; and (4) issues of public health and safety and other exigencies related to the National Coordinator carrying out his or her duties in accordance with sections 3001(b) and (c) of the PHSA. We proposed that ONC would have discretion in deciding the appropriate timeframe for a response and proposed CAP from the health IT developer.

We proposed that if the health IT developer contends that the certified health IT in question conforms to Program requirements, the health IT developer must include in its response all appropriate documentation and explain in writing why the health IT is conforming.

We requested comment on our proposed processes described above, including whether the timeframe for responding to a notice of potential non-conformity or non-conformity is reasonable and whether there are additional factors that we should consider.

Comments. Many commenters supported the proposed processes for notices of potential non-conformity and non-conformity. Multiple commenters, however, requested discussion between ONC and the health IT developer, which could also include the ONC–ACB, regarding a complaint or surveillance issue prior to the issuance of a notice of potential non-conformity or non-conformity. Commenters stated that such discussion would help ensure the appropriateness of, and necessity for, the issuance of a notice of potential non-conformity or non-conformity. A commenter also recommended that ONC engage with end-users of certified health IT and establish a process in which end-

[10] The Freedom of Information Act, 18 U.S.C. 1905, and the Uniform Trade Secrets Act generally govern the disclosure and descriptions of these types of information.

users can offer feedback on certified health IT to help alert ONC to potential and actual non-conformities.

Many commenters requested that ONC clarify the circumstances that would cause ONC to send a notice of potential non-conformity or non-conformity to a health IT developer. These commenters also expressed concerns that, as proposed, ONC could issue a notice of non-conformity without first issuing a notice of potential non-conformity. Commenters opined that a notice of non-conformity should not be the first instance of notification to a health IT developer in the ONC direct review process. A commenter recommended that ONC provide a model notification to industry and stakeholders of the content of a notice of potential non-conformity and non-conformity.

Response. We thank commenters for their thoughtful comments on this aspect of the proposed direct review processes. We have finalized the proposed processes for notices of potential non-conformity and non-conformity with the following clarifications and revisions discussed below and finalized in § 170.580(b)(1) through (3).

We agree with commenters regarding the benefits of open discussion between ONC, health IT developers, and as applicable, ONC–ACBs, during the direct review process. While we encourage discussions between ONC and health IT developers prior to the issuance of a notice of potential non-conformity or non-conformity, we cannot guarantee that such discussions will always precede a notice because ONC may need to take immediate steps to expedite direct review and corrective action or have other reasons for not first discussing the matter. We emphasize that our first and foremost goal is to work with health IT developers to address any non-conformities in certified health IT in a timely manner and across all customers, and we encourage discussion as early as possible in the process to help achieve this goal.

We also appreciate the suggestion that ONC engage with end-users and we encourage end-users to contact us with their concerns. Specifically, end-users can submit a complaint through the ONC-established complaint process at: *https://www.healthit.gov/healthitcomplaints.*

While we do not believe we could develop a model notice that would be of value to health IT developers because each instance of potential non-conformity or non-conformity will likely be unique, we do offer the following clarifications. ONC may issue a notice of non-conformity without first issuing a notice of potential non-conformity if supported by the circumstances and information available to ONC. ONC must be able to issue a notice of non-conformity in situations where information establishes and ONC determines that there is an actual non-conformity in order to put the health IT developer on notice and begin the corrective action process without delay. In comparison, ONC may issue a notice of potential non-conformity when it has a reasonable belief, based on information at its disposal, that there may be a non-conformity with the certified health IT. We further note that a notice of potential non-conformity and notice of non-conformity are separate and distinct notices, and ONC can issue them concurrently, as necessary. In such situations, each notice will include the appropriate timeframe for the health IT developer to submit a response. As stated above, we will send notices of potential non-conformity and non-conformity by certified mail and the official date of receipt will be the date of the delivery confirmation to the address on record consistent with § 170.505.

Developer Response

We have restructured and revised the requirements for health IT developer responses to notices of potential non-conformity and non-conformity (*see* § 170.580(b)(1)(ii) and (b)(2)(ii)). These revisions are intended to clarify ONC's expectations regarding health IT developer responses and to emphasize that the proposed and finalized ''Records Access'' provision (§ 170.580(b)(3)) is a separate requirement.

Health IT developers must respond to a 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 to the certified health IT under review, and (3) providing ONC with a written explanation, within 30 days, unless adjusted by ONC, addressing the potential non-conformity, including all appropriate documentation.

Health IT developers must respond to a notice of non-conformity in the same fashion as described for a notice of potential non-conformity above *and,* in addition, must submit a proposed CAP (*see* § 170.580(b)(2)(ii)(A)(*4*)). We note that we did not propose in the Proposed Rule that the health IT developer could respond to a notice of non-conformity through a written explanation addressing the non-conformity in addition to submitting a proposed CAP. We have, however, finalized this new provision in the final rule to allow health IT developers to explain, agree with, or refute the notice of non-conformity, which parallels a health IT developer's opportunity to respond to a notice of potential non-conformity. This opportunity to respond is in addition to submitting a proposed CAP and will not delay or prolong the CAP process. In addition, we note that ONC may still propose termination under § 170.580(e), as necessary, despite a written explanation from the health IT developer that refutes the notice of non-conformity. We further note that a health IT developer may choose to contest the notice of potential non-conformity or not cooperate with ONC or a third party acting on behalf of ONC. However, we again emphasize that in such situations ONC may take action under the proposed termination provisions (*see* § 170.580(e)).

Comments. We received numerous comments on the proposed 30-day default response period for notice of potential non-conformity or non-conformity. This includes the requirement, which is also stated in section II.A.1.c.(2) of this final rule below, that a health IT developer must submit a proposed CAP to ONC within 30 days of the date that ONC notifies the health IT developer of an actual non-conformity, unless ONC specifies a different timeframe. A few commenters supported our proposal and response timeframe. Many commenters suggested that the 30-day default response period should be the minimum time period to respond to a notice. Other commenters stated that a 30-day default response period is too short, particularly when corrective action is required, because non-conformities may be complex and difficult to resolve. One commenter suggested that the 30-day default response period is too long. The commenter stated that, based on past experience working with numerous certified systems to address non-conformities, 30 days is a long time for the problem to be addressed, much less to develop a plan to address the problem. Many commenters requested clarification about instances when the response period would be ''more or less'' time than 30 days, as proposed. Many commenters also suggested that the response period be measured in business days.

Response. We have finalized this requirement as proposed for responding to both a notice of potential non-conformity and a notice of non-conformity with clarifications in response to comments. We maintain that 30 days is an appropriate default response period that will afford health IT developers ample time to respond to a notice and ensure that health IT developers address non-conformities in a timely fashion. We provide clear guidance regarding the factors ONC will use to determine whether the health IT developer should submit a response and/or CAP in more or less time than 30 days (§ 170.580(b)(1)(ii)(B) and (b)(2)(ii)(B)). ONC must retain discretion to increase or decrease the 30-day period when necessary due to the wide range and complexity of non-conformities. We emphasize that ONC will work with health IT developers to develop acceptable CAPs with reasonable timeframes for completion. We also clarify that health IT developers may request an extension for submittal of a CAP. In order to make this extension request, a health IT developer must submit a written statement to ONC that explains and justifies the request.

For clarity, we previously adopted the definition of ''day or days'' in § 170.102 to mean calendar day or calendar days (Temporary Certification Program final rule; 75 FR 36162 and 36203).

We clarify, as noted above, that a health IT developer's response to a notice of potential non-conformity or non-conformity includes providing ONC, and/or a third party acting on behalf of ONC, with access to the certified health IT under review (§ 170.580(b)(1)(ii) and (b)(2)(ii)). We note that this is a clarification of the requirement in the Proposed Rule and does not introduce a new requirement for health IT developers (81 FR 11058). We proposed in the ''Authority and Scope'' section of the Proposed Rule that this rulemaking was intended to address ONC's direct review of certified health IT and provide ONC with access to the certified health IT and relevant records (''records access'' proposal) to assist in determining whether a non-conformity exists and addressing a found non-conformity.

ONC Determination

We have added and finalized provisions that specify how ONC would respond to a health IT developer's response to a notice of potential non-conformity and notice of non-conformity. These provisions provide further transparency and clarification of the review processes, particularly with regard to ONC actions. However, we emphasize that, as specified under the ''ONC–ACB's Role'' section of this final rule above, ONC may end its review at any time.

We have finalized a provision that addresses ONC's options after receiving the health IT developer's written explanation in response to a notice of potential non-conformity. ONC will do one of the following (§ 170.580(b)(1)(iii)): (1) Issue a written determination ending its review (which, may also include a rescission of a suspension (*see* the ''suspension'' section of this final rule for further discussion)); (2) request additional information and continue its review in accordance with a new timeframe it establishes (*see* § 170.580(b)(1)(ii)(A)(*3*) and (b)(1)(ii)(B)); (3) substantiate a non-conformity and issue a notice of non-conformity; or (4) issue a notice of proposed termination.

We have also finalized a similar provision that addresses ONC's options after receiving the health IT developer's written response to a notice of non-conformity. ONC will either issue a written determination ending its review or continue with its review under the provisions of this section. The continuation of ONC's review would likely be to proceed through the CAP process as outlined in this final rule, but may instead be to issue a proposed termination or take other appropriate action under the provisions of this final rule.

Comments. Many commenters expressed concern that the proposed records access requirement is too broad, extends beyond what is required for ONC–ACB surveillance, and could require health IT developers to produce large amounts of information. Commenters suggested that the proposed language should be more narrowly focused on records that directly bear on the specific certified capabilities affected by the non-conformity(ies) and materials relevant to the issue under review. Commenters were also concerned about protecting the confidentiality of health IT developer records. Commenters questioned the necessity of sharing records with other federal agencies and appropriate entities.

A commenter noted that documents or records obtained by ONC during the course of direct review could contain protected health information (PHI), trade secrets, or other sensitive information without a sufficient basis or adequate assurances that this information would be protected from further disclosure.

Response. We have finalized this requirement as proposed with the following clarifications. This approach to records access and sharing of records is necessary for ONC to conduct a comprehensive review of certified health IT, and will supplement ONC's access to the certified health IT under review. This approach supports the review of uncertified capabilities that interact with certified capabilities and will assist ONC in determining whether certified health IT conforms to applicable Program requirements. Further, the relevant records and federal departments, agencies, and offices will be determined on a case-by-case basis with consideration of the matter under review. We clarify that ''complaint records'' under the records access requirements include, but are not limited to, issue logs and help desk tickets.

As stated and outlined in the Proposed Rule (81 FR 11063), we are committed to implementing appropriate safeguards to ensure that any proprietary business information or trade secrets that ONC might encounter would be kept confidential by ONC to the extent permissible by federal law. To that end, we strongly recommend that health IT developers clearly mark, as described in HHS Freedom of Information Act regulations at 45 CFR 5.65(c), any information they regard as trade secret or confidential commercial or financial information prior to disclosing the information to ONC.

Regarding the disclosure of PHI to ONC, we refer to our previous guidance provided on this issue in consultation with the HHS Office for Civil Rights. Specifically, in the 2015 Edition Final Rule, we explained that a health care provider is permitted, without patient authorization, to disclose PHI to an ONC–ACB for purposes of the ONC–ACB's authorized surveillance activities (80 FR 62716). Health care providers are permitted to make disclosures to a health oversight agency (as defined in 45 CFR 164.501) for oversight activities (as described in 45 CFR 164.512(d)) authorized by law, including activities to determine compliance with program standards, and ONC may delegate its authority to ONC–ACBs to perform surveillance of certified health IT under the Program.[11] This disclosure of PHI to an ONC–ACB does not require a business associate agreement with the ONC–ACB since the ONC–ACB is not performing a function on behalf of the covered entity. In the same way, a provider, health IT developer, or other person or entity is permitted to disclose PHI directly to ONC, without patient authorization and without a business associate agreement, for purposes of ONC's direct review of certified health IT or the performance of any other

[11] *See:* 45 CFR 164.512(d)(1)(iii); 80 FR 62716*;* and ONC Regulation FAQ #45 [12–13–045–1] available at *http://www.healthit.gov/policy-researchers-implementers/45-question-12-13-045.*

oversight responsibilities of ONC to determine compliance under the Program.

We further clarify that, as we contemplated in the Proposed Rule, it may be necessary for ONC to engage additional resources and specialized expertise to timely and effectively respond to potential non-conformities or non-conformities (81 FR 11058), and that this may include engaging outside experts, consultants, or other persons or entities (consultants) for the purpose of assisting ONC in its direct review of certified health IT. In the same way that ONC authorizes ONC–ACBs to conduct surveillance of certified health IT under the Program, ONC may authorize such consultants to perform fact-finding, analyses, and/or other functions that support ONC's direct review of the certified health IT; and pursuant to ONC's health oversight authority (as defined in 45 CFR 164.512(d)(1)(iii)), persons and entities are permitted to disclose PHI to such consultants for the purpose of carrying out these authorized activities, without patient authorization and without a business associate agreement.

We note that subsequent disclosures of identifiable patient health information by ONC, or persons or entities acting on ONC's behalf, are limited to those expressly allowed by law—such as under the Privacy Act of 1974 and/or the Freedom of Information Act (FOIA), as applicable.

(2) Corrective Action

We proposed in the Proposed Rule that if ONC finds that certified health IT does not conform to Program requirements, ONC would take appropriate action with the health IT developer to remedy the non-conformity as outlined below.

We proposed that ONC would require a health IT developer to submit a proposed CAP to ONC. The CAP would provide a means to correct the identified non-conformities across all the health IT developer's customer base.

We proposed, as described above in section II.A.1.c.(1) of this preamble and in the Proposed Rule, that a health IT developer must submit a proposed CAP to ONC within 30 days of the date that ONC notifies the health IT developer of the non-conformity, unless ONC specifies a different timeframe. We explained in the Proposed Rule that this approach aligns with and does not change the corrective action process specified in § 170.556(d) and used by ONC–ACBs. The primary difference between this approach and the approach specified § 170.556(d) is that in § 170.556(d) the health IT developer must submit a CAP to an ONC–ACB within 30 days of being notified of the potential non-conformity. We proposed in the Proposed Rule that this 30-day period be the default for receiving a response/CAP, but that ONC may alter the response period based on non-conformities that may pose a risk to public health or safety, or other exigencies related to the National Coordinator carrying out his or her duties in accordance with sections 3001(b) and (c) of the PHSA (81 FR 11063).

We proposed in the Proposed Rule that ONC would provide direction to the health IT developer as to the required elements of the CAP and would work with the health IT developer to develop an acceptable CAP. We proposed that a CAP must include, at a minimum, for each non-conformity:

- A description of the identified non-conformity;
- An assessment of the nature, severity, and extent of the non-conformity, including how widespread they may be across all of the health IT developer's customers of the certified health IT;
- How the health IT developer will address the identified non-conformity, both at the locations where the non-conformity was identified and for all other potentially affected customers;
- A detailed description of how the health IT developer will assess the scope and impact of the non-conformity(ies), including identifying all potentially affected customers, how the health IT developer will promptly ensure that all potentially affected customers are notified of the non-conformity and plan for resolution, how and when the health IT developer will resolve issues for individual affected customers, and how the health IT developer will ensure that all issues are in fact resolved; and
- The timeframe under which corrective action will be completed.

We proposed that when ONC receives a proposed CAP (or a revised proposed CAP) it shall either approve the proposed CAP or, if the plan does not adequately address all required elements, instruct the health IT developer to submit a revised proposed CAP. In addition to the required elements above, we proposed that a health IT developer would be required to submit an attestation to ONC. We explained that the attestation would follow the form and format specified by the CAP and would be a binding official statement by the health IT developer that it has fulfilled all of its obligations under the CAP, including curing the identified non-conformities and related deficiencies and taking all reasonable steps to prevent their recurrence.

We stated in the Proposed Rule that based on this attestation and all other relevant information, ONC would determine whether the non-conformity(ies) had been cured and, if so, would lift the CAP. However, we proposed that if it were later discovered that the health IT developer had not acted in the manner attested, ONC could reinstitute the CAP or proceed to suspend or terminate the certification of any encompassed Complete EHR or Health IT Module of the certified health IT.

We proposed that ONC would report the CAP and related data to the publicly accessible CHPL. The purpose of this reporting requirement, as it is for ONC–ACBs under current regulations, would be to ensure that health IT users, implementers, and purchasers are alerted to potential conformity issues in a timely and effective manner. This approach is consistent with the public health and safety, program integrity, and transparency objectives described previously in the Proposed Rule (81 FR 11064) and in the 2015 Edition final rule (80 FR 62725–26).

We requested comment on our proposed CAP processes as described above.

Comments. Many commenters stated that ONC should use the same construct for CAPs as was established in § 170.566(d) for non-conformities found by ONC–ACBs. A few commenters noted that the proposed corrective action requirements and the ''ONC–ACB CAP'' requirements are consistent concerning the authority of ONC and ONC–ACBs to provide direction on required elements of the CAP, but are inconsistent with regard to the proposed ability of ONC to ''*prescribe*'' such corrective action as may be appropriate to fully address the identified non-conformity(ies). Some commenters suggested that ONC clarify this language so that ONC is able to ''prescribe'' the elements required of the CAP, but not health IT developer actions.

Response. We thank commenters for their thoughtful comments on this aspect of the proposed corrective action process. In consideration of these comments, we have finalized the corrective action requirement and CAP elements at § 170.580(c)(2), subject to the following changes and clarification discussed below. As discussed above, our approach to corrective action aligns with the corrective action process specified in § 170.556(d) for ONC–ACB actions. Section 170.556(d) does not, however, ''prescribe'' corrective action. Therefore, to further align with

§ 170.556(d) and in response to comments, we have removed ''prescribe'' from the regulation text. We emphasize that this change is only a clarification of the proposed language and does not represent a narrower policy than proposed.

Our goal with CAPs under ONC direct review and ONC–ACB surveillance is to remedy the non-conformity(ies) as quickly and effectively as possible. Therefore, we will include such required elements as part of a CAP as we determine is necessary to comprehensively and expeditiously resolve the identified non-conformity(ies). We will, however, work with health IT developers to determine the most appropriate elements for CAPs and strive to assist in the creation of CAPs that are no more or less prescriptive than necessary to remedy the non-conformity(ies) quickly and effectively.

Comments. Multiple commenters suggested that CAPs as a result of ONC direct review should be based only on non-conformities with existing certification criteria of the Program.

Response. In this final rule, a non-conformity is a failure of certified health IT or its developer to conform to the requirements of the Program. We emphasize, as discussed in detail in section II.A.1.a.(1) of this preamble, that Program requirements are not limited to compliance with certification criteria. A CAP will be based on a finding and notice of non-conformity, which necessarily involves a failure to meet Program requirements (§ 170.580(c)). Similarly, the elements of the CAP will address the actions a health IT developer must take to correct the identified non-conformity(ies) (*i.e.,* bring its certified health IT back into conformity with the Program requirements that are the basis of the non-conformity(ies)).

Comments. A commenter requested that we clarify the criteria necessary for resolving non-conformities under a CAP. Commenters requested that we specify the criteria that would lead to the rejection of a proposed CAP and recommended that we not reject a proposed CAP without giving the health IT developer an opportunity to discuss the issue(s) with ONC. One commenter suggested that ONC institute a process for health IT developers to respond to a rejection of a CAP.

Response. We cannot define the specific criteria necessary for resolving non-conformities under a CAP because such criteria will be determined on a case-by-case basis. However, as noted above and in the Proposed Rule, ONC will provide direction to health IT developers as to the required elements of a CAP and will work with health IT developers to develop acceptable CAPs. We note that we have restructured and reordered the required elements for a CAP in the final rule for clarity and to avoid inclusion of redundant factors (*see* § 170.580(c)(2)). We have also adopted two new elements for CAPs that serves to clarify how a health IT developer would demonstrate the resolution of all non-conformities and issues (a proposed CAP element) and prevent the non-conformity from re-occurring. We discuss these CAP elements below.

Comments. A commenter suggested that we allow a health IT developer to request an extension for submitting and completing corrective action in certain cases.

Response. ONC will permit health IT developers to submit requests for extension of the 30-day period to submit a CAP and the period ONC allocates for completion of the CAP. In order to make these requests, a health IT developer 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. We have added a provision at § 170.580(c)(5) to reflect this policy. We clarify, however, that ONC may propose to terminate the certification of the health IT under review if, after 90 days of notifying the health IT developer of a non-conformity, ONC is unable to approve a CAP because the health IT developer has not submitted a CAP, proposed or revised, that adequately addresses all required elements of the CAP as determined by ONC (§ 170.580(c)(4)). This clarification of the 90-day time limit for approving a CAP aligns with the CAP requirement for ONC–ACBs (§ 170.556(d)(5)(ii)).

Comments. A few commenters requested that we revise the proposed required CAP elements so that health IT developers are not required to ensure that all issues are resolved. Commenters stated that health IT developers cannot guarantee the absolute resolution regarding a provider's implementation within the required timeframe because some providers may not immediately implement the software update or modify their workflows in all ways necessary to ensure resolution.

Response. We have finalized this requirement to ensure that all issues are resolved. The requirement is consistent with the corrective action requirements in § 170.556(d)(3)(iv) and is a necessary requirement for corrective action. In response to the comment recited below regarding the need for more than just reliance on a health IT developer's attestation for verification of a CAP's completion, we have included a new required CAP element that clarifies how health IT developers are expected to meet the requirement to ensure that the non-conformity and all issues are resolved. A health IT developer must include in a CAP a detailed description of the supporting documentation that will be provided to demonstrate that the identified non-conformities and all issues are resolved. When ONC approves the CAP, we may require the supporting documentation to include testing results, independent expert analysis and verification, and/or other appropriate documentation to provide assurance that all issues have been resolved. Further, we understand that provider cooperation and actions must be taken into consideration. Therefore, we clarify that we expect a health IT developer will take and document the reasonable steps it took to ensure that all non-conformities and issues are resolved.

We proposed elements that, at a minimum, must be included in a CAP. We received comments regarding the consequences of certification termination and our 'certification ban' and 'heightened scrutiny' proposals (*see* the ''Consequences of Certification Termination'' section below) requesting that we ensure sufficient protection for providers affected by non-conformities as well as supporting some form of heightened scrutiny of health IT that had a non-conformity and was subsequently terminated. In consideration of these comments and our stated goals in the Proposed Rule to promote public confidence in certified health IT and ensure the integrity of the Program, we have added a prospective element for CAPs. All CAPs must provide an explanation of, and agreement to execute, the steps that will be prevent the non-conformity from re-occurring. We believe this specific element of a CAP will help prevent reoccurrences of circumstances that led to the non-conformity(ies). This will support the integrity of the Program by addressing not only current problems, but also instituting ''safeguards'' against further problems. Equally important, this CAP element will promote public confidence in certified health IT, including health IT that had a non-conformity. For example, a health IT developer can offer its customers reassurance that not only was the non-conformity corrected, but that steps have also been taken to prevent it from re-occurring.

Comments. A commenter suggested that ONC review a Complete EHR or Health IT Module following the completion of a CAP, rather than accepting the attestation as proof of conformity.

Response. We have finalized the attestation requirement as proposed. We appreciate the commenter's concern, but believe attestation is an appropriate means for confirming that the health IT developer has fulfilled all of its obligations under the CAP, including curing the identified non-conformities and related deficiencies for all affected customers and taking all reasonable steps to prevent their recurrence. In addition, we emphasize three points. As specified above, a health IT developer must submit, and have approved by ONC, a CAP that includes a detailed description of the supporting documentation that the health IT developer will provide to demonstrate that the identified non-conformities and all issues are resolved. Second, an attestation serves as a binding official statement by the health IT developer. Third, if we later discover that the health IT developer had not acted in the manner attested, we may reinstitute the CAP or proceed to suspend or terminate the certification of the Complete EHR or Health IT Module (*see* § 170.580(c)(7), (d)(1), and (e)(1)(vi)).

Comments. Commenters generally supported reporting CAPs to the CHPL. Multiple commenters stated, however, that the CHPL alone is not an effective means for notifying customers because purchasers will not be in the habit of looking at the CHPL regularly. Commenters suggested that health IT developers should utilize more direct forms of notification. Commenters suggested that health IT developers send ''push'' alerts and notifications. One commenter disagreed with reporting CAPs to the CHPL and expressed concern regarding the disclosure of trademark and proprietary software capabilities and/or functionalities, as well as the potential damage to health IT developers' reputations.

Response. We thank commenters for their support of this proposal and for expressing their concerns. We have finalized this requirement as proposed. The reporting of CAP information to the CHPL is already required as specified in the 2015 Edition final rule (80 FR 62714) and at § 170.556(e)(3) and we will continue this approach with CAPs that are a result of ONC direct review. This reporting will alert health IT users, implementers, and purchasers to potential conformity issues in a timely and effective manner. Further, as mentioned above, health IT developers must notify all potentially affected customers of the non-conformity and plan for resolution as part of a CAP.

We understand that health IT developers may have concerns regarding disclosure of trademark and proprietary software capabilities and/or functionalities and potential damage to their reputations. To address these concerns, as discussed in the ''Notice of Potential Non-Conformity or Non-Conformity'' section of this final rule above, we will implement safeguards to keep trademark or proprietary information confidential to the extent permissible by federal law.

(3) Suspension

We proposed in the Proposed Rule that ONC may suspend a certification for similar reasons as allowed for ONC–ACBs, which were discussed in the 2015 Edition final rule (80 FR 62759). Specifically, we proposed that ONC would be permitted to initiate certification suspension procedures for a Complete EHR or Health IT Module for any one of the following reasons:

- Based on information it has obtained, ONC believes that the certified health IT poses a potential risk to public health or safety or other exigent circumstances exist. More specifically, ONC would suspend a certification issued to any encompassed Complete EHR or Health IT Module of the certified health IT if the certified health IT was, but not limited to: Contributing to a patient's health information being unsecured and unprotected in violation of applicable law; increasing medical errors; decreasing the detection, prevention, and management of chronic diseases; worsening the identification and response to public health threats and emergencies; leading to inappropriate care; worsening health care outcomes; or undermining a more effective marketplace, greater competition, greater systems analysis, and increased consumer choice. Such results would conflict with section 3001(b) of the PHSA, which instructs the National Coordinator to perform the duties in keeping or recognizing a certification program that, among other requirements, ensures patient health information is secure and protected in accordance with applicable law, reduces medical errors, increases efficiency, and leads to improved care and health care outcomes. As discussed in the ''Termination'' section below, we proposed that ONC could terminate a certification on the same basis *if* it concludes that a certified health IT's non-conformity(ies) cannot be cured;
- The health IT developer fails to timely respond to any communication from ONC, including, but not limited to: Fact-finding, a notice of potential non-conformity, or a notice of non-conformity;
- The information 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;
- The health IT developer fails to timely submit a proposed CAP that adequately addresses the elements required by ONC; or
- The health IT developer does not fulfill its obligations under the CAP.

We also proposed that ONC may suspend the certification of a Complete EHR or Health IT Module *at any time* when ONC believes that the certified health IT poses a potential risk to public health or safety, other exigent circumstances exist concerning the product, or due to certain actions or inactions by the product's health IT developer as detailed above. We noted that the processes for ONC–ACBs, as detailed in the 2015 Edition final rule (80 FR 62759), would not be altered by our proposals in the Proposed Rule.

Comments. We received many comments regarding our proposed suspension criteria. Multiple commenters supported the suspension criteria as proposed and emphasized the need to protect public health and safety. Other commenters expressed concerns regarding ONC's proposed criteria for suspending the certification of a Complete EHR or Health IT Module. These commenters urged ONC to more clearly define the standards and criteria for suspension and to reserve suspension for particular cases of significant risk to patient health and safety. Commenters also stated that ONC should not suspend certification(s) when a health IT developer is working with ONC and acting in good faith to remedy the non-conformity through a CAP.

Response. We thank commenters for their thoughtful comments on this aspect of our proposed suspension process. We agree with commenters that suspension should be limited to situations involving a serious risk to public health or safety, as these are the situations that would require immediate action. Therefore, in consideration of these comments, we have finalized a more limited basis for suspension than proposed. Specifically, ONC may *only* suspend a certification when ONC has a reasonable belief that the certified health IT may present a serious risk to public health or safety. As explained in section II.A.1.a.(3) of this preamble, in assessing whether there is a serious risk to public health or safety, ONC would consider the nature, extent, and severity of the risk and the conditions giving rise to it, in light of the information available to ONC at the time. Separately, ONC could conclude that certified health IT poses a serious risk to public health or safety were it aware of information calling into question the validity of the health IT's certification.

We clarify that ONC would still be able to suspend the certification of the health IT after the health IT developer begins corrective action if it identifies a serious risk to public health or safety.

Comments. A commenter suggested that we not have the discretion to suspend a certification of a Complete EHR or Health IT Module at any time. The commenter stated that the reasons provided for suspending certification were too broad and that suspension, in the absence of a final legal or regulatory ruling, confers a presumption of guilt and responsibility on the health IT developer.

Response. We have finalized the ability to suspend at any time if such action is necessary to protect public health or safety. We note our response to the previous comment which emphasizes the now limited scope of suspension focusing on risks to public health and safety. We further note, in response to the commenter, that suspension is part of the finalized regulation.

Comments. A few commenters requested clarification regarding the distinction between criteria for suspension and termination and how to decide which is appropriate in certain situations. Another commenter recommended that ONC should, as a matter of process, issue a notice of suspension before issuing a notice of termination.

Response. As stated in our responses above, at this time, we are choosing to limit our discretion to only suspend a certification when we believe that certified health IT presents a serious risk to public health or safety. This change not only clarifies why ONC would suspend a certification, but also draws a clear distinction between the reasons to suspend and the reasons to terminate a certification as described later in this final rule. This change also means that if ONC finds grounds for suspension, ONC will always first take the step to suspend the certification before initiating termination proceedings. We emphasize, however, that we may proceed with termination without first suspending a certification for other matters as outlined under the ‘‘Scope of Review’’ section and the termination provisions in this final rule.

Suspension Process

We proposed that ONC would issue a notice of suspension when appropriate. We stated that ONC's process for obtaining information to support a suspension could involve, but would not be limited to: Fact-finding; requesting information from an ONC–ACB; contacting users of the health IT; and/or reviewing complaints. We proposed that a suspension would become effective upon the health IT developer's receipt of the notice of suspension.

We proposed that the notice of suspension would include, but not be limited to: ONC's explanation for the suspension; the information ONC relied upon to reach its determination; the consequences of suspension for the health IT developer and the Complete EHR or Health IT Module under the Program; and instructions for appealing the suspension. We also stated that the notice of suspension would be sent via certified mail and the official date of receipt would be the date of the delivery confirmation consistent with § 170.505.

Comments. Multiple commenters supported the suspension process as proposed. One commenter suggested that ONC implement intermediate solutions short of suspension, such as: Fines or other financial penalties; a requirement that health IT developers bear the costs of repair or transition to another system; or, a clear statement of health IT developers' tort liability for the consequences of non-conformities.

Response. We have decided not to implement intermediate ‘‘solutions’’ as suggested by the commenter because the purpose of suspension as proposed is to enable ONC to act swiftly to address non-conforming certified health IT that present a serious risk to public health or safety and intermediate ‘‘solutions’’ or ‘‘penalties’’ would delay such action. Additionally, at present, ONC does not have authority to level fines or other financial penalties in these situations and the liability of a health IT developer to customers, other parties, or other matters is outside the scope of this final rule.

Clarifications Regarding Notice of Suspension

A notice of suspension will be effective on the date listed in the notice of suspension. We clarify that ONC will issue a notice of potential non-conformity or non-conformity at the same time it issues the notice of suspension. These notices will provide the health IT developer opportunities to respond to the basis for suspension. We further clarify the contents of a notice of suspension. We stated in the Proposed Rule that a notice of suspension would include the information ONC relied upon to reach its determination. We clarify, including in regulation, that the information we were referencing is information ONC provides with, and in support of, its determination.

Notification and Publication of Suspension

We proposed that a health IT developer would be required to notify its affected and potentially affected customers of the certification suspension in a timely manner. We also proposed that ONC would publicize the suspension on the CHPL to alert interested parties, such as purchasers of certified health IT or programs that require the use of certified health IT. We requested comments on these processes, including how timely a health IT developer should notify affected and potentially affected customers of a suspension and what other means we should consider using for publicizing certification suspensions.

Comments. We received many comments on the proposed requirements for notifying affected and potentially affected customers of a suspension. Commenters suggested that a health IT developer should not be required to notify its affected and potentially affected customers of a certification suspension until ONC reaches a final determination and concludes the appeal process. Some commenters requested we clarify the meaning of ‘‘timely manner’’ in the context of customer notification. One commenter suggested ONC require health IT developers to notify customers within 10 business days after receipt of the suspension notice. Some commenters supported publicizing suspensions on the CHPL and suggested other mechanisms for notifying customers, such as real-time electronic notifications.

A few commenters suggested changes regarding the party that should make a notification of suspension and the party(ies) that should be notified. A commenter suggested that ONC should notify customers of a suspension, as opposed to the health IT developer notifying customers as proposed. The commenter also suggested that ONC notify customers of a health IT developer whose Complete EHR or Health IT Module is being *considered* for suspension. Another commenter suggested that if notifications of suspension are required, they should be sent to all customers of the product, not just those affected and potentially affected by the non-conformity.

Response. We have finalized the notification requirements as proposed with the following clarification. We require that a health IT developer must notify ''all potentially affected customers'' as opposed to ''all affected and potentially affected'' customers as we proposed. We removed ''affected'' in this final rule because all ''affected'' customers would also be considered ''potentially affected'' customers; thus the language was redundant. All potentially affected customers should be notified of suspensions in a timely manner after the effective date of the suspension, regardless of whether a health IT developer is appealing the determination. We believe that ''potentially affected customers'' is the appropriate population for health IT developers to notify and is broad enough to protect customers that are or may be affected by the suspension.

We believe a health IT developer is the appropriate party to alert its customers of a suspension as it would know best the potentially affected customers. It would be inappropriate to alert customers of a health IT developer whose Complete EHR or Health IT Module is being considered for suspension because such action might unfairly disadvantage a health IT developer whose Complete EHR or Health IT Module may not warrant suspension after further investigation and consideration.

As suspension would be based on a serious risk to public health or safety, we believe it is imperative that customers be aware of the suspension. The notification will permit customers to take immediate action to protect public health and safety; and if the suspension is appealed, provide customers with additional time to consider their options and next steps. We believe ''timely'' is an appropriate term because the timeliness of the notification to all potentially affected customers may vary based on the circumstances of the case. While we believe that ONC must have discretion to address each situation accordingly, we agree with the commenter that notification within 10 days or less of the effective date of the suspension may be reasonable in many circumstances.

Last, we maintain that notification via the CHPL is an appropriate and effective step for widespread dissemination of a suspension determination to all stakeholders as the CHPL serves as the authoritative, comprehensive listing of health IT that has been tested and certified under the Program. We will further consider whether other forms of publication and dissemination, such as use of the ONC listserv, would be an appropriate and effective communication tool under the circumstances.

Consequences of Suspension

We proposed that ONC would issue a cease and desist notice to health IT developers to immediately stop the marketing and sale of the Complete EHR or Health IT Module as ''certified'' under the Program when it suspends the Complete EHR's or Health IT Module's certification. We proposed that in cases of a certification suspension, inherited certified status for the Complete EHR or Health IT Module would not be permitted. We requested comment on whether a health IT developer should only be permitted to certify new Complete EHRs or Health IT Modules while the certification in question is suspended, if such new certification of other Complete EHRs or Health IT Modules would correct the non-conformity for all affected customers. We also requested comment as to whether correcting the non-conformity for a certain percentage of all affected customers or certain milestones demonstrating progress in correcting the non-conformity (*e.g.,* a percentage of customers within a period of time) should be sufficient to lift the prohibition.

Comments. Multiple commenters supported our proposed prohibition on the marketing and sale of a Complete EHR or Health IT Module during a suspension. One commenter noted that such a restriction is supportive of safe information systems. Other commenters stated that the prohibition on marketing and sale of the suspended Complete EHR or Health IT Module as ''certified'' is inappropriate and represents significant ''overreach,'' while some commenters stated that it would not be an ''overreach'' if there were a valid patient safety concern.

Response. We thank commenters for their thoughtful comments and have finalized the 'consequences of suspension' in relation to the Program with the following revision and clarifications. As noted above and in the Proposed Rule, we proposed that ONC would issue a cease and desist notice to health IT developers to immediately stop the marketing and sale of a Complete EHR or Health IT Module as ''certified'' under the Program when it suspends the Complete EHR's or Health IT Module's certification (81 FR 11064). We did not specifically include ''licensing'' as part of this prohibition. However, we believe licensing is a form of product sale as in both cases a health IT developer likely receives some type of compensation. We also note that we specifically discuss licensing of certified health IT in the ''Corrective Action'' section of the Proposed Rule (*see* 81 FR 11063). Our intention with this cease and desist notice was to protect the health and safety of users by completely prohibiting health IT developers from representing suspended health IT as ''certified.'' Therefore, we have specifically listed ''licensing'' as part of this prohibition to provide additional clarity. Affirmatively adding ''licensing'' to this section is consistent with ONC's intent to cover all the ways in which health IT software is made available to customers in the health IT marketplace, as well as our stated goal throughout the ''Suspension'' section in the Proposed Rule (81 FR 11064) and this final rule to protect public health and safety.

As discussed earlier in this section, we have finalized a more limited basis for suspension than proposed, which is that we may only suspend a certification when we believe that the certified health IT presents a serious risk to public health or safety. Thus, by definition, in cases of suspension, ONC will only prohibit the marketing, licensing, and sale of a Complete EHR or Health IT Module when it presents serious risk to public health or safety. We believe this approach is consistent with comments and supports public health and safety.

Comments. A few commenters expressed disagreement with our proposal to prohibit inherited status certification for a suspended Complete EHR or Health IT Module, while more commenters expressed disagreement with the possibility of a prohibition on the certification of a health IT developer's new Complete EHRs and Health IT Modules while the certification in question is suspended. Commenters stated that such restrictions are too far-reaching and suspension should only apply to the health IT under review. Some commenters suggested that a prohibition on new testing and certifications should only apply if a product is affected by the non-conforming product or there is reason to believe there is a wider, more pervasive deficiency with the health IT developer. A commenter suggested that our basis for determining progress for lifting the prohibition should be measured against what the health IT developer does to implement corrected products with providers.

Response. We have added a provision at § 170.580(d)(5) that bans the certification (which includes all types of certification, such as inherited certified status and gap certification) of any of a health IT developer's health IT if the health IT developer has the certification on one of its products suspended. The suspension would only be lifted if, as determined by ONC, all affected customers have been provided appropriate remediation. As discussed in the Proposed Rule, a ban may incentivize the health IT developer to cure the non-conformity in an efficient manner. As the basis for suspension is now limited to a reasonable belief that the certified health IT presents a serious risk to public health or safety, we believe the ban is now even more essential to motivating a health IT developer to quickly address and correct what we believe to be a serious risk to public health or safety. We refer readers to section II.1.d.(1) of this final rule for further details on meeting the requirement for providing all affected customers with appropriate remediation.

Clarification Regarding ''Rescission'' of a Suspension

We proposed in the Proposed Rule that ONC would only ''rescind'' a certification suspension if the health IT developer completes all elements of an approved CAP and/or ONC confirms that all non-conformities have been corrected. We have renamed this provision as ''cancellation.'' A suspension can be canceled, 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. We believe this revised provision for canceling a suspension is appropriate because suspension is limited to situations in which ONC has a reasonable belief that the certified health IT may present a serious risk to public health or safety; therefore, the basis for cancellation is the opposite of the basis for suspension. The basis for establishing that there is no longer reason to believe that the certified health IT presents a serious risk to public health or safety may be based on information ONC obtains or information provided by a health IT developer. It could be for the same reasons as proposed (*i.e.,* the health IT developer completes all elements of an approved CAP and/or ONC confirms that all non-conformities have been corrected) or possibly for other reasons.

(4) Termination

We proposed that ONC may terminate certifications issued to Complete EHRs or Health IT Modules under the Program if: (1) The health developer fails to timely respond to any communication from ONC, including, but not limited to: (a) Fact-finding; and (b) a notice of potential non-conformity or non-conformity; (2) the information provided by the health IT developer in response to fact-finding, a notice of potential non-conformity, or a notice of non-conformity is insufficient or incomplete; (3) the health IT developer fails to timely submit a proposed CAP that adequately addresses the elements required by ONC as described in section II.A.1.c.(2) of this preamble; (4) the health IT developer does not fulfill its obligations under the CAP developed in accordance with proposed § 170.580(c); or (5) ONC concludes that the certified health IT's non-conformity(ies) cannot be cured. We requested comment on the proposed reasons for termination and on any additional circumstances for which commenters believe termination of a certification would be warranted.

Proposed Termination and Termination

Comments. A few commenters suggested less severe alternatives to termination, such as a probation period or implementation of intermediate solutions short of termination.

Response. We thank commenters for their thoughtful comments. We explain in section II.A.1.c.(1) and (2) of this final rule (and also explained in the Proposed Rule (81 FR 11062–64)) that, prior to termination, ONC affords the health IT developer multiple opportunities to address and correct a non-conformity(ies) through responses to notices of potential non-conformity and/or non-conformity and a CAP. We believe that, if the health IT developer fails to address and correct the non-conformity(ies) at these stages in the direct review process, termination is an appropriate next step. A probation period would not adequately address the non-conforming health IT and/or non-responsive health IT developer in such situations. We emphasize once again that our goal is to work with health IT developers to correct non-conformities and that termination is a last resort.

In response to the comments and due to the severity of termination of a certification, we have added a new, intermediate step in the direct review process called ''proposed termination.'' The proposed termination step will provide health IT developers with an additional opportunity to resolve issues regarding a non-conformity prior to termination. We emphasize that the bases for ''proposed termination'' in this final rule are nearly identical to the bases for ''termination'' in the Proposed Rule (81 FR 11084). The only differences are that in this final rule we have clarified that a health IT developer's failure to cooperate with ONC and/or a third party acting on behalf of ONC and a failure to timely submit in writing a proposed CAP are also bases for termination. We clearly stated in the Proposed Rule that these actions are required of health IT developers (*see* 81 FR 11062–63); therefore, non-compliance with these requirements will serve as a basis for proposed termination.

As stated previously in this preamble under the discussion of § 170.505, we will send any notice of proposed termination by certified mail and the official date of receipt will be the date of the delivery confirmation to the address on record. A health IT developer may respond to a notice of proposed termination, but must do so within 10 days of receiving the proposed termination notice and must include appropriate documentation explaining in writing why its certification should not be terminated. ONC will have up to 30 days to review the information submitted by the health IT developer and reach a decision. ONC may extend this timeframe if the complexity of the case requires additional time for ONC review.

We have also finalized a provision that requires ONC to respond to the health IT developer's response to a notice of proposed termination within 30 days, unless ONC extends this timeframe due to the complexity of the case. The ONC response will either be to proceed with direct review, cease direct review, or proceed to termination (§ 170.580(e)(4)). This requirement aligns with our stated goals in the Proposed Rule of promoting transparency and enhanced communication by providing health IT developers with information about ONC's progress during the direct review process.

We refer readers to § 170.580(e) in this final rule for the specific provisions of proposed termination.

Comments. Multiple commenters supported the criteria for termination as proposed. Some commenters requested clearer and more substantive standards for termination of a certification.

Response. We thank commenters for their support. As discussed in the preceding response, we have finalized the steps health IT developers must take to avoid termination as proposed in the Proposed Rule (81 FR 11065). We believe these criteria are substantive and clear as they describe specific situations of health IT developer inaction and incurable non-conformities in the health IT that would warrant termination by ONC. We also believe these criteria will incentivize health IT developers to cooperate in the direct review process and address non-conformities. Further, in regard to cooperation, we have specifically included, consistent with our proposals in the Proposed Rule, the failure of a health IT developer to cooperate with ONC direct review as a basis for certification termination. Additionally, we believe the addition of the proposed termination step further clarifies our process for terminating a certification. We emphasize that 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; or (ii) the health IT developer does not respond in writing to a proposed termination notice within the timeframe specified above. We note that the termination provisions have been finalized at § 170.580(f) because of the addition of the ''proposed termination'' step, which has been added to the final regulation at § 170.580(e).

Comments. A commenter requested that we define ''timely'' in the context of termination.

Response. ''Timely'' is the appropriate term because it accounts for the timeframe for a health IT developer to respond to ONC, submit a CAP, and contact customers. The timeliness of these actions will vary based on the circumstances of the case. Therefore, ONC must have discretion to address each situation on a case by case basis.

Termination Process, Notification, and Publication

We proposed that a termination would be issued consistent with the processes outlined below, but noted that the proposed termination processes do not change the certification termination processes for ONC–ACBs in § 170.556(6).[12] We stated that a notice of termination would include, but may not be limited to: ONC's explanation for the termination; the information ONC relied upon to reach its determination; the consequences of termination for the health IT developer and the Complete EHR or Health IT Module under the Program; and instructions for appealing the termination. We proposed that ONC would send a written notice of termination to the agent of record for the health IT developer of the Complete EHR or Health IT Module. We stated that the written termination notice would be sent via certified mail and the official date of receipt would be the date of the delivery confirmation.

As we proposed for suspension of a certification, the health IT developer must notify the affected and potentially affected customers of the identified non-conformity(ies) and termination of certification in a timely manner. Additionally, we proposed that ONC would publicize the termination on the CHPL to alert interested parties, such as purchasers of certified health IT or entities administering programs that require the use of health IT certified under the Program. We requested comments on these processes, including how timely a health IT developer should notify affected and potentially affected customers of a termination of a Complete EHR's or Health IT Module's certification and what other means we should consider for publicizing certification terminations.

Comments. Multiple commenters suggested changes for the proposed process for notifying customers of a termination. Some commenters recommended that health IT developers should not notify customers until ONC reaches a final determination and concludes all appeals. One commenter suggested that health IT developers should send notification to all customers, not just those affected and potentially affected by the non-conformity. Some commenters noted that reporting terminations to the CHPL is not effective and suggested that health IT developers use real-time electronic notifications in addition to reporting to the CHPL.

Response. We thank commenters for their thoughtful comments on this aspect of the proposed termination process. We have, however, finalized the notification requirements as proposed with the following clarification. As we clarified for the ''Suspension'' portion of the direct review processes, we require that a health IT developer must notify ''all potentially affected customers'' as opposed to ''all affected and potentially affected'' customers as we proposed. We removed ''affected'' in this final rule because all ''affected'' customers would also be considered ''potentially affected'' customers. All ''potentially affected customers'' should be notified of terminations in a timely manner, regardless of whether a health IT developer is appealing the determination. We believe that this is the appropriate population for health IT developers to notify and is broad enough to protect customers that are or may be affected by the termination. The notification will permit customers to take immediate action, as they deem necessary, coinciding with the termination; and if the termination is appealed, provide customers with additional time to consider their options and next steps.

We believe that notification via the CHPL is an appropriate and effective step for widespread dissemination of a termination determination to all stakeholders as the CHPL serves as the authoritative, comprehensive listing of health IT that has been tested and certified under the Program. We will further consider whether other forms of publication and dissemination, such as use of the ONC listserv, would be an appropriate and effective communication tool under the circumstances.

We clarify the contents of a notice of termination and, similarly, a notice of proposed termination. We stated in the Proposed Rule that a notice of termination would include the information ONC relied upon to reach its determination. We clarify, including in regulation, that the information we were referencing is information ONC provides with, and in support of, its determination. In addition, as to only the notice of termination, we clarify that the 'consequences of termination' in relation to the Program are the consequences specified in § 170.580(f)(3) (notifying potentially affected customers) and in § 170.581 (discussed in more detail in the ''Consequences of Certification Termination'' section of this final rule).

Termination Effective Date and Appeal

We proposed that the termination of a certification would be effective either upon: (1) The expiration of the 10-day period for filing an appeal as specified in section II.A.1.c.(5) of this preamble, if the health IT developer does not file an appeal; or, if a health IT developer files an appeal, (2) upon a final determination to terminate the certification as described below in the ''Appeal'' section of this preamble.

Comments. Many commenters stated that the proposed 10 days to file an appeal following a termination is insufficient, especially if no new information can be included as part of a hearing on appeal.

Response. We refer readers to the ''Appeal'' section of this preamble below for our response to this concern.

Rescission of a Notice of Termination

We have finalized a provision that permits ONC to rescind a determination to terminate a certification before it becomes effective if ONC determines that termination is no longer appropriate. To illustrate, ONC may rescind the determination to terminate on its own initiative or based on information provided by the developer

[12] We note that ONC–ACB ''termination'' actions are technically referred to as ''withdrawals'' of certifications. We explain this distinction in detail in section II.A.d.(1) of this final rule.

that convinces ONC that the termination decision was made in error or is otherwise no longer appropriate. We have included this provision as part of the termination process in order to address situations where a certification was terminated, but it would be inefficient to proceed through the appeals process or inappropriate to effectuate the termination. This requirement aligns with our stated goals in the Proposed Rule of working with health IT developers, ensuring the integrity of the Program, and promoting transparency.

(5) Appeal

We proposed that if ONC suspends or terminates a certification for a Complete EHR or Health IT Module, the health IT developer of the Complete EHR or Health IT Module may appeal the determination to the National Coordinator in accordance with the proposed processes outlined below. We proposed that a health IT developer may appeal an ONC determination to suspend or terminate a certification issued to a Complete EHR or a Health IT Module if the health IT developer asserts: (1) ONC incorrectly applied Program methodology, standards, or requirements for suspension or termination; or (2) ONC's determination was not sufficiently supported by the information used by ONC to reach the determination to suspend or terminate a certification.

We proposed that a request for appeal of a suspension or termination must be submitted in writing by an authorized representative of the health IT developer whose certified Complete EHR or certified Health IT Module was subject to the determination being appealed. We also proposed that the request for appeal must be filed in accordance with the instructions specified in the notice of termination or notice of suspension. We stated that these instructions for filing a request may include, but would not be limited to, requiring the health IT developer to: (1) Provide a copy of the written determination by ONC to suspend or terminate the certification and any supporting documentation; and (2) explain the reasons for the appeal.

We proposed that the appeal request must be submitted to ONC within 10 days of the health IT developer's receipt of the notice of suspension or notice of termination. We proposed that an appeal request would stay the termination of a certification issued to a Complete EHR or Health IT Module until a final determination is reached on the appeal. However, we noted that a request for appeal would not stay a suspension of a Complete EHR or Health IT Module. We proposed that, while an appeal would stay a termination, a Complete EHR or Health IT Module would be prohibited from being marketed or sold as ''certified'' during the stay. This was similar to the proposed effects of a suspension.

We proposed that the National Coordinator would assign the appeal to a hearing officer who would adjudicate the appeal on his or her behalf. We stated that the hearing officer may not preside over an appeal in which he or she participated in the initial suspension or termination determination by ONC or has a conflict of interest in the pending matter.

We stated in the Proposed Rule that there would be two parties involved in an appeal: (1) The health IT developer that requests the appeal; and (2) ONC. We proposed that the hearing officer would have the discretion to make a determination based on two options: (1) The written record as submitted to the hearing officer by the health IT developer with the appeal filed in accordance with proposed requirements, which would include ONC's written statement and supporting documentation, if provided; or (2) the information described in option 1 and a hearing conducted in-person, via telephone, or otherwise. We specified that the hearing officer would have the discretion to conduct a hearing if he or she: (1) Requires clarification by either party regarding the written record; (2) requires either party to answer questions regarding the written record; or (3) otherwise determines a hearing is necessary. We specified that the hearing officer would neither receive testimony nor accept any new information that was not presented with the appeal request or was specifically and clearly relied upon to reach the determination to suspend or terminate the certification by ONC. We specified that the default process for the hearing officer would be a determination based on option 1 described above.

We proposed that once the health IT developer requests an appeal, ONC would have an opportunity to provide the hearing officer with a written statement and supporting documentation on its behalf (*e.g.,* a brief). We stated that the failure of ONC to submit a written statement would not result in any adverse findings against ONC and may not in any way be taken into account by the hearing officer in reaching a determination.

We proposed that the hearing officer would issue a written determination to the health IT developer within 30 days of receipt of the appeal, unless the health IT developer and ONC agree to a finite extension approved by the hearing officer. We proposed that the National Coordinator's determination, as issued by the hearing officer, would be the agency's final determination and not subject to further review.

We requested comments on the proposed appeal processes. Specifically, we requested comment on whether the allotted time for the hearing officer to issue a written determination should be lessened or lengthened, such as 15, 45, or 60 days. We also requested comment on whether an extension should be permitted and whether it should only be permitted under the extension circumstances proposed or for other reasons and circumstances.

Clarification Regarding the Appeal of Concurrent Suspension and Termination

We clarify that there may be situations where a certification is both suspended and terminated. For instance, ONC may suspend a certified Complete EHR or Health IT Module because it presents a serious risk to public health or safety. With the certification suspended pending corrective action, ONC may later propose to terminate and subsequently terminate the certification on the basis that the health IT developer did not cooperate with the direct review. In such a situation, the health IT developer must submit two separate statements of intent to appeal and requests for appeal in writing to ONC in accordance with § 170.580(g)(2) in order to appeal the suspension *and* the termination. We note that, in most cases, a health IT developer's opportunity to appeal a suspension in accordance with § 170.580(g)(3) would lapse prior to ONC's decision to terminate the certification.

In these cases (a suspension and termination of the same certification), the hearing officer would issue separate final determinations for the suspension and termination. For instance, the hearing officer may find that ONC terminated the certification prematurely and therefore reverse the termination on that basis, which would reinstate the certification. At the same time, however, the hearing officer may uphold ONC's decision to suspend the certified health IT because, for instance, it posed a serious risk to public health or safety or because the health IT developer failed to timely appeal the suspension.

Comments. A commenter stated that the health IT developer should be able to appeal an initial assessment of non-conformity, a CAP, and/or the terms of a CAP.

Response. We have finalized an approach that only permits appeals of ONC determinations to suspend or terminate a certification of a Complete EHR or Health IT Module. ONC has the authority to determine whether health IT remains in conformity with voluntary Program requirements. A notice of non-conformity and CAP are remedial steps designed to bring certified health IT back into conformity with Program requirements. Upon an ONC determination to suspend or terminate a certification, we believe a health IT developer should be afforded the opportunity to appeal the determination because of the consequences health IT developers and certified health IT face due to these actions (*i.e.,* the prohibition on the marketing, licensing, and sale of suspended health IT as ''certified'' and the consequences of termination specified in § 170.581) and the likely negative impact this will have on the ability of a health IT developer to sell or license its health IT to providers and consumers, as many HHS programs require participants to have and/or use certified health IT.

Comments. Multiple commenters questioned the proposed bases for appeal and suggested that we clarify the requirements. Some commenters requested more specificity in the first basis for appeal. Commenters requested that in order to meet this basis for appeal ONC must first identify and state specifically how it applied Program methodology, standards, and requirements for suspension or termination findings. Commenters also requested that ONC clarify the meaning of ''sufficient support'' in the second basis for appeal.

Response. We appreciate the comments on this proposal. We have removed the redundancy in the first basis for appeal by simply stating ''Program requirements.'' We believe that the proposed bases for appealing ONC decisions are now clear and appropriate. The two bases for appeal require that an ONC decision is based on Program requirements for health IT developers and certified health IT and is supported by sufficient information. We describe in the ''Suspension'' and ''Termination'' sections of this final rule that ONC will provide an explanation of the suspension or termination determination in a notice of suspension or notice of termination, as applicable. ONC will also provide information to support its determination and the consequences for the health IT developer and the Complete EHR or Health IT Module under the Program. This information will enable the health IT developer to assess whether ONC has correctly applied Program requirements and whether ONC's determination was sufficiently supported by information provided with the determination. We maintain that ''sufficiently supported'' is an appropriate term to use in the second basis for appeal because information provided with the determination will vary on a case-by-case. We clarify, as we have similarly done in the ''Suspension'' and ''Termination'' sections of this final rule, that this standard conveys that ONC's determination must be supported by information provided with the determination. Accordingly, we have finalized the bases for appeal in § 170.580(g)(1) with the revisions discussed above.

Comments. We received many comments regarding the appeal timeframes. Commenters stated that the proposed 10 days to file an appeal following a termination is insufficient, particularly if, as proposed, no new information can be included as part of an appeal hearing. The commenters asserted that collecting appropriate records for the appeal would be time consuming. Many commenters also proposed a two-step process for filing an appeal: (1) Filing a statement of intent to appeal; and (2) filing a request for appeal with supporting documentation. Commenters generally supported the 30-day timeframe for the hearing officer to make a final determination, while some commenters recommended that this timeframe be flexible based on the complexity of each case.

Response. We understand commenters' concerns regarding the 10-day period to file an appeal and, therefore, have accepted the commenters' recommendations for a two-step process for filing a statement of intent to appeal and then filing the appeal and supporting documentation. Specifically, in § 170.580(g)(3), we include requirements that a statement of intent to appeal must be filed within 10 days of receipt of the notice of suspension or notice of termination; and an appeal, including all supporting documentation, must be filed within 30 days of the filing of the intent to appeal.

In accordance with this two-step process, a termination will become effective upon: (1) The expiration of the 10-day period for filing a statement of intent to appeal if the health IT developer does not file a statement of intent to appeal; (2) the expiration of the 30-day period for filing an appeal if the health IT developer files a statement of intent to appeal, but does not file a timely appeal; or (3) a final determination to terminate the certification if a health IT developer files an appeal (§ 170.580(f)(2)(ii)).

We thank commenters for their support of the 30-day timeframe for the hearing officer to make a final determination. To provide flexibility for complex cases and unforeseen circumstances, we have finalized the proposal to permit the hearing officer to extend the timeframe for issuing a decision if the health IT developer and ONC agree to a finite extension and it is approved by the hearing officer. We believe this will provide the parties and the hearing officer with necessary flexibility as recommended by commenters.

We have revised the proposed 'determination by the hearing officer' provision to clarify that the hearing officer will not issue a written determination to the health IT developer if ONC cancels the suspension or rescinds the termination determination (§ 170.580(g)(7)). We have described ONC's ability to cancel a suspension and rescind termination determination, as well as ONC's rationale for allowing such actions, in sections II.A.1.c.(3) and (4) of this preamble, respectively.

Comments. Multiple commenters disagreed with our proposal that a request for appeal would not stay a suspension of a Complete EHR or Health IT Module. Specifically, commenters stated that the inability of a health IT developer to market and sell a product as ''certified'' while the product is suspended is overly punitive and could have untoward impacts on end-users.

Response. We have finalized this requirement as proposed. A request for appeal will not stay a suspension. As discussed in the ''Suspension'' section of this preamble, ONC may now only suspend the certification of health IT if it has a reasonable belief that the certified health IT may present a serious risk to public health or safety. In such situations, ONC must take immediate action to protect customers and incentivize the health IT developer to correct the non-conformity as soon as possible. A stay of a suspension would be inappropriate because it would delay this immediate action.

Comments. Many commenters expressed concerns regarding the appointment and qualifications of the hearing officer. Commenters asserted that the hearing officer should not be assigned by the National Coordinator or be selected from within ONC, as this could cause a conflict of interest and raise questions about the impartiality of the hearing officer. Commenters suggested that we clarify the required qualifications for the hearing officer. Commenters also opined that the hearing officer should not make the sole determination on whether to hold a hearing and should not be able to make a determination without a hearing.

Response. We have finalized the 'appointment of a hearing officer' provisions as proposed with an added requirement and clarifications in response to comments. We understand commenters' concerns regarding the impartiality of the hearing officer and agree that the hearing officer must be an impartial arbiter of appeals. The hearing officer will be chosen by the National Coordinator as the National Coordinator is best situated to identify a hearing officer, whether from within or outside ONC, that can represent him or her and have the requisite skills, qualifications, and knowledge to adjudicate these appeals. As proposed, in order to reduce the potential for conflicts of interest, the hearing officer will not be able to preside over an appeal in which he or she participated in the initial suspension or termination determination by ONC or has a conflict of interest in the pending matter. Additionally, in consideration of commenters' concerns and our commitment to an impartial appeals process, we have added a requirement at § 170.580(g)(5)(ii) that requires a hearing officer to be trained in a nationally recognized ethics code that articulates nationally recognized standards of conduct for hearing officers/officials. For example, an acceptable nationally recognized ethics code is, but is not limited to, the *National Association of Hearing Officials' Model Code of Ethics.*

The decision as to whether to hold a hearing will be left to the discretion of the hearing officer, as he or she will be most familiar with the facts of the case and will be best equipped to make such a determination.

Comments. Commenters disagreed with the proposed requirement that the hearing officer will neither receive testimony nor accept any new information that was not presented with the appeal request or was included with the determination. Another commenter suggested we revise the regulation text to clarify that the hearing officer will not receive certain testimony and information.

Response. We have finalized the requirement as proposed. This requirement will facilitate the appropriate development of the record prior to appeal, encourage health IT developers to submit a thorough and comprehensive appeal request, and facilitate expeditious resolutions of appeals. However, in consideration of comments, we have finalized a two-step process for filing a statement of intent to appeal and then filing the appeal and supporting documentation, which will afford health IT developers additional time to compile information and records to support their appeals. This process is discussed in more detail above in response to other comments.

In consideration of the commenter's request for revised regulation text, we have revised the relevant appeal provision (§ 170.580(g)(6)(iii)) to clarify that the hearing officer will not receive witness testimony and new information beyond that which is permitted with filing an appeal and given at a hearing. We have also made clear that the written record includes the ONC determination to suspend or terminate a certification and information to support the issued determination (§ 170.580(g)(6)(i)).

Comments. Commenters recommended that ONC implement a more formal, multi-round appeals process.

Response. Because we provide multiple opportunities for health IT developers to address the bases for ONC actions to suspend and/or terminate the certification of a Complete EHR or Health IT Module, we do not believe a more elaborate appeals process is generally necessary. However, for terminations, we have added another opportunity to resolve the matter through a ''proposed termination'' step that we have finalized in this final rule. The review, determination, and appeal processes in this final rule provide sufficient and equitable opportunities for health IT developers to address non-conformities found in their certified health IT, while ensuring the timely resolution of matters that may pose a serious risk to public health or safety.

Comments. Commenters disagreed with the proposal that ONC's failure to submit a written statement will not result in any adverse findings against ONC and may not in any way be taken into account by the hearing officer in reaching a determination. The commenters stated that ONC should be obligated to provide a written statement, including any and all information, analysis, and documentation it used to come to its determination. Additionally, the commenters asserted that this statement should be made available to the health IT developer.

Response. We have finalized the requirement substantially as proposed with the following revisions and clarifications. To clarify, if ONC suspends or terminates a certification, ONC will send a notice of suspension or termination, respectively, to the health IT developer (*see* § 170.580(d)(2) and (f)(2)). As detailed in paragraphs (d)(2)(i) and (f)(2)(i), the notice will include an explanation and information to support ONC's determination. Therefore, we have revised this provision to clearly state that ONC will have an opportunity to provide the hearing officer with an additional written statement and supporting documentation on its behalf that clarifies, as necessary, its determination to suspend or terminate the certification. We have further revised the provision to clarify that not only would the written statement and supporting documentation be included as part of the written record, but it must also be provided to the health IT developer within 15 days of the health IT developer's filing of an intent to appeal.

Comments. A commenter stated that ONC's assertion that an appeal determination is final and not subject to further review misstates the reviewability of administrative decisions by federal courts.

Response. This provision does not address the reviewability of administrative decisions by federal courts. The purpose of this regulatory provision is to convey that there are no further administrative reviews of the determination.

Comments. A commenter expressed concern that health IT developers were not afforded appeal rights for ONC–ACB determinations. The commenter explained that, if there are two different enforcement bodies (ONC and ONC–ACBs) that may make determinations, there should be equal rights for a health IT developer to appeal those determinations.

Response. We refer readers to section II.A.1.b of this final rule for an explanation of our decision not to extend appeal rights for ONC–ACB determinations.

Comments. A commenter suggested that providers should be included in the appeals process because providers will often make the initial complaint concerning a non-conformity.

Response. We encourage providers and other interested stakeholders to contact ONC throughout ONC's direct review with information about non-conformities that would be relevant during ONC's direct review of certified health IT. We do not, however, believe providers should be parties to an appeal. The matters potentially under review relate to the continued conformity of certified health IT to Program requirements that health IT developers have voluntarily accepted as part of certification of their health IT.

d. Consequences of Certification Termination

We stated in the Proposed Rule that, in general, this rulemaking does not address the consequences of certification termination beyond requirements for recertification. We stated that any consequences of, and remedies for, termination beyond recertification requirements are outside the scope of this rulemaking.

Comments. A commenter emphasized that all users of certified health IT, not just those participating in the EHR Incentive Programs, should be taken into account when addressing the consequences of certification termination. Other commenters expressed concern about the impact certification termination could have on providers participating in the EHR Incentive Programs (*e.g.,* with attestation) and other affected programs. These commenters pointed out that providers using a health IT product with a terminated Complete EHR or Health IT Module certification or one under appeal would risk failing to comply with CMS regulations. Commenters recommended that ONC coordinate with CMS to ensure sufficient protection for affected providers.

Response. We thank commenters for their feedback. We reiterate as stated above and in the Proposed Rule, that any consequences of, and remedies for, termination beyond recertification requirements are outside the scope of this rulemaking (*i.e.,* final rule). We, however, emphasize that we, and HHS as a whole, are committed to working with all users and providers in cases of termination to mitigate the impact on participants of programs requiring the use of certified health IT, particularly participants in HHS programs. As mentioned earlier under the ''termination'' section of this preamble, we intend to use the CHPL and other appropriate forms of publication and dissemination to notify users of health IT certification terminations.[13] We will also coordinate with affected HHS programs to facilitate the notification of their participants and to identify and make available appropriate remedies for participants. As noted in the Proposed Rule, CMS has issued a FAQ[14] for the EHR Incentive Programs informing participants about their options if the health IT they are using to participate in the programs has its certification terminated.

We note that an ONC certification termination under appeal stays the termination. This means the health IT remains certified while the appeal is ongoing. Similarly, health IT with a suspended certification as a result of ONC direct review is still certified and could be identified as certified health IT for HHS program purposes. While our goals with this final rule are to enhance Program oversight and health IT developer accountability for the performance, reliability, and safety of certified health IT, we remind stakeholders that we have finalized methods (*e.g.,* CAPs) designed to identify and remedy non-conformities so that health IT can maintain its certification.

(1) Certification Ban, Recertification, and Heightened Scrutiny

We proposed in the Proposed Rule that a Complete EHR or Health IT Module that has had its certification terminated can be tested and recertified once all non-conformities have been adequately addressed. We proposed that the recertified Complete EHR or Health IT Module (or replacement version) must maintain a scope of certification that, at a minimum, includes all the previously certified capabilities. We proposed that the health IT developer must request permission from ONC to participate in the Program before submitting the Complete EHR or Health IT Module (or replacement version) for testing to an ONC–ATL and recertification (certification) by an ONC–ACB under the Program. As part of its request, we proposed that a health IT developer must submit a written explanation of what steps were taken to address the non-conformities that led to the termination. We also proposed that ONC would need to review and approve the request for permission to participate in the Program before testing and recertification (certification) of the Complete EHR or Health IT Module (or replacement version) can commence under the Program.

We proposed in the Proposed Rule that if the Complete EHR or Health IT Module (or replacement version) is recertified (certified), the certified health IT product should be subjected to some form of heightened scrutiny by ONC or an ONC–ACB for a minimum of one year. We requested comments on the forms of heightened scrutiny (*e.g.,* quarterly in-the-field surveillance) and length of time for the heightened scrutiny (more or less than one year, such as six months or two years) of a recertified Complete EHR or recertified Health IT Module (or replacement version) that previously had its certification terminated. We requested comment on whether heightened scrutiny (surveillance or other requirements) should apply for a period of time (*e.g.,* six months, one year, or two years) to all currently certified Complete EHRs or certified Health IT Modules, future versions of either type, and all new certified health IT of a health IT developer that has a product's certification terminated under the Program.

We proposed in the Proposed Rule that the testing and certification of any health IT of a health IT developer that has the certification of one of its health IT products terminated under the Program or withdrawn from the Program when the subject of a potential non-conformity (notice of potential non-conformity) or non-conformity would be prohibited (''Program Ban''). We stated that the only exceptions would be if: (1) The non-conformity is corrected and implemented to all affected customers; or (2) the certification and implementation of other health IT by the health IT developer would remedy the non-conformity for all affected customers. We noted in the Proposed Rule that prohibiting the certification of new products, unless it serves to correct the non-conformity for all affected customers, may incentivize a health IT developer to cure the non-conformity. In correcting the non-conformity for all affected customers, we stated that this would not include those customers that decline the correction or fail to cooperate. We requested comment on this proposal, including how the health IT developer should demonstrate to ONC that all necessary corrections were completed. We further requested comment as to whether correcting the non-conformity for a certain percentage of all affected customers or certain milestones demonstrating progress in correcting the non-conformity (*e.g.,* a percentage of customers within a period of time) should be sufficient to lift the prohibition.

We discuss the proposals, comments, and our responses below beginning with the ''Program Ban'' proposal. We note that we have renamed the proposed ''Program Ban'' as ''Certification Ban'' (also simply referred to as ''Ban'' in this final rule). This name more accurately aligns with the effect of the Ban, which is to prohibit the certification of health IT. This also assists in clarifying that testing of health IT may still occur, which as discussed below, may be necessary as part of the process of ''reinstatement and remediation of all

[13] As mentioned under the ''suspension'' section of this preamble, we will take the same steps to notify users of health IT that has its certification suspended under the Program.

[14] *See* CMS EHR Incentive Programs FAQ 12657: *https://questions.cms.gov/faq.php?isDept=0&search=decertified&searchType=keyword&submitSearch=1&id=5005.*

affected customers.'' We note that we address the ''recertification'' proposal as part of the ''Reinstatement and Remediation for All Affected Customers'' discussion. This approach provides the most clarity regarding the final policies of this final rule.

Certification Ban

Comments. Many commenters opposed the Ban, stating that it should only apply to health IT that has a non-conformity. Commenters stated that a Ban would prevent timely upgrades, such as delivery of new functionality or necessary enhancements to users. Other commenters supported the Ban. One commenter requested clarification on how health IT developers are defined for the purposes of the Ban, inquiring if the Ban includes corporate subsidiaries of health IT developers and if they are also subject to the Ban.

Response. We thank commenters for their input and have finalized this proposal, subject to revisions and clarifications in response to comments. We continue to believe, despite the potential impact on other customers of health IT developers, that prohibiting the certification of health IT, unless it serves to correct the non-conformity, may incentivize a health IT developer to cure non-conformities and remedy the situation for affected customers. Therefore, we have finalized a Certification Ban. We have, however, included revisions both for clarity and to provide more flexibility for health IT developers to meet the requirements for lifting a Certification Ban. These revisions are discussed directly below and in the ''Reinstatement and Remediation for All Affected Customers'' section that follows.

We first clarify that ''termination'' in this final rule means an ONC action to ''terminate'' or ''revoke'' the certification status of a Complete EHR or Health IT Module. Conversely, an action by an ONC–ACB to ''terminate,'' ''remove,'' or ''revoke'' the certificate of a Complete EHR or Health IT Module is referred to as ''withdrawal.'' ISO/IEC 17065 defines the requirements for conformity assessment by ONC–ACBs and defines ''withdrawal'' (as defined in ISO 17000)[15] as a revocation or cancellation of the statement of conformity.[16] This occurs in two situations: (1) When an ONC–ACB proactively removes a certification based on its own accord; or (2) when a health IT developer initiates the discontinuation of a product's certification and requests that the ONC–ACB remove the product's certificate. We make the distinction between ''termination'' and ''withdrawal'' to conform with ISO's use of ''withdrawal'' throughout the ISO standards. However, ONC retains use of the term ''termination'' in this final rule because we enforce Program requirements directly, not under delegated authority and not subject to ISO standards, as is the case for ONC–ACBs. We use this new terminology in our explanation of final Ban provisions below, throughout the new §§ 170.580 and 170.581, and in revisions to § 170.556(d)(6) that we are finalizing in this final rule to align with ISO/IEC 17065. In § 170.556(d)(6), we changed ''termination'' to ''withdrawal'' and ''terminating'' to ''withdrawing.''

We clarify that the certification of any of a health IT developer's health IT is prohibited when the certification of one or more of the health IT developer's Complete EHRs or Health IT Modules is (1) terminated by ONC under the Program; (2) withdrawn from the Program by an ONC–ACB because the health IT developer requested it to be withdrawn when the health IT developer's health IT was the subject of a potential non-conformity or non-conformity as determined by ONC; (3) 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; or (4) withdrawn by an ONC–ACB because the health IT developer requested it to be withdrawn 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 pending surveillance (*e.g.,* the health IT developer received notice of pending randomized surveillance). This more detailed specification regarding when a Certification Ban applies is consistent with our proposals, including our proposal to apply the Certification Ban to withdrawals completed by ONC–ACBs. We clarify that for ONC–ACBs' withdrawals as specified in (3) and (4) above, the focus is on non-conformities with certification criteria and not non-conformities arising from §§ 170.523(k)(1) (disclosure of information about limitations and additional types of costs associated with their certified health IT), 170.523(l) (compliance with rules governing the use of the ONC Certification and Design Mark), or 170.523(n) (submit user complaints to ONC–ACBs).

We also clarify that the Certification Ban affects health IT developers participating in the Program, their subsidiaries, and their successors.

Reinstatement and Remediation for All Affected Customers

Comments. A commenter requested clarification on what qualifies as adequately addressing a non-conformity. We received mixed comments on whether a terminated health IT product (if presented for recertification) should be required to maintain a scope of certification that, at a minimum, includes all the previous certified capabilities. A few commenters supported our proposal, stating that any reduction in scope penalizes providers who may face significant financial penalties, and that physicians rely on their purchased product to best fulfill their practice needs. In contrast, some commenters expressed general opposition to our proposed approach.

One commenter recommended that the Certification Ban be lifted once ONC is satisfied with the corrective action rather than be dependent on customer acceptance or adoption of the corrected certified IT or other remedies. Similarly, a couple of other commenters recommended that all users must have the correction available (whether they choose to install or not). One of these commenters contended that decisions to implement patches may dictate when the customer's non-conforming health IT will be corrected for the customer.

Response. We have finalized the proposed requirements that a health IT developer must request permission to participate in the Program, explain the steps taken to address the non-conformities that led to the certification termination (or withdrawal), and receive approval from ONC to participate in the Program again. Specifically, for the Certification Ban to be lifted, we require that: (1) A health IT developer must request in writing ONC's permission to participate in the Program; (2) the request must demonstrate that the customers affected by the certificate termination or withdrawal have been provided appropriate remediation; and (3) ONC is satisfied with the health IT developer's demonstration that all affected customers have been provided with appropriate remediation and grants reinstatement into the Program. These requirements are consistent with our proposals and address our primary goal of addressing affected customers, particularly the requirement of appropriate remediation. We discuss the aspects of ''appropriate remediation'' in our responses to comments below.

We agree with some commenters that a reduction in scope unfairly penalizes customers who rely on their purchased or licensed certified health IT to best fulfill their practice needs. As stated in

[15] ISO/IEC 17000 (2004).

[16] We note that ISO does not explicitly define ''terminate.''

the Proposed Rule, health IT is tested and certified to meet adopted certification criteria and requirements. It should continue to meet those certification criteria and requirements when implemented. Therefore, in determining whether a health IT developer has demonstrated that all affected customers have been provided with appropriate remediation, we will require that the scope of certified health IT previously provided to the affected customers be maintained (*i.e.,* a health IT developer must demonstrate, and ONC is satisfied, that all the necessary certified health IT has been made available to affected customers). We note, as discussed in more detail below, that an affected customer can choose alternative means of remediation, which would be sufficient for lifting the Ban.

We agree with commenters that the Certification Ban may be lifted once ONC is satisfied that all non-conformities have been addressed and the correction is *made available* for all affected customers. However, in providing appropriate remediation to affected customers, we acknowledge that there may be other ways for health IT developers to correct situations for customers short of correcting the certified version or providing a replacement certified version. Therefore, we provide that, as determined by ONC, other certified health IT may be made available by the health IT developer that would remedy the non-conformity for all affected customers. This certified health IT may be the health IT of another health IT developer.

We also agree with commenters that there may be reasons why a customer does not implement the corrected certified version or other available certified health IT in a timely manner or at all. As noted in the Proposed Rule (81 FR 11066), we will take into consideration customers' responses (*e.g.,* the customer declines or postpones the correction or signs a release of obligation, which may be the result of a financial settlement) when we determine whether a health IT developer has demonstrated that appropriate remediation has been provided to all affected customers.

We clarify that ONC has sole discretion to lift a Certification Ban. The Certification Ban shall remain in effect until ONC is satisfied that the health IT developer has taken the required steps to lift the Certification Ban, as described above. If ONC chooses not to lift the Certification Ban, the health IT developer may reapply for reinstatement after taking the necessary actions to address the conditions for reinstatement.

Comments. Commenters requested clarification regarding what would be tested and certified upon applying for ''recertification.''

Response. As part of ONC's considerations as to whether to lift the Certification Ban, ONC, or a third party acting on its behalf, may require the health IT presented as replacement certified health IT for affected customers to be tested by an ONC–ATL, particularly if the replacement health IT is a version of the health IT that previously had the non-conformity that led to termination or withdrawal. This may also be the case when one of multiple Health IT Modules used to maintain the same scope of the terminated or withdrawn certified health IT was never the subject of ONC direct review or ONC–ACB surveillance but includes the same capabilities that were connected to the non-conformity (*e.g.,* CPOE capabilities). After passing necessary testing, the health IT could be certified by an ONC–ACB.

Comments. A commenter recommended that a health IT developer be required to provide their customer list to ONC and ONC could verify that the correction has been completed for a random selection of users. This commenter also suggested that ONC could alternatively rely on the health IT developer to attest that all installed products have been corrected or are available to users.

Response. We agree with the commenter that either approach could be used by ONC to verify that appropriate remediation has been provided for all affected customers. However, as noted above, we will require the health IT developer to *demonstrate* that all affected customers have been provided with appropriate remediation, which would include listing the form of remediation. We may also randomly or methodically verify this information with affected customers.

Heightened Scrutiny

Comments. A few commenters recommended that heightened scrutiny only apply to the functionality that was subject of the alleged non-conformity and not to all health IT of a health IT developer. Some commenters requested that we further define heightened scrutiny. A couple of commenters suggested that heightened scrutiny should vary based on the scope of the non-conformity. One commenter supported using multiple forms of heightened scrutiny, including in-the-field surveillance. Two commenters recommended going beyond randomized in-the-field surveillance where the health IT developer would be surveilled more frequently.

We received mixed comments as to the length of heightened scrutiny. Some commenters recommended six months, while others recommended one year.

Response. We have not finalized our proposal for applying heightened scrutiny at this time because, after consideration of the public comments, we believe that existing procedures already adequately result in ''heightened scrutiny,'' where appropriate. As noted above, it is possible that remediation for customers affected by a termination or withdrawal could consist of providing certified health IT that never had a non-conformity. In such instances, there would be no need for any form of heightened scrutiny. Further and again as noted above, the process of reinstatement will provide an opportunity for ONC to scrutinize any health IT presented for recertification. We also believe that surveillance conducted by ONC–ACBs as part of their routine activities can provide additional scrutiny of ''recertified'' health IT. To this point, ONC–ACBs conducting reactive surveillance (*e.g.,* complaints-based) can take into account whether the health IT at issue was ''recertified'' health IT and whether the nature of the complaint correlates with a prior non-conformity found in the health IT. As for in-the-field surveillance, it could be weighted towards health IT that was ''recertified.''

We note that we have added an element to a CAP that addresses steps to prevent a non-conformity from re-occurring (*see* the ''Corrective Action'' section earlier in this final rule).

(2) ONC–ACB Response to a Non-Conformity

We stated in the Proposed Rule that ONC–ACBs are accredited to ISO/IEC 17065. Section 7.11.1 of ISO/IEC 17065 instructs certification bodies to consider and decide upon the appropriate action to address a non-conformity found, through surveillance or otherwise, in the product the certification body certified.[17] Section 7.11.1 lists, among other appropriate actions, the reduction in scope of certification to remove non-conforming product variants or withdrawal of the certification. We stated in the Proposed Rule that these are not appropriate responses to a non-conformity under the Program.

We proposed in § 170.523 to revise the PoPC for ONC–ACBs, to prohibit

[17] 45 CFR 170.599(b)(3).

ONC–ACBs from reducing the scope of a certification when the health IT is under surveillance or a CAP. The proposed revision addressed two situations: (1) When health IT is suspected of a non-conformity (*i.e.,* under surveillance or surveillance is pending); and (2) when health IT has a non-conformity (*i.e.,* under a CAP). We proposed that a health IT developer's withdrawal of its certified health IT from the Program when the certified health IT is under surveillance, or surveillance is pending, by an ONC–ACB should not be without prejudice (*i.e.,* the health IT developer would be subject to a ''Certification Ban'' of its health IT). We further proposed that the same proposed consequences for health IT and health IT developers related to certification termination under ONC direct review (*i.e.,* all of the § 170.581 proposals) should apply to certification withdrawals issued by ONC–ACBs. We requested comment on these proposals.

Reduction in Scope

Comments. Some commenters opposed the proposed requirement to maintain the scope of a certification when the health IT is under surveillance or a CAP, while a few commenters supported our proposal. One commenter stated that they believe these requirements could potentially be too prescriptive and could stifle innovation among health IT developers. However, another commenter stated that providers rely on their certified health IT to provide the functionality as represented to them both in general and for the EHR Incentive Programs and allowing a reduction in scope of certification to remove non-conforming product variants after implementation unfairly penalizes providers.

Response. We thank commenters for their feedback. To ensure alignment between ONC review and actions and ONC–ACBs' surveillance and actions under the Program, we have finalized our proposal in § 170.523(o) to prohibit the reduction in scope of certified health IT (1) when the certified health IT is suspected of a non-conformity (*i.e.,* under surveillance or surveillance is pending); and (2) when health IT has a non-conformity (*i.e.,* under a CAP). We agree with commenters that, as we stated in the Proposed Rule, a reduction in scope would absolve a health IT developer from correcting a non-conformity. Health IT is tested and certified to meet adopted criteria and requirements. It should continue to meet those criteria and requirements when implemented. If not, the health IT developer should correct the health IT for affected customers or be subjected to certification withdrawal. While we expect that health IT developers would correct the non-conformity in most cases, we do permit various options for health IT developers to address the situation if the health IT certification is withdrawn.[18] Therefore, we do not agree that the approach is overly prescriptive or that it will stifle innovation.

Voluntary Withdrawal When Suspected of a Non-Conformity

Comments. One commenter stated that voluntary withdrawal by a health IT developer might be the most satisfactory action to enable the majority of the health IT to remain viable in the marketplace. Two commenters recommended that we state that a health IT developer's withdrawal of its certified health IT from the Program constitutes an admission of non-conformity.

Response. We thank commenters for their feedback. We agree with the commenters that a health IT developer's withdrawal of its certified health IT from the Program could be utilized to avoid a finding of non-conformity. Therefore, we have finalized the proposed consequences for a health IT developer's withdrawal of its certified health IT from the Program when the health IT is suspected of a non-conformity (*i.e.,* under surveillance or surveillance is pending) by an ONC–ACB. Specifically, a health IT developer's health IT would be subject to a Certification Ban as discussed under the ''Certification Ban'' section of the preamble above.

Application of § 170.581 to Certification Withdrawals Executed by ONC–ACBs

We have finalized the proposed ''Program Ban'' (now called ''Certification Ban''), including application to certification withdrawals executed by ONC–ACBs. We refer readers to the ''Certification Ban, Recertification, and Heightened Scrutiny'' section above for the comments we received on these proposals and the revisions we have made in response to comments.

2. Establishing ONC Authorization for Testing Labs Under the Program; Requirements for ONC–ATL Conduct; and ONC Oversight and Processes for ONC–ATLs

a. General Comments on ONC–ATL Approach

Comments. Commenters overwhelmingly supported the proposals to establish ONC–ATLs and provide for ONC oversight of ONC–ATLs under the Program. Two commenters stated that they do not support ONC accreditation in addition to current NVLAP accreditation, but expressed support for establishing ''ONC administrative controls'' over the accredited testing labs similar to ONC's oversight of the ONC–ACBs. Some commenters recommended that we include more robust testing or consider outlining a testing framework with appropriate testing methodologies to be utilized by ONC–ATLs.

Response. We thank commenters for their support and have finalized the requirements for ONC–ATL status and the framework for ONC oversight of ONC–ATLs under the Program. In response to the two commenters stating that they do not support ''ONC accreditation'' in addition to current NVLAP accreditation, we believe these commenters misinterpreted our proposals as we did not propose any additional ONC accreditation requirements. To clarify, the proposals being finalized in this final rule do not require labs applying for ONC–ATL status to obtain additional accreditation beyond NVLAP accreditation for health IT testing. Further, these new provisions are in line with the commenters' recommendations by providing ONC with ''administrative controls'' over ONC–ATLs in a manner similar to ONC–ACBs by enabling ONC to authorize and have oversight of ONC–ATLs under the Program. We appreciate commenters' recommendations regarding more robust testing and testing frameworks, however, these recommendations are outside the scope of our proposals.

b. Regulatory Provisions for Inclusion of ONC–ATLs in the Program

The following sections detail each new and amended regulatory provision that we proposed and have finalized for subpart E of part 170, starting with 45 CFR 170.501, in order to include ONC–ATLs as part of the Program. As stated as our intention in the Proposed Rule, for authorization and other processes, we have followed and leveraged all of the processes established for ONC–ACBs.

[18] Please also see the options for health IT developers to address certification termination/withdrawal discussed under the ''Certification Ban'' section of the preamble above.

(1) § 170.501 ''Applicability''

We proposed to revise paragraph (a) of § 170.501 to include references to ''applicants for ONC–ATL status,'' ''ONC–ATL,'' and ''ONC–ATL status.''

Comments. Commenters expressed support for the proposed revisions.

Response. We thank commenters for their support and have adopted the revisions to § 170.501 as proposed. The revisions make clear that ONC–ATLs are now part of the rules under this subpart. We have also revised § 170.501 to clearly state that this subpart includes requirements related to the direct review processes adopted in this final rule. These references were inadvertently left out of § 170.501 in the Proposed Rule, although they were included elsewhere in the preamble discussion and regulation text. Further, we revised § 170.501 to clarify that accreditation organizations only apply to become an ONC–AA under the Program and not the accreditor for testing under the Program. NVLAP is the permanent accreditor for testing under the Program (*see* 76 FR 1278). For regulatory clarity, we have reorganized the prior provisions and new provisions into four paragraphs.

(2) § 170.502 ''Definitions''

We proposed to revise the definition of the term ''applicant,'' in § 170.502, to include a corresponding reference to ONC–ATL in order for such term to have equal meaning in the case of a testing lab that is applying for ONC–ATL status.

We proposed to revise the definition of the term ''gap certification,'' in § 170.502, to include a corresponding reference to ONC–ATL in paragraph (1) of that definition in order to give equal weight to test results issued by an ONC–ATL. We also proposed to add ''under the ONC Health IT Certification Program'' to paragraphs (1) and (2) of the definition to improve the clarity of the definition.

We proposed in § 170.502 to define the term ''ONC–Authorized Testing Lab'' or ''ONC–ATL'' to mean an organization or consortium of organizations that has applied to and been authorized by the National Coordinator to perform the testing of Complete EHRs and Health IT Modules to certification criteria adopted by the Secretary in subpart C of this part.

Comments. Commenters expressed support for the proposed revisions and additions to § 170.502.

Response. We thank commenters for their support and have finalized the revisions and additions to § 170.502 as proposed.

(3) § 170.505 ''Correspondence''

We proposed to revise § 170.505 to include references to ONC–ATL as appropriate.

Comments. Commenters expressed support for the proposed revisions to this section.

Response. We thank commenters for their support and have finalized the revisions to § 170.505 as proposed. This will reflect the addition of an applicant for ONC–ATL status and ONC–ATLs to the Program framework. We also refer readers to section II.A.1.c (''Review Processes'') for further revisions to § 170.505 finalized in this final rule.

(4) § 170.510 ''Type of Certification''

We proposed to revise the section heading of § 170.510 to specifically reference the authorization scope of ONC–ACB status. We also proposed to revise the introductory text within this section to more clearly convey that this section is solely focused on applicants for ONC–ACB status.

Comments. Commenters expressed support for the proposed revisions.

Response. We thank commenters for their support and have finalized the revisions to § 170.510 as proposed.

(5) § 170.511 ''Authorization Scope for ONC–ATL Status''

We proposed to establish a new section (§ 170.511) to clearly define the scope of the authorization an ''applicant'' testing lab may be able to seek from the National Coordinator. We proposed that such authorization be limited to the certification criteria adopted by the Secretary in subpart C of this part. We proposed that an applicant for ONC–ATL status could seek for the scope of its authorization all certification criteria, a subset of all of the certification criteria (*e.g.,* to support only privacy and security testing), one certification criterion, or a portion of one certification criterion. We stated that the latter two options provide opportunities for entities that may perform industry testing of health IT for limited and/or distinct capabilities (*e.g.,* electronic prescribing) that align with certification criteria to participate in the Program.

Comments. Commenters expressed support for the new proposed section for ONC–ATLs. Some commenters recommended ONC permit the acceptance of certification results from an organization that has already performed testing and certification of health IT that are aligned with, or could be aligned with, ONC certification criteria.

Response. We thank commenters for their support for the new section and have finalized the section as proposed to support specialized testing and testing efficiencies for health IT. We stated in the Permanent Certification Program final rule, in response to comments, that we did not believe it was appropriate to rely on testing results from laboratories that were not NVLAP-accredited as we could not independently verify the accreditation processes for the testing labs (76 FR 1281). We believe our approach of requiring narrowly scoped NVLAP accreditation and ONC–ATL status for limited testing under the Program (*e.g.,* e-prescribing) provides the efficiencies (*i.e.,* avoid duplicative testing and reduces regulatory burden) that commenters requested, while maintaining ONC oversight and the integrity of certified health IT and the Program.

(6) § 170.520 ''Application''

We proposed to reorder the regulatory text hierarchy to reference the ONC–ACB application requirements under § 170.520(a) and then the ONC–ATL application requirements under § 170.520(b). For the ONC–ATL requirements, we proposed that an ONC–ATL applicant would need to seek authorization based on the scope proposed in § 170.511 and follow the proposed set of ONC–ATL application requirements. More specifically, we proposed that the application information include the same general identifying information as for ONC–ACB applicants; the same authorized representative designation; documentation that the applicant has been accredited by NVLAP to ISO/IEC 17025; and a written agreement executed by the authorized representative stating that the applicant will adhere to the PoPC for ONC–ATLs.

Comments. Commenters expressed support for the ONC–ATL application requirements. Some commenters noted that NVLAP bases its accreditation of testing labs under the Program on both ISO/IEC 17025 *and* elements specific to the Program (*e.g.,* test procedure requirements and competencies). One commenter requested that we establish a minimum set of testing documentation for test results. This commenter also requested that we require ONC–ATLs to submit a list of all received complaints on a quarterly basis, which would be the same as the requirement for ONC–ACBs.

Response. We thank commenters for their support and have finalized the ONC–ATL application requirements with one clarification based on the comments received. We clarify that ''documentation that confirms that the applicant has been accredited by

NVLAP to ISO/IEC 17025'' includes accreditation by NVLAP to health IT competencies and other Program-specific requirements as noted by commenters. To provide this clarity in § 170.520, we have revised paragraph (b)(3) to read ''documentation that confirms that the applicant has been accredited by NVLAP, including to ISO/IEC 17025.'' To ensure uniformity, ONC, NVLAP, the ONC–AA, ONC–ACBs, and accredited testing labs have collaborated and agreed upon a minimum set of documentation that ONC–ATLs shall provide the ONC–ACBs for their certification evaluation, review, and decision. Last, we note that the recommendation to require ONC–ATLs to submit quarterly reports on complaints is outside of the scope of our proposals as we did not propose such a requirement for ONC–ATLs as we did for ONC–ACBs in the 2015 Edition proposed rule.

(7) § 170.523 ''Principles of Proper Conduct for ONC–ACBs''

We proposed to revise paragraph (h)(1) of § 170.523 to explicitly include ONC–ATLs as an entity from whom ONC–ACBs would receive test results. We further proposed to modify paragraph (h)(2) of § 170.523 to include a six month time window from the authorization of the first ONC–ATL to permit the continued acceptance by ONC–ACBs of *any* test results from a NVLAP-accredited testing laboratory. As stated in the Proposed Rule, this approach would provide adequate transition time for ONC–ACBs to continue issuing certifications based on test results for new and revised certification criteria issued by a ''NVLAP-accredited testing laboratory'' and would also serve as a mobilizing date for a testing lab that has not yet applied for ONC–ATL status. We requested comment, however, on the transition period from NVLAP-accredited testing laboratories to ONC–ATLs. Specifically, we requested comment on whether we should alternatively establish that ONC–ACBs may only be permitted to accept *any* test results from a NVLAP-accredited testing laboratory for a period of time from the effective date of a subsequent final rule. We stated that this approach would provide a more certain timetable for ONC–ACBs compared to the proposed approach, but may not provide sufficient time for all NVLAP-accredited testing laboratories to transition to ONC–ATL status. We also requested comment on whether the transition period should be shorter than six months (*e.g.,* three months) or longer (*e.g.,* nine months) under either the proposed approach or the alternative approach.

We proposed in § 170.523(h)(2) to permit the use of test results from a NVLAP-accredited testing laboratory for certifying previously certified health IT to unchanged certification criteria (gap certification) because, as proposed, NVLAP-accredited testing laboratories would be replaced with ONC–ATLs. We stated that this proposal would permit the test results issued by NVLAP-accredited testing laboratories under the Program (*e.g.,* test results for health IT tested to the 2014 Edition) to continue to be used for gap certification. As a related proposal, we proposed to remove references to ONC–ATCBs in § 170.523(h). ONC–ATCBs tested and certified health IT to the 2011 Edition. The 2011 Edition has been removed from the Code of Federal Regulations and ONC–ACBs no longer maintain active certifications for health IT certified to the 2011 Edition.

Comments. Commenters expressed support for our proposed revisions to § 170.523 to accommodate inclusion of ONC–ATLs in the Program. One commenter commented on the proposed accredited testing lab to ONC–ATL transition timeframe. The commenter recommended that we adopt a specified timeframe from the effective date of this final rule for NVLAP-accredited testing labs to become authorized as ONC–ATLs rather than a six-month timeframe from the authorization of the first ONC–ATL. Another commenter stated that the removal of reference to ONC–ATCBs could imply that gap certification is not permitted based on the use of test results from a 2011 Edition certification issued by an ONC–ATCB. The commenter recommended that we clarify whether test results used for 2011 Edition certified health IT could be used for the purposes of gap certification.

Response. We appreciate commenters' support for our proposed revisions to § 170.523 and have finalized our revisions to include ONC–ATLs and remove references to ONC–ATCBs from the section. We agree with the commenter that the best approach to meet our goal stated in the Proposed Rule of establishing a certain timetable to facilitate the transition for accredited testing labs to ONC–ATLs would be to set a timeframe from the effective date of this final rule for the transition. Therefore, we have established a timeframe of ''six months from the effective date of this final rule'' to provide a more certain timeframe. We believe this timeframe, over eight months from the issuance of this final rule, provides sufficient time to account for any potential delays or unforeseen circumstances (*e.g.,* time and resource conflicts with significant requests for 2015 Edition testing and certification by health IT developers).

The removal of reference to ONC–ATCBs was not meant to imply that gap certification is not permitted based on the use of test results from a 2011 Edition certification issued by an ONC–ATCB. Therefore, we have revised the regulation text to add back in specific reference to ONC–ATCBs in § 170.523(h)(3). We believe this step will sufficiently clarify that these test results may still be used for gap certification. We emphasize, however, that granting gap certification has always been at the discretion of an ONC–ACB. We would, however, expect that an ONC–ACB would consider the temporal nature of test results and other relevant changes in the health IT brought forward for gap certification when determining whether to grant gap certification.

(8) § 170.524 ''Principles of Proper Conduct for ONC–ATLs''

We proposed to establish, in a new section (§ 170.524), a set of PoPC to which ONC–ATLs must adhere, which are similar to the set of rules and conditions for ONC–ACBs. We stated that adherence to these conduct requirements would be necessary for ONC–ATLs to maintain their authorization and to remain in good standing under the Program. As outlined and described in the Proposed Rule, many of the proposed PoPC for ONC–ATLs would remain consistent with those to which ONC–ACBs are already required to adhere.

Comments. Commenters expressed support for the new PoPC for ONC–ATLs.

Response. We thank commenters for their support and have adopted the new PoPC for ONC–ATLs in § 170.524. Consistent with the clarification we provided for § 170.520, we clarify that the requirement to maintain ''NVLAP accreditation to ISO/IEC 17025'' entails more than just accreditation to ISO/IEC 17025 as NVLAP accredits testing labs to other requirements under the Program. To provide this clarity in § 170.524, we have revised paragraph (a) to read ''Maintain its NVLAP accreditation, including accreditation to ISO/IEC 17025.''

Comments. One commenter stated, in regard to the proposed PoPC allowing ONC to periodically observe testing on site (unannounced or scheduled), that it would be more efficient for ONC staff to try and coordinate with the ONC–ATL for on-site visits since each testing session involves a significant amount of coordination and scheduling.

Response. We appreciate the commenter's point, but have retained the discretion in the final PoPC to observe, unannounced, on-site health IT testing. As with the PoPC for ONC–ACBs, we believe the prospect of unannounced visits supports Program compliance monitoring and the overall integrity of the Program. We note, however, that we intend to work with ONC–ATLs, as we do with ONC–ACBs, to provide the necessary notice to conduct useful and efficient on-site observation of health IT testing.

(9) § 170.525 ''Application Submission''

We proposed to include reference to an applicant for ONC–ATL status in paragraphs (a) and (b) of § 170.525 to clearly recognize that testing labs would be applying for ONC–ATL status. We proposed the same application rules that apply to applicants for ONC–ACB status.

Comments. Commenters expressed support for the proposed addition to this section.

Response. We thank commenters for their support and have finalized the inclusion of ''an applicant for ONC–ATL status'' in § 170.525 as proposed.

(10) § 170.530 ''Review of Application''

We proposed to revise paragraphs (c)(2), (c)(4), (d)(2), and (d)(3) of § 170.530 to include an ONC–ATL as part of the application review process. Further, in so doing, we proposed to follow all of the same application review steps and processes that we follow for applicants for ONC–ACB status.

Comments. Commenters expressed support for the proposed revisions to this section.

Response. We thank commenters for their support and have finalized the revisions to § 170.530 as proposed.

(11) § 170.535 ''ONC–ACB Application Reconsideration''

We proposed to revise the section heading of § 170.535 to include reference to ONC–ATLs. We also proposed to revise paragraphs (a) and (d)(1) of § 170.535 to equally reference that an ONC–ATL could be part of the application reconsideration process. Further, in so doing, we proposed to follow all of the same application reconsideration steps and processes that we require and follow for applicants for ONC–ACB status.

Comments. Commenters supported our proposed revisions to this section.

Response. We thank commenters for their support and have finalized the revisions to § 170.535 as proposed.

(12) § 170.540 ''ONC–ACB Status''

We proposed to revise the section heading of § 170.540 to include reference to ONC–ATLs. We also proposed to revise paragraphs (a) through (d) of § 170.540 to equally reference an ONC–ATL as part of the rules currently governing the achievement of ONC–ACB status. As stated in the Proposed Rule, these rules would include: The acknowledgement of ONC–ATL status; that an ONC–ATL must prominently and unambiguously identify the scope of its authorization; that ONC–ATL authorization must be renewed every three years; and that ONC–ATL status would expire three years from when it was granted unless renewed.

Comments. Commenters supported our proposed revisions to this section.

Response. We thank commenters for their support and have finalized the revisions to § 170.540 as proposed.

(13) § 170.557 ''Authorized Certification Methods''

We proposed to revise the section heading of § 170.557 to include a reference to ''testing.'' We also proposed to update the regulatory text hierarchy to have paragraph (a) be applicable to ONC–ATLs and paragraph (b) be applicable to ONC–ACBs.

Comments. Commenters expressed support for our proposed revisions to this section.

Response. We thank commenters for their support and have finalized the proposed revisions to make § 170.557 applicable to ONC–ATLs as we believe the requirement to provide for remote testing for both development and deployment sites is equally applicable to testing labs as it is to certification bodies.

(14) § 170.560 ''Good Standing as an ONC–ACB''

We proposed to revise the section heading of § 170.560 to include reference to ONC–ATLs. We also proposed to revise the paragraph hierarchy to make the paragraph (a) requirements applicable to ONC–ACBs (without modification) and to make the paragraph (b) requirements applicable to ONC–ATLs following the same set of three requirements as for ONC–ACBs.

Comments. Commenters supported our proposed revisions to the section.

Response. We thank commenters for their support and have finalized the revisions to § 170.560 as proposed. We believe mirroring the requirements of § 170.560 between ONC–ACBs and ONC–ATLs provides for consistent administration for both testing and certification under the Program.

(15) § 170.565 ''Revocation of ONC–ACB Status''

We proposed to revise the section heading of § 170.565 to include reference to ONC–ATLs. We also proposed to revise paragraphs (a) through (h) to include references to an ONC–ATL, as applicable. We proposed to apply the same oversight paradigm of Type-1 and Type-2 [19] violations to ONC–ATLs as we apply to ONC–ACBs. We further proposed to follow the same process for ONC–ATLs that is already included in this section for ONC–ACBs. We proposed to specifically add paragraph (d)(1)(iii) for ONC–ATL suspension provisions because the suspension provisions in paragraph (d)(1)(ii) are too specific to ONC–ACBs and simply referencing ONC–ATLs in that paragraph would cause confusion. Similarly, we proposed to specifically add paragraph (h)(3) related to the extent and duration of revocation to clearly divide the rules applicable to ONC–ACBs from those that would be applicable to ONC–ATLs. We explained that this proposed revision would place the current ONC–ACB applicable regulation text in paragraph (h)(2) of this section.

Comments. Commenters expressed support for the proposed revisions and additions to this section. One commenter requested clarification as to whether the timeframes proposed referenced calendar or business days. Another commenter stated that requiring an ONC–ATL or ONC–ACB to submit a written response within three days upon receipt of a notice of proposed suspension seems short since the National Coordinator has five days to respond to an ONC–ATL or ONC–ACB's written response to a notice of proposed suspension.

Response. We thank commenters for their support and have finalized the revisions and additions to § 170.565 as proposed. Our approach will enable ONC to treat similar fact-based non-compliance situations equitably among ONC–ACBs and ONC–ATLs. In regard

[19] Type-2 violations constitute non-compliance with 45 CFR 170.560 (Good standing as an ONC–ACB) (45 CFR 170.565(b)). An ONC–ACB must maintain good standing by: (a) Adhering to the Principles of Proper Conduct for ONC–ACBs; (b) 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 Complete EHRs and/or Health IT Module(s) for which it does not have authorization; and (c) Following all other applicable federal and state laws.

to the requested clarification for the use of ''days,'' we previously adopted the definition of ''day'' or ''days'' in § 170.102 to mean ''calendar day'' or ''calendar days'' (Temporary Certification Program final rule; 75 FR 36162, 36203). As stated in the Permanent Certification Program final rule, we believe suspension could be an effective way to protect purchasers of certified products and ensure patient health and safety. The requirements for an ONC–ATL or ONC–ACB to submit a written response to a proposed suspension within three days supports this goal, while still giving ONC–ACBs and ONC–ATLs an opportunity to respond. The National Coordinator has an additional two days to be able to consider the ONC–ATL or ONC–ACB response in conjunction with the reasons for proposing the suspension.

(16) § 170.570 Effect of Revocation on the Certifications Issued To Complete EHRs and Health IT Module(s)

We explained in the Proposed Rule that § 170.570 specifies rules applicable to certifications issued to Complete EHRs and/or Health IT Modules in the event that an ONC–ACB has had its status revoked. Section 170.570 includes steps that the National Coordinator can follow if a Type-1 violation occurred that called into question the legitimacy of certifications conducted by the former ONC–ACB. These provisions were put in place to provide clarity to the market about the impact that an ONC–ACB's status revocation would have on certified health IT in use as part of the EHR Incentive Programs.

In the context of an ONC–ATL having its status revoked, we did not specifically propose to modify § 170.570 to include a set of rules applicable to such a scenario. We stated that the same provisions were not necessary given the tangible differences between test results for a *not yet* certified Complete EHR and/or Health IT Module and an issued certification being used by hundreds or thousands of providers for participation in other programs, HHS or otherwise. We did, however, request comment on whether there would be any circumstances in which additional clarity around the viability of test results attributed to a not yet certified Complete EHR and/or Health IT Module would be necessary. We also requested comment as to whether we should include provisions similar to those already in this section to account for an instance where an ONC–ATL has its status revoked as a result of a Type-1 violation, which calls into question the legitimacy of the test results the ONC–ATL issued and, thus, could call into question the legitimacy of the subsequent certifications issued to Complete EHRs and/or Health IT Modules by a potentially unknowing or deceived ONC–ACB.

Comments. The majority of commenters agreed that § 170.570 did not need to be modified for a Complete EHR and/or Health IT Module *not yet* certified. Commenters stated that if a Complete EHR and/or Health IT Module had not yet been certified and its testing lab had its status revoked, the health IT developer could find another testing lab to complete its testing before certification. A couple of commenters recommended additional provisions for situations where an ONC–ATL is suspended for Type-1 violations (fraud or negligence) affecting the validity of the test results, but not for non-test-related issues (*e.g.* business practices or failure to report to ONC) that could also cause an ONC–ATL to have its status revoked. Several commenters also requested that we clarify how the National Coordinator would apply recertification requirements for ONC–ATL or ONC–ACB revocation due to a Type-2 violation.

Response. We thank commenters for their feedback. While we did not specifically propose to modify § 170.570 to include a set of rules applicable to an ONC–ATL having its status revoked, we did request comment on modifying § 170.570 to account for situations where an ONC–ATL has its status revoked as a result of a Type-1 violation, which calls into question the legitimacy of the test results the ONC–ATL issued and, thus, could call into question the legitimacy of the subsequent certifications issued to Complete EHRs and/or Health IT Modules by a potentially unknowing or deceived ONC–ACB. Given the feedback from commenters expressing the need for provisions to address certifications when ONC revokes an ONC–ATL's status and also determines that the test results are unreliable because of fraud or negligence or for other reasons that call into question the legitimacy of the test results the ONC–ATL issued, we have revised § 170.570 to address these situations.

We note that § 170.570 does not include the review of health IT certifications by the National Coordinator due to the revocation of ONC–ATL or ONC–ACB status for Type-2 violations. Under this section, the review of health IT certifications by the National Coordinator is limited to revocations based on a ''Type 1 violation that called into question the legitimacy of certifications issued to health IT.''

Comments. Several commenters requested clarification on how the National Coordinator would make an assessment on whether a health IT was ''improperly certified.'' Commenters also requested that ONC evaluate the likelihood that remaining ONC–ACBs would be able to accommodate all requests for recertification within the specified 120-day time period under § 170.570, noting that ONC–ACBs do not always have tremendous flexibility to schedule around other obligations, particularly during busy certification periods.

Response. As specified in § 170.570, the National Coordinator would review the facts surrounding the revocation and publish a notice on ONC's Web site if it was determined that Complete EHRs and/or Health IT Module(s) were ''improperly certified.'' We anticipate that this review would be case-specific and dependent on the basis of the revocation. To note, we have revised the regulation text to replace ''improperly certified'' with more accurate terminology. We believe use of ''unreliable testing or certification'' is more accurate and provides clarity for the situations under review as compared to ''improperly tested'' or ''improperly certified,'' particularly in situations where an ONC–ACB unknowingly uses unreliable test results.

In the Permanent Certification Program final rule (76 FR 1299–1300), we stated that programmatic steps, such as identifying ONC–ACB(s) that could be used for recertification, could be taken to assist health IT developers with achieving timely and cost effective recertifications. However, based on our accumulated knowledge of the time it takes for testing and certification under the Program and in response to comments, we acknowledge that there may be circumstances where it may not be possible for ONC–ATLs to accommodate all requests for retesting, as necessary, and ONC–ACBs to accommodate all requests for recertification within the 120-day time period. Accordingly, we have revised § 170.570 to permit the National Coordinator to extend the time that the certification status of affected Complete EHRs and/or Health IT Module(s) remains valid as necessary for the proper retesting and recertification of the affected health IT (*see* § 170.570(c)(2)).

B. Public Availability of Identifiable Surveillance Results

In the 2014 Edition final rule, for the purposes of increased Program transparency, we instituted a requirement for the public posting of the test results used to certify health IT (77 FR 54271). We also instituted a requirement that a health IT developer publicly disclose any additional types of costs that a provider would incur for using the health IT developer's certified health IT to participate in the EHR Incentive Programs (77 FR 54273–74). Building on these transparency and public accountability requirements for health IT developers, we took steps, in the 2015 Edition final rule, to increase the transparency related to certified health IT through required surveillance, broadened certified health IT disclosure requirements, and enhanced reporting requirements (80 FR 62719–25). For instance, we now require ONC–ACBs to report non-conforming findings and, when necessary, CAP information to the publicly accessible CHPL (80 FR 62725). The purpose of this reporting requirement, as described in the 2015 Edition final rule, is to ensure that health IT users, implementers, and purchasers are alerted to conformity issues in a timely and effective manner, consistent with the patient safety, program integrity, and transparency objectives of the 2015 Edition final rule (80 FR 62716–17).

In furtherance of our efforts to increase Program transparency and health IT developer accountability for their certified health IT we proposed in the Proposed Rule to revise § 170.523(i) of the PoPC for ONC–ACBs by adding language that would require ONC–ACBs to make identifiable surveillance results publicly available on their Web sites on a quarterly basis. We stated that these surveillance results would include information such as, but may not be limited to: Names of health IT developers; names of products and versions; certification criteria and Program requirements surveilled; and outcomes of surveillance. We further stated that this information is already collected by ONC–ACBs as part of their surveillance efforts under the Program and should be readily available for posting on their Web sites (81 FR 11070).

We clarified in the Proposed Rule that we do not require that publicly posted surveillance results include information that is proprietary, trade secret, or confidential (*e.g.,* ''screenshots'' that may include such information). We noted our expectation that health IT developers and ONC–ACBs would ensure that such information is not posted when making available the proposed information (*i.e.,* but not limited to, names of health IT developers; names of products and versions; certification criteria and Program requirements surveilled; and outcomes of surveillance).

We requested public comment on the publication of identifiable surveillance results. Specifically, we requested comment on the types of information to include in the surveillance results and the format (*e.g.,* summarized or unrefined surveillance results) that would be most useful to stakeholders. In addition to the proposal for ONC–ACBs to publish these results quarterly on their Web sites, we requested comment on the value of publishing hyperlinks on the ONC Web site to the surveillance results posted on the ONC–ACBs' Web sites (81 FR 11070).

Comments. We received overwhelming support for the publication of identifiable surveillance results by ONC–ACBs. A couple of commenters, however, questioned the benefit of posting conforming results, suggesting the number of results would be too low to be significant.

Response. We appreciate commenters' support for the publication of identifiable surveillance results by ONC–ACBs and are finalizing our proposal to make identifiable surveillance results of ONC–ACBs publicly available according to the form, manner, and frequency discussed below. We emphasize that these surveillance results will consist of findings of conformity, which are not currently published on the CHPL.

As we stated in the Proposed Rule, the publication of identifiable surveillance results with findings of conformity, much like the publication of non-conformities and CAPs on the CHPL under the 2015 Edition final rule, will help make health IT developers more accountable to the customers and users of their certified health IT. Customers and users will be provided with valuable information about the continued performance (*i.e.,* conformity under the Program) of certified health IT. The identifiable surveillance results will serve to inform providers and others currently using certified health IT as well as those that may consider switching their certified health IT or purchasing certified health IT for the first time. While we expect that the prospect of publicly identifiable surveillance results will motivate some health IT developers to improve their maintenance efforts, we continue to believe that published surveillance results will reassure customers and users of certified health IT that their health IT continues to conform to certification and Program requirements. This is because, based on ONC–ACB surveillance results to date, most of the surveilled certified health IT and health IT developers are maintaining conformity with certification criteria and Program requirements. The publishing of identifiable surveillance results will also provide a more complete context of surveillance in the certified health IT industry; rather than only sharing identifiable non-conforming results, and when applicable, CAPs (*see* § 170.523(f)).

We disagree with the commenters that suggested there may be little value in posting identifiable surveillance results because the number of results will be too low to be of significance. Such surveillance results will include both reactive (*e.g.,* complaints-based) and randomized surveillance results, which over time will establish a surveillance and conformity history of certified health IT.

Comments. Commenters generally agreed with the proposed list of information to be included in publicly available surveillance results (*i.e.,* the names of health IT developers; names of products and versions; certification criteria and Program requirements surveilled; and outcomes of surveillance). Several health IT developers suggested that the information listed for publication should be specifically limited to the information identified in the Proposed Rule, which should be a ''ceiling rather than a floor.'' Some commenters also recommended releasing the same type of surveillance results information that is required to be made public as part of CAPs under § 170.523(f)(1)(xxii). Commenters recommended this approach to ensure Program consistency, prevent interim work product or information obtained in the course of surveillance from being disclosed, and prevent the inclusion of proprietary or sensitive information.

Most commenters recommended ONC–ACBs provide summary identifiable surveillance results. Some commenters cautioned that ONC–ACBs should clearly indicate that surveillance of specific certified health IT should not imply a problem or potential problem with the health IT. One commenter encouraged ONC to share model forms of how results would be published so that a common understanding of the form, content, and structure is established in advance of their publication. The same commenter also recommended that we engage in outreach with industry, providers, health IT developers, and public interest stakeholders to help them understand and interpret public surveillance information.

Commenters expressed support for publishing hyperlinks on the ONC Web site to the quarterly identifiable surveillance results posted on the ONC–ACBs' Web sites. Several commenters also recommended posting the identifiable surveillance results on the CHPL, rather than having them spread across multiple ONC–ACB Web sites.

Response. Based on the comments received and the goals of our proposal, as stated above and in the Proposed Rule, we have finalized our proposed approach with the following clarifications. This approach requires the public posting of the information specified in the Proposed Rule (81 FR 11070–71) and the relevant information already required to be posted, when appropriate, on the CHPL as part of a CAP (80 FR 62725). Specifically, the information required to be reported for all surveillance results under this final rule will include: The names of health IT developers; names of products and versions; certification criteria and Program requirements surveilled; identification of the type of surveillance (*i.e.,* reactive or randomized); the dates surveillance was initiated and completed; and the number of sites that were used in randomized surveillance. This information is consistent with the proposed information, the types of information already required to be posted for CAPs (which is more information than we have specified above for quarterly reporting of all identifiable surveillance results), and with commenter feedback.

We did not specifically list the identification of the type of surveillance (*i.e.,* reactive or randomized), dates the surveillance was initiated and completed, or the number of sites surveilled as types of information to be reported in the Proposed Rule. However, the Proposed Rule refers to ''continued performance,'' which requires the identification of the dates surveillance was conducted in order to measure performance over a period of time. Additionally, we believe information regarding whether the surveillance was reactive or random and the number of sites that were surveilled will be useful to stakeholders in understanding surveillance results.

The Proposed Rule included the 'outcome of surveillance' as a specific type of information, but we have determined that it is unnecessary. We note that the outcome of surveillance is implied by definition (surveillance results). Furthermore, outcomes that include identifiable non-conforming surveillance results are already required to be posted on the CHPL.

We agree with commenters that requiring the surveillance information to be posted in one location will better serve stakeholders. Allowing ONC–ACBs to post identifiable surveillance results in different locations would create difficulties for stakeholders who would have to search all surveillance results across multiple ONC–ACBs' Web sites. Further, such an approach would not account for an ONC–ACB choosing to exit the Program. Alternatively, as commenters suggested, the CHPL would address these challenges and is consistent with our consideration in the Proposed Rule of having the hyperlinks on the ONC Web site as a means of providing stakeholders with a centralized and more readily available means for accessing the results. The CHPL is housed on the ONC Web site. The posting of surveillance results on the CHPL is responsive to commenter feedback and will prevent stakeholders from having to navigate multiple sites for the surveillance information. This approach will also decrease the burden for ONC–ACBs as they do not have to host and update the surveillance results on their own Web sites. To further reduce the burden for ONC–ACBs, we will also provide guidance to ONC–ACBs on how to most efficiently submit the information to the CHPL.

As suggested by comments and consistent with our goal of making identifiable surveillance results accessible and useful to customers and other stakeholders, we are modifying the CHPL. For example, we intend to include a disclaimer clearly indicating that the fact that surveillance was done does not imply a problem with the health IT. However, we note that conducting surveillance is a Program requirement and a required responsibility of an ONC–ACB and it may or may not be based on information indicating a potential problem with the certified health IT. We will make clear that a search of a particular product listed on the CHPL returning no surveillance results would mean that the product has never been surveilled. We also plan to provide other guidance as necessary, such as an explanation of the differences between reactive and random surveillance.[20]

Comments. Commenters expressed support for our proposal to not require the inclusion of certain information that is proprietary, trade secret, or confidential. One commenter stated, however, that it was unclear as to who decides what information is proprietary or a trade secret and suggested that it should be ONC's sole decision and the only reasonable grounds for exclusion should be threats to patient confidentiality. Another commenter expressed concerns that it was unclear how ONC can balance the needs of health IT developers to protect their proprietary information with the desire to provide meaningful information related to surveillance of health IT.

Response. We appreciate both the support and concerns raised by commenters. As discussed above, we have specified the types of surveillance results that must be submitted to the CHPL and made public. We do not believe that any of the required information would implicate the release of proprietary, trade secrets, or confidential information. Further, as noted in the Proposed Rule (81 FR 11063), we are confident that the concerns of commenters regarding the disclosure of proprietary or sensitive information will be adequately addressed through appropriate safeguards implemented at the discretion of ONC–ACBs. ONC–ACBs have already been directly and effectively submitting data to the CHPL on certified health IT. They have demonstrated the capability, working with health IT developers, to submit the requisite information while protecting health IT developers' proprietary, trade secret, and confidential information. We expect this will continue with the surveillance results information that must be disclosed as a result of this new requirement. For a more detailed discussion of the safeguards ONC will implement for proprietary information, trade secrets, or confidential information, please see section II.A.1.c.(1), ''Notice of Potential Non-Conformity or Non-Conformity,'' of this final rule.

Comments. The majority of commenters expressed support for the proposal that identifiable surveillance results be posted quarterly. One commenter encouraged us to set the quarterly timeframe as a minimum threshold and to consider the value of more frequent publication, such as monthly.

Response. We appreciate the comments in support of the proposed requirement that identifiable surveillance results be posted quarterly. We have adopted a quarterly posting requirement, as proposed, but with incorporation of the commenter's recommendation that quarterly posting be the minimum threshold. We believe that submission through the CHPL of the minimum set of data will support

[20] Program guidance can be found on the ONC Web site at *https://www.healthit.gov/policy-researchers-implementers/onc-health-it-certification-program-guidance.*

the efficient submission of the additional surveillance results and the submission of the results with other data on certified health IT that is required to be submitted more frequently. This will enable ONC–ACBs to submit identifiable surveillance results more frequently if they are available and ready for submission.

To provide sufficient time for implementation by ONC and the ONC–ACBs, including necessary revisions to the CHPL to support user-friendly display of the identifiable surveillance results, we anticipate that posting of the first identifiable surveillance results will occur by the end of the first quarter of 2017. This means the identifiable surveillance results for January through March of 2017 would be posted no later than in early April of 2017. As a reminder, certain identifiable non-conforming surveillance results are already submitted to the CHPL on a weekly basis (*see* § 170.523(f)). This requirement serves to provide consumers and end-users with prompt notification of non-conformities and corrective actions associated with certified health IT.

Comments. A few commenters expressed concern that the cost estimate for ONC–ACBs to post all identifiable surveillance results seemed too low, unless there is almost no change to what ONC–ACBs are already doing. The commenters asserted that the volume of updates would be significantly higher than currently required because it would include both conforming and non-conforming results.

Response. We appreciate the commenters' concerns. As discussed above, we believe that our adopted approach for making identifiable surveillance results public will be more efficient and less burdensome than proposed. We also refer readers to the ''Regulatory Impact Statement'' section of this final rule for our cost estimates for the reporting of identifiable surveillance results by ONC–ACBs.

Comments. A few commenters recommended that we include additional functionality on our Web site (CHPL) so that stakeholders may specifically learn how certified health IT products support interoperability. Commenters asserted that visible, comparative information will give health IT developers an opportunity to understand where performance can be improved to support providers electronically exchange health information.

Response. We appreciate the commenters' feedback and will consider the feedback as part of our efforts to support widespread interoperability and electronic health information exchange. While this comment is outside the scope of our proposal, we believe that the quarterly posting of identifiable surveillance results on the CHPL is consistent with the commenters' request. Further, the CHPL currently supports the searching and comparing of certified health IT based on certification criteria. For example, users can search certified health IT listed on the CHPL to determine which health IT is certified to the 2015 Edition ''transitions of care'' certification criterion (§ 170.315(b)(1)). This criterion and its included capabilities support interoperability.

Alignment of § 170.556(e)(1) With § 170.523(i)(2)

We proposed to revise § 170.556(e)(1) for clarity and consistency with § 170.523(i)(2) by adding that the ongoing submission of in-the-field surveillance results to the National Coordinator throughout the calendar year must, at a minimum, be done on a quarterly basis.

Comments. A few commenters suggested we adopt the same language in both § 170.523(i)(2) and § 170.556(e)(1), rather than saying both ''quarterly'' and ''rolling.''

Response. We agree with comments and have revised § 170.556(e)(1) to be consistent with § 170.523(i)(2) by stating that the results of in-the-field surveillance must be submitted to the National Coordinator, at a minimum, on a quarterly basis.

Annual Summative Report of Surveillance Results

We proposed to reestablish a requirement that ONC–ACBs submit an annual summative report of surveillance results to the National Coordinator. We noted in the Proposed Rule that this previous requirement was unintentionally removed in the 2015 Edition final rule when we established a quarterly reporting requirement for surveillance results.

Comments. One commenter stated that the annual summative report should function as a general overview of the surveillance activities and the quarterly report should contain more detailed findings.

Response. We appreciate the feedback on this proposal and have finalized it as proposed. We intend to provide, as necessary, more specific guidance to ONC–ACBs on submitting the annual summative surveillance report.

III. National Technology Transfer and Advancement Act and the Office of Management and Budget Circular A–119

The National Technology Transfer and Advancement Act (NTTAA) of 1995 (15 U.S.C. 3701 *et seq.*) and the Office of Management and Budget (OMB) Circular A–119 [21] require the use of, wherever practical, standards that are developed or adopted by voluntary consensus standards bodies to carry out policy objectives or activities, with certain exceptions. In the Proposed Rule, we proposed to ''adopt'' one voluntary consensus standard (ISO/IEC 17025) for use in the Program.

Comments. We received no comments on the ISO/IEC 17025 standard as it relates to the NTTAA and OMB Circular A–119.

Response. While we stated in the Proposed Rule that we proposed to ''adopt'' ISO/IEC 17025, we clarify that we were not proposing to adopt the standard under our authorities for the purposes of certifying health IT. Rather, consistent with the stated purpose of our proposal provided in the Proposed Rule, we have finalized the *use* of the ISO/IEC 17025 standard for the accreditation of testing laboratories in the Program. The use of this standard is consistent with the requirements of the NTTAA and OMB Circular A–119.

IV. Incorporation by Reference

The Office of the Federal Register has established requirements for materials (*e.g.,* standards and implementation specifications) that agencies incorporate by reference in the **Federal Register** (79 FR 66267; 1 CFR 51.5(b)). Specifically, § 51.5(b) requires agencies to discuss, in the preamble of a final rule, the ways that the materials they incorporate are reasonably available to interested parties and how interested parties can obtain the materials; and summarize, in the preamble of the final rule, the materials they incorporate by reference.

Anyone may purchase the standard and we provide a uniform resource locator (URL) for the standard. As required by § 51.5(b), we also provide a summary below of the standard we have adopted and incorporate by reference in the **Federal Register**.

ISO/IEC 17025:2005 General requirements for the competence of testing and calibration laboratories

URL: ISO/IEC 17025:2005 (ISO/IEC 17025) is available for purchase on the ISO Web site at: *http://www.iso.org/iso/catalogue_detail.htm?csnumber=39883.*

[21] *http://www.whitehouse.gov/omb/circulars_a119.*

Summary: Accreditation bodies that recognize the competence of testing and calibration laboratories should use ISO/IEC 17025 as the basis for their accreditation. Clause 4 specifies the requirements for sound management. Clause 5 specifies the requirements for technical competence for the type of tests and/or calibrations the laboratory undertakes.

The use of ISO/IEC 17025 will facilitate cooperation between laboratories and other bodies, and assist in the exchange of information and experience, and in the harmonization of standards and procedures.

Comments. We received one comment supporting our proposal to use and incorporate by reference the ISO/IEC 17025 standard.

Response. As noted under the NTTAA section above, we proposed to ''adopt'' ISO/IEC 17025. However, we clarify that we were not proposing to adopt the standard under our authorities for the purposes of certifying health IT. Rather, consistent with the stated purpose of our proposal provided in the Proposed Rule, we have finalized the *use* of the ISO/IEC 17025 standard for the accreditation of testing laboratories in the Program and have also incorporated by reference the standard in the **Federal Register**.

Address Change

We have updated the address for ONC in the ''incorporation by reference'' sections of the regulations at §§ 170.299(a) and 170.599(a) as ONC's address changed in 2015.

Reordering of § 170.599(b)

We have reordered the listing of standards in § 170.599(b). This reordering is consistent with the procedures of the Office of the Federal Register, which dictate that standards should be listed by the alphanumeric ID (excluding the date) for each standard, and then by the standard date.

V. Collection of Information Requirements

Under the Paperwork Reduction Act of 1995 (PRA), agencies are required to provide 60-day notice in the **Federal Register** and solicit public comment on a proposed collection of information before it is submitted to OMB for review and approval. In order to fairly evaluate whether an information collection should be approved by OMB, section 3506(c)(2)(A) of the PRA requires that we solicit comment on the following issues:

1. Whether the information collection is necessary and useful to carry out the proper functions of the agency;
2. The accuracy of the agency's estimate of the information collection burden;
3. The quality, utility, and clarity of the information to be collected; and
4. Recommendations to minimize the information collection burden on the affected public, including automated collection techniques.

We solicited comment on these issues in the Proposed Rule (81 FR 11071–11072) for the matters discussed in detail below.

A. ONC–AA and ONC–ACBs

Under the Program, accreditation organizations that wish to become the ONC-Approved Accreditor (ONC–AA) must submit certain information, organizations that wish to become an ONC–ACB must comply with collection and reporting requirements, and ONC–ACBs must comply with collection and reporting requirements, records retention requirements, and submit annual surveillance plans and annually report surveillance results. In the 2015 Edition proposed rule (80 FR 16894), we estimated fewer than ten annual respondents for all of the regulatory ''collection of information'' requirements that applied to the ONC–AA and ONC–ACBs, including those previously approved by OMB. In the 2015 Edition final rule (80 FR 62733), we concluded that the regulatory ''collection of information'' requirements for the ONC–AA and the ONC–ACBs were not subject to the PRA under 5 CFR 1320.3(c). We further note that the PRA (44 U.S.C. 3518(c)(1)(B)(ii)) exempts the information collections specified in 45 CFR 170.565 that apply to ONC–ACBs, which are collection activities that would occur during administrative actions or investigations involving ONC against an ONC–ACB.

Comments. We received no comments specific to the ONC–AA and ONC–ACBs regarding the ''collection of information'' requirements applicable to them or our past determinations.

Response. We continue to maintain our past determinations in that we estimate fewer than ten annual respondents for all of the regulatory ''collection of information'' requirements that apply to the ONC–AA and ONC–ACBs and that the ''collection of information'' requirements for the ONC–AA and the ONC–ACBs are not subject to the PRA under 5 CFR 1320.3(c). As previously noted, the PRA (44 U.S.C. 3518(c)(1)(B)(ii)) exempts the information collections specified in 45 CFR 170.565 that apply to ONC–ACBs, which are collection activities that would occur during administrative actions or investigations involving ONC against an ONC–ACB.

B. ONC–ATLs

In the Proposed Rule, we estimated fewer than ten annual respondents for all of the proposed regulatory ''collection of information'' requirements for ONC–ATLs under Part 170 of Title 45. As stated in the Proposed Rule, for this reason, the regulatory ''collection of information'' requirements for ONC–ATLs under the Program are not subject to the PRA under 5 CFR 1320.3(c). We further noted in the Proposed Rule that the PRA (44 U.S.C. 3518(c)(1)(B)(ii)) exempts the information collections specified in 45 CFR 170.565 that apply to ONC–ATLs, which are collection activities that would occur during administrative actions or investigations involving ONC against an ONC–ATL.

We explained in the Proposed Rule that since the establishment of the Program in 2010, there have never been more than six applicants or entities selected for ONC–ATCB or accredited testing lab status. We stated our expectations that there will be no more than eight ONC–ATLs participating in the Program, which included the five accredited testing labs currently operating under the Program and an estimated three more testing labs that may consider becoming accredited and seek ONC–ATL status because of our proposal to permit ONC–ATL status based on health IT testing accreditation to only one certification criterion or a partial certification criterion.

We requested comments on these conclusions and the supporting rationale on which they were based.

In the Proposed Rule, we specified that the ''collection of information'' requirements that apply to ONC–ATLs are found in § 170.520(b); proposed § 170.524(d) and (f); and § 170.540(c). We estimated the burden hours for these requirements in case our conclusions in the Proposed Rule were found to be misguided based on public comments or for other reasons and to seek comments on the burden hours as a means of informing our regulatory impact analysis (*see* section VI (''Regulatory Impact Statement'') of this preamble). The estimated total burden hours as specified in the Proposed Rule are expressed in Table 1 below. We explained in the Proposed Rule that the estimated total burden hours were based on an estimated eight respondents (ONC–ATLs) for the reasons noted above and in the Proposed Rule. With similar requirements to ONC–ACBs, we estimated the same number of burden hours for ONC–ATLs to comply with

§§ 170.520(b) and 170.540(c) as cited in the 2015 Edition proposed rule (80 FR 16894). In the Proposed Rule, we made the same determination for ONC–ATL records retention requirements under proposed § 170.524(f) as we did for the ONC–ACB records retention requirements (*i.e.,* no burden hours) (80 FR 16894). We also estimated two responses per year at one hour per response for ONC–ATLs to provide updated contact information to ONC per § 170.524(d).

TABLE 1—ESTIMATED ANNUALIZED TOTAL BURDEN HOURS

Type of respondent	Code of Federal Regulations section	Number of respondents	Number of responses per respondent	Average burden hours per response	Total burden hours
ONC–ATL	45 CFR 170.520(b)	8	1	1	8
ONC–ATL	45 CFR 170.524(d)	8	2	1	16
ONC–ATL	45 CFR 170.524(f)	8	n/a	n/a	n/a
ONC–ATL	45 CFR 170.540(c)	8	1	1	8
Total burden hours for all collections of information.					32

Comments. We received one comment from an accredited testing lab suggesting that we increase the burden hours for application submission and general updates of accreditation by a factor of four or more to more accurately reflect time spent by the ONC–ATL due to time spent internally by the organization preparing for the submission.

Response. We have accepted the commenter's suggestion and increased the burden hour estimates by a factor of four for relevant requirements as reflected in Table 2 below. The revised estimated costs of these requirements can be found in section VI (''Regulatory Impact Statement'') of this final rule.

TABLE 2—ESTIMATED ANNUALIZED TOTAL BURDEN HOURS

Type of respondent	Code of Federal Regulations section	Number of respondents	Number of responses per respondent	Average burden hours per response	Total burden hours
ONC–ATL	45 CFR 170.520(b)	8	1	4	32
ONC–ATL	45 CFR 170.524(d)	8	2	4	64
ONC–ATL	45 CFR 170.524(f)	8	n/a	n/a	n/a
ONC–ATL	45 CFR 170.540(c)	8	1	4	32
Total burden hours for all collections of information.					128

We continue to estimate fewer than ten annual respondents for all of the regulatory ''collection of information'' requirements for ONC–ATLs under Part 170 of Title 45. Accordingly, the ''collection of information'' requirements/burden that are associated with this final rule are not subject to the PRA under 5 CFR 1320.3(c). As noted in the Proposed Rule, the PRA (44 U.S.C. 3518(c)(1)(B)(ii)) exempts the information collections specified in 45 CFR 170.565 that apply to ONC–ATLs, which are collection activities that would occur during administrative actions or investigations involving ONC against an ONC–ATL.

C. Health IT Developers

We proposed in 45 CFR 170.580 that a health IT developer would have to submit certain information to ONC as part of a review of the health IT developer's certified health IT and if ONC took action against the certified health IT (*e.g.,* requiring a CAP to correct a non-conformity or suspending or terminating a certification for a Complete EHR or Health IT Module). However, we concluded in the Proposed Rule that the PRA exempts these information collections because 44 U.S.C. 3518(c)(1)(B)(ii) excludes collection activities during the conduct of administrative actions or investigations involving the agency against specific individuals or entities.

Comments. We received no comments specific to the ''collection of information'' requirements applicable to health IT developers and our PRA determination.

Response. We continue to maintain that the ''collection of information'' requirements for health IT developers that are associated with this final rule, including providing access to the health IT as clarified earlier in the preamble, are not subject to the PRA under 44 U.S.C. 3518(c)(1)(B)(ii), which excludes collection activities during the conduct of administrative actions or investigations involving the agency against specific individuals or entities.

VI. Regulatory Impact Statement

A. Statement of Need

While ONC-authorized certification bodies (ONC–ACBs) have been delegated authority to issue certifications for health IT on ONC's behalf under the ONC Health IT Certification Program (''Program''), they do not have responsibility to address the full range of requirements applicable to health IT certified under the Program, such as those that may pose a risk to public health or safety and are inconsistent with section 3001(b) of the PHSA. In addition, ONC–ACBs may be unable to effectively administer Program requirements in certain circumstances due to practical challenges. In contrast, ONC is well-positioned to review certified health IT against the full range of requirements under the Program. This final rule is being published to enhance Program oversight by providing a regulatory framework for ONC to directly review of health IT in certain circumstances and to take appropriate responsive actions to address potential non-conformities and non-conformities, including requiring the correction of non-conformities as determined by ONC in health IT certified under the Program and suspending and terminating certifications issued to Complete EHRs and Health IT Modules.

This final rule also sets forth processes for ONC to timely and directly address testing issues by enabling ONC to authorize and further oversee ONC-accredited testing laboratories (ONC–ATLs). These processes will serve to align the testing structure with ONC's authorization and oversight of ONC–ACBs. In addition, this final rule will increase the transparency and availability of information about certified health IT through the publication of identifiable surveillance results. The publication of identifiable surveillance results supports further accountability of health IT developers to their customers and users of certified health IT.

B. Alternatives Considered

We assessed alternatives to our proposed approaches (*i.e.,* ONC's direct review of certified health IT and the authorization and oversight of accredited testing labs (ONC–ATLs)). One alternative would have been to maintain the approach for the Program prior to this final rule in which ONC–ACBs had sole responsibility for issuing and administering certifications in accordance with ISO/IEC 17065, the PoPC for ONC–ACBs, and other requirements of the Program. This approach would also have left the testing structure as it existed before this final rule. A second alternative would have been for ONC to take further responsibility for the testing, certification, and ongoing conformity of health IT with Program requirements by making testing and certification determinations and/or reviewing all determinations made under the Program. We requested comments on our assessment of alternatives and any alternatives that we should also consider.

Comments. Some commenters stated that ONC direct review is unnecessary, while other commenters stated that review of certified health IT should be left to ONC–ACBs.

Response. As we stated in the Proposed Rule, we continue to believe that adopting either alternative approach would be misguided. The current approach, which relies on ONC–ACBs to review certified health IT and take necessary actions, does not provide a regulatory framework for addressing non-conformities in certified health IT that present a serious risk to public health or safety or that present issues described in § 170.580(a)(2)(ii). As stated in the Proposed Rule, we fully considered the Program structure when initially establishing the Program and have made appropriate modifications as the Program has evolved. These past considerations primarily focused on a market-driven approach for the Program with testing and certification conducted on behalf of ONC and with ONC retaining and establishing direct and indirect oversight over certain activities. We also noted in the Proposed Rule and in this final rule that ONC–ACBs play an integral role in the Program and have the necessary expertise and capacity to effectively administer specific Program requirements. Similarly, accredited testing labs also play an integral role in the Program's success through the testing of health IT.

ONC direct review will complement ONC–ACBs' roles under the Program and serve to address matters, for example, beyond their resources and expertise. ONC direct oversight of ONC–ATLs will ensure that, like with ONC–ACBs, testing labs are directly and immediately accountable to ONC for their performance across a variety of Program items that affect the testing of health IT. Overall, the provisions in this final rule serve to enhance the Program by providing more consistency and accountability for Program participants, which will provide greater confidence in certified health IT when it is implemented, maintained, and used. Accordingly, and for the reasons outlined in this final rule, maintaining the Program as it is currently structured is not acceptable. If we did not change the current testing structure, a lack of parity in ONC oversight for testing and certification would continue to exist. ONC direct oversight of ONC–ATLs will ensure that, like with ONC–ACBs, testing labs are directly and immediately accountable to ONC for their performance across a variety of Program items that affect the testing of health IT. For the reasons outlined throughout this final rule, and specifically detailed in section II.A.1, we do not believe that continuing the Program with a framework for only ONC–ACB surveillance of certified health IT is a viable option or alternative.

C. Overall Impact

We examined the impact of the final rule as required by Executive Order 12866 on Regulatory Planning and Review (September 30, 1993), Executive Order 13563 on Improving Regulation and Regulatory Review (February 2, 2011), the Regulatory Flexibility Act (5 U.S.C. 601 *et seq.*), section 202 of the Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1532), and Executive Order 13132 on Federalism (August 4, 1999).

1. Executive Orders 12866 and 13563—Regulatory Planning and Review Analysis

Executive Orders 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). A regulatory impact analysis (RIA) must be prepared for major rules with economically significant effects ($100 million or more in any one year). It has been determined that this final rule is an economically significant rule as the potential costs associated with this final rule could be greater than $100 million per year. Accordingly, we have prepared an RIA that to the best of our ability presents the costs and benefits of this final rule.

a. Costs

We have identified and estimated the potential monetary costs for health IT developers, ONC–ATLs, the federal government (*i.e.,* ONC), and health care providers as a result of this final rule. We have categorized and addressed costs as follows: (1) Costs for health IT developers to correct non-conformities as determined by ONC; (2) costs for ONC and health IT developers related to an ONC inquiry into certified health IT non-conformities and ONC direct review, including costs for the new ''proposed termination'' step; (3) costs for health IT developers and ONC associated with the appeal process following a suspension/termination of a Complete EHR's or Health IT Module's certification; (4) costs for health care providers to transition to another certified health IT product when the certification of a Complete EHR or Health IT Module that they currently use is terminated; (5) costs for ONC–ATLs and ONC associated with ONC–ATL accreditation, application, renewal, and reporting requirements; (6) costs for ONC–ATLs and ONC related to revoking ONC–ATL status; and (7) costs for ONC–ACBs to submit identifiable surveillance results to the CHPL. We also provide an overall annual monetary cost estimate for the final rule (*see* (8) Total Annual Cost Estimate). We note that we have rounded all estimates to the nearest dollar and all estimates are expressed in 2016 dollars.

Comments on the Proposed Rule

General

Comments. Commenters expressed concerns that the costs of direct review could flow downstream to health IT developers, health care providers, and ONC–ATLs.

Response. We appreciate commenters' concerns and agree that certain stakeholders may incur costs as a result of this final rule. We have, therefore, estimated the direct costs for health IT developers and ONC due to ONC actions stemming from direct review under the provisions of this final rule, such as the costs for health IT developers to respond to a notice of potential non-conformity or notice of non-conformity or to file an appeal of an ONC determination. We have also estimated the indirect costs for health care providers because these costs may arise if ONC were to terminate the certification of health IT being used by health care providers to participate in a program requiring the use of certified health IT. We note that we do not believe there are any costs for ONC–ATLs related to direct review conducted by ONC.

Costs for Health IT Developers To Correct Non-Conformities Identified by ONC

Comments. A commenter asserted that substantial costs should be attributed to the reassessment of health IT for current conformity and estimated it would take at least 400 hours to perform a gap and risk assessment per product.

Response. We stated in the Proposed Rule that some health IT developers may reassess their products for conformity. We also stated in the Proposed Rule (81 FR 11073–74) and maintain that health IT developers should always be ensuring that their products are safe and conducting conformity and safety assessments of their health IT as part of proper quality management. We are unable to project the number of assessments that would occur beyond what is observed under the existing regulatory and market structure. Therefore, we have not included these costs in our quantitative cost estimates.

Comments. Some commenters noted that, if ONC alleges non-conformities outside the scope of certification criteria or test procedures, there could be a significant burden for health IT developers to respond to investigations and to change their products.

Response. We thank commenters for their thoughtful comments on this aspect of our proposal. We refer readers to section II.A.1.a of this final rule for a detailed discussion of what constitutes a non-conformity. As discussed in more detail in section C.1.a.(1) of this regulatory impact statement, while there would likely be costs to correct a non-conformity found as a result of ONC direct review under the processes outlined in this final rule, it is difficult to project such instances and costs given unpredictability of non-conformity occurrences and the underlying need to correct non-conformities. We have, however, estimated the costs to ONC and health IT developers related to an ONC inquiry into certified health IT non-conformities and ONC direct review in section C.1.a.(2) of this RIA.

Costs for ONC and Health IT Developers Related to an ONC Inquiry Into Certified Health IT Non-Conformities and ONC Direct Review

Comments. Some commenters suggested that we underestimated the costs to health IT developers, both in terms of dollars and ''softer'' costs, such as negative pressure on innovation. Commenters suggested we estimate the costs for ONC investigations. Commenters also stated that there should be a cost associated with unsubstantiated allegations and complaints. Commenters noted that ONC staff may lack appropriate expertise to conduct investigations.

Response. We clarify that the estimates for the review of, and inquiry into, certified health IT includes investigations (*see* section C.1.a.(2) of this RIA). In consideration of comments and due to the potential complexity of such investigations, we have increased the high end of our estimated range of costs by doubling our original high-end estimate for health IT developers and ONC. The unsubstantiated allegations and complaints noted by the commenters are captured in our low-end range of cost estimates.

We appreciate commenters' concerns regarding whether ONC staff will have the expertise to conduct investigations. ONC is evaluating the expertise and capabilities of current ONC staff and, if necessary, will hire additional staff with the requisite expertise and capabilities. However, we have no basis for estimating these potential costs in this RIA. These potential staffing costs will be driven by the volume of ONC direct review situations and the volume of additional responsibilities of ONC staff.

Costs for Health IT Developers and ONC Associated With the Appeal Process Following a Suspension/Termination of a Complete EHR's or Health IT Module's Certification

Comments. A commenter stated that ONC's estimated costs for a health IT developer to provide required information to appeal a suspension or termination are conservative, and these tasks would require experienced personnel who possess a high degree of technical knowledge.

Response. We appreciate the commenter's concern, but maintain that our estimate is reasonable, particularly due to the wide range of hours calculated. We agree with the commenter that compiling information for an appeal will require experienced personnel with technical expertise and we accounted for this expertise by assuming that the expertise of the employee(s) needed to participate in the appeal would be equivalent to a GS–15, Step 1 federal employee.

Costs for Health Care Providers To Transition to Another Certified Health IT Product When the Certification of a Complete EHR or Health IT Module That They Currently Use Is Terminated

Comments. Commenters were concerned about the financial impact of this final rule on health care providers, specifically the downstream costs for providers to transition to another certified health IT product. Multiple commenters suggested that our estimated average cost per product per health care provider to implement a new certified health IT product of approximately $33,000 is too low. Commenters also noted that the health care provider will probably not get a refund from the health IT developer and will have to acquire and possibly install a new product. A commenter suggested that ONC should account for the costs of labor, retraining employees, and lost productivity, in addition to the licensing and implementation costs of a new product. Another commenter suggested that in addition to direct financial costs of transitioning to another certified health IT product, ONC should calculate the costs associated with errors and inefficiencies caused by the transition.

Response. We thank commenters for their thoughtful comments on our cost estimates, but have adopted these estimates as proposed. We agree with commenters that there may be costs associated with the labor, retraining of employees, lost productivity, and errors and inefficiencies caused by the transition, but we have been unable to identify reliable data upon which we could base or revise our cost estimates. The relationship between a provider and a health IT developer will be guided by relevant contracts and licenses. Transition costs will most likely be costs negotiated as part of the health IT transactions and will vary with respect to the complexity of the health IT system and the tear-down, data transfer, and implementation of the new system while still providing patient care. We discuss these relationships and the associated costs in more detail in section C.1.a.(4) of this RIA.

Costs for ONC–ATLs and ONC Associated With ONC–ATL Accreditation, Application, Renewal, and Reporting Requirements

Comments. A couple of commenters questioned why existing accredited testing labs would incur an $11,000 fee. One accredited testing lab stated that our ATL-specific cost estimates were reasonable.

Response. We have adopted the accreditation cost estimates as proposed. On-site assessments are required prior to initial accreditation, during the first renewal year, and every two years thereafter. As such, the current five accredited testing labs would incur the on-site assessment fee once during the initial three-year ONC–ATL authorization period. Based on our consultations with NIST, we estimate a full scope on-site assessment for all criteria required for accreditation will cost approximately $11,000. This is the estimate we have used to calculate the estimated burden. However, we note that these values are approximated and will vary depending on the agreements established between health IT developers and ONC–ATLs.

Comments. A couple of commenters suggested that ONC should reevaluate its method for estimating the applicant staff time necessary to prepare and participate in the full scope on-site assessment. Commenters opined that since ONC–ACBs have already gone through this assessment, there should be actual experience data from those ONC–ACBs that could provide a more reliable estimate.

Response. Based on information provided by ONC–ACBs, we have revised our estimate for the applicant staff time necessary to prepare and participate in the full scope on-site assessment from 200 hours to 130 hours. Accordingly, we have also revised our cost estimate for a limited scope on-site assessment to 65 hours, which is half the estimate for the full scope on-site assessment. Based on these adjusted estimates for staff time for a GS–15, Step 1 federal employee, we estimate the applicant staff cost for a full scope on-site assessment at $15,956 and the applicant staff cost for a limited scope on-site assessment at $7,978.

Comments. We received one comment from an accredited testing lab suggesting that we increase the burden hours for application submission and general updates of accreditation by a factor of four or more to more accurately reflect time spent by the ONC–ATL due to time spent internally by the organization preparing for the submission.

Response. We have accepted the commenter's suggestion and increased the burden hour estimates by a factor of four for the following requirements: (1) ONC–ATL application at 45 CFR 170.520(b); (2) reporting changes at 45 CFR 170.524(d); and (3) renewal at 45 CFR 170.540(c).

Comments. A couple of commenters noted that we estimated $55,623 as the annualized cost for the first accreditation/application and 3-year authorization and we estimated $84,372 as the annualized cost to renew accreditation, application, and authorization during the first three-year ONC–ATL authorization period. They were confused as to why a renewal cost would be higher than the cost for a new testing lab.

Response. We have revised these estimates as described below in the ''Costs to the Applicant/ONC–ATL'' section below. We also clarify that the proposed renewal cost per testing lab ($50,623) is lower than the cost for each new testing lab applicant ($55,623). The reason the annualized cost is higher for renewals than for new applicants is because we initially calculated for five renewals (there are currently five accredited testing labs) and three new applicants.

Costs for ONC–ACBs To Submit Identifiable Surveillance Results to the CHPL

Comments. A couple commenters suggested that the proposed cost estimate for ONC–ACBs posting identifiable surveillance results of $205 is too low. These commenters suggested that approximately six hours would be required.

Response. As discussed in section II.B of this final rule, ONC–ACBs will be required to report the following information for all surveillance results: The names of health IT developers; names of products and versions; certification criteria and Program requirements surveilled; identification of the type of surveillance (*i.e.,* reactive or random); the dates surveillance was initiated and completed; and the number of sites that were used in randomized surveillance. However, in order to reduce the burden on ONC–ACBs, ONC will post surveillance results on the CHPL. This is consistent with our consideration in the Proposed Rule of having the hyperlinks on the ONC Web site as a way of providing stakeholders with a more readily available means for accessing the results. ONC–ACBs will be required to submit the data into the CHPL directly, but will not be required to host and update the data on their own Web sites as proposed.

We estimate that submitting identifiable surveillance results on a quarterly basis will further limit the burden on ONC–ACBs, but acknowledge that the expanded scope and volume of surveillance information will require additional time to submit the results to the CHPL than the four hours proposed. Therefore, in response to comments, we estimate that it will take an employee 20 hours annually to report identifiable surveillance results to the CHPL.

Cost Estimates

The only changes to the cost estimates from the Proposed Rule are: (1) We doubled the high-end estimate for ONC staff time related to ONC's review and inquiry into certified health IT and health IT developer staff time associated with providing ONC with all requested records and documentation that ONC would use to make a suspension and/or termination determination, including for the new ''proposed termination'' step; (2) based on information provided by ONC–ACBs, we revised our estimate for the applicant staff time necessary to prepare and participate in a full and a limited scope on-site assessment; (3) based on public comments, we increased the burden hour estimates for ONC–ATLs by a factor of four from the estimates in the Proposed Rule for the requirements in 45 CFR 170.520(b) (ONC–ATL application), 45 CFR 170.524(d) (reporting changes to ONC), and 45 CFR 170.540(c) (ONC–ATL status renewal); and (4) we added cost estimates for ONC–ACBs to report identifiable surveillance results to the CHPL.

We made employee assumptions about the level of expertise needed to complete the requirements in this section of the final rule. We correlated that expertise with the corresponding grade and step of an employee classified under the General Schedule Federal Salary Classification, relying on the associated employee hourly rates for the Washington, DC locality pay area as published by the Office of Personnel Management. We assumed that an applicant expends one hundred percent (100%) of an employee's hourly wage on benefits and overhead for the employee. Therefore, we doubled the employee's hourly wage to account for benefits. We concluded that a 100% expenditure on benefits is an appropriate estimate based on research conducted by HHS.

We used the General Schedule Federal Salary Classification for private sector employee wage calculations because the majority of the tasks and requirements that would be performed by private sector employees do not easily fall within a particular occupational classification identified by the Bureau of Labor Statistics (BLS). For instance, while we estimated costs for specialized testing lab personnel to support accreditation, we also estimated costs for participating in administrative reviews and appeals and reporting certain information to ONC. As noted above, in all instances, we correlated the expertise needed to complete the task or requirement with the corresponding grade and step of a federal employee classified under the General Schedule Federal Salary Classification.

(1) Costs for Health IT Developers To Correct Non-Conformities Identified by ONC

We acknowledged in the Proposed Rule that this rulemaking may: (1) Lead health IT developers to reassess whether their certified health IT is conforming; and (2) require health IT developers to correct non-conformities found by ONC in their certified health IT. We also stated in the Proposed Rule that the costs to perform either of the above would be determined on a case-by-case basis, likely vary significantly based on various factors, and that we did not have reliable information on which to base costs estimates for these activities (81 FR 11074). We seek to clarify that these statements were made to provide a comprehensive view of all potential costs. However, estimating the prevalence of entities incurring these potential costs that would be attributable to this final rule presents a substantial challenge. There are no new certification requirements in this final rule and health IT developers have already been certified to applicable certification criteria and other Program requirements. Independent of this final rule, health IT developers should still be ensuring that their products are safe and conducting conformity and safety assessments of their health IT as part of proper quality management. These activities are typically a regular cost of doing business to ensure that their certified health IT is not, for example, creating public health and/or safety issues by causing medical errors (*see* 81 FR 11073–74). If ONC identifies/finds a non-conformity with a certified capability under the direct review processes outlined in this final rule, then the costs to correct the non-conformity are a result of this final rule. However, due to the difficulty of projecting such instances given the underlying need to correct non-conformities, we have not been able to include these costs in our quantitative cost estimates.

(2) Costs for ONC and Health IT Developers Related to an ONC Inquiry Into Certified Health IT Non-Conformities and ONC Direct Review

ONC has broad discretion to review certified health IT. However, we anticipate that such direct review will be relatively infrequent and will focus on situations that pose a risk to public health or safety. We estimate that a health IT developer may commit, on average and depending on complexity, between 80 and 800 hours of staff time to provide ONC with all requested records, access to the technology as needed, and documentation that ONC would use to conduct the fact-finding, make a non-conformity determination, approve a CAP, and make a suspension and/or termination determination, including the new ''proposed termination'' step. We assumed that the expertise of the employee(s) needed to comply with ONC's requests would be equivalent to a GS–15, Step 1 federal employee. The hourly wage with benefits for a GS–15, Step 1 employee located in Washington, DC is approximately $122.74. Therefore, we estimate the cost for a health IT developer to cooperate with an ONC review and inquiry into certified health IT will, on average, range from $9,819 to $98,192. We note that some health IT developers' costs are expected to be less and some health IT developers' costs are expected to be more than this estimated cost range.

In comparison, the BLS average hourly wage for a nonsupervisory employee under the North American Industry Classification System (NAICS) 541511, ''Custom Computer Programming Services,'' is $42.67.[22] We assumed that, just as with the General Schedule Federal Salary Classification, an applicant expends one hundred percent (100%) of an employee's hourly wage on benefits for the employee. Therefore, we doubled the employee's hourly wage to account for benefits, bringing the average hourly wage with benefits to $85.34. Accordingly, the BLS estimated wages for a health IT developer to cooperate with an ONC review and inquiry into certified health IT will, on average, range from $6,827 to $68,272, which is considerably lower than the General Schedule Federal Salary Classification estimates. We estimate that ONC may commit, on average and depending on complexity, between 20 and 1,200 hours of staff time to complete a review and inquiry into certified health IT. We assumed that the expertise of a GS–15, Step 1 federal employee(s) will be necessary. Therefore, we estimate the cost for ONC to review and conduct an inquiry into certified health IT will, on average, range from $2,455 to $147,288. We note that some reviews and inquiries may cost less and some may cost more than this estimated cost range.

(3) Costs for Health IT Developers and ONC Associated With the Appeal Process Following a Suspension/Termination of a Complete EHR's or Health IT Module's Certification

As discussed in section II.A.1.c.(5) of this final rule's preamble, § 170.580(g) permits a health IT developer to appeal an ONC determination to suspend or terminate a certification issued to a Complete EHR or Health IT Module. We estimate that a health IT developer may commit, on average and depending on complexity, between 80 to 240 hours of staff time to provide the required information to appeal a suspension or termination and respond to any requests from the hearing officer. We assumed that the expertise of the employee(s) needed to participate in the appeal would be equivalent to a GS–15, Step 1 federal employee. The hourly wage with benefits for a GS–15, Step 1 employee located in Washington, DC is approximately $122.74. Therefore, we estimate the cost for a health IT developer to appeal a suspension or termination will, on average, range from $9,819 to $29,458. We note that some health IT developers' costs are expected to be less and some health IT developers' costs are expected to be more than this estimated cost range. In comparison, the BLS average hourly wage with benefits is $85.34. Therefore, the cost for a health IT developer to appeal a suspension or termination using BLS wages will, on average, range from $6,827 to $20,482.

We estimate that ONC would commit, on average and depending on complexity, between 200 and 800 hours of staff time to conduct an appeal. This would include the time to represent ONC in the appeal and support the costs

[22] *See http://beta.bls.gov/dataViewer/view/timeseries/CEU6054151108.*

for the hearing officer. We assumed that the expertise of a GS–15, Step 1 federal employee(s) will be necessary. Therefore, we estimate the cost for ONC to conduct an appeal will, on average, range from $24,548 to $98,192. We note that some appeals may cost less and some may cost more than this estimated cost range.

(4) Costs for Health Care Providers To Transition to Another Certified Health IT Product When the Certification of a Complete EHR or Health IT Module That They Currently Use Is Terminated

This cost analysis with regards to health care providers focuses on the direct effects of the termination of a Complete EHR's or Health IT Module's certification under this final rule's provisions as a certification termination would have the greatest potential impact. We note and emphasize that the estimated costs for health care providers as a result of a certification termination could be incurred absent the provisions in this final rule. ONC–ACBs currently have the authority to terminate (and suspend) the certifications of Complete EHRs and Health IT Modules. In this regard, ONC–ACBs have terminated certifications for both Complete EHRs and Health IT Modules.

The most recent termination of a certification by an ONC–ACB occurred in June 2016 when a health IT developer failed to submit a CAP related to transparency requirements. No eligible professionals (EPs) attested under the Medicare EHR Incentive Program to using this certified health IT product. Another termination by an ONC–ACB occurred in September 2015 when the certifications of a health IT developer's Complete EHRs and Health IT Modules were terminated for failure to respond and participate in routine surveillance requests.[23] Only 48 eligible professionals attested under the Medicare EHR Incentive Program to using these certified health IT products. In April 2013, an ONC–ACB terminated the certifications of Complete EHRs and Health IT Modules because they did not meet the required functionality.[24] Those certified health IT products had no Medicare attestations. Considering that these are the only terminations and impacts over the five years of the Program and consistent with our stated intent to work with health IT developers to correct non-conformities found in their certified health IT under the provisions in this final rule, we maintain that it is highly unlikely that the high end of our estimated costs for health care providers will ever be realized.

We estimate the monetary costs that will be sustained by health care providers to transition to another certified health IT product when the certification of a Complete EHR or Health IT Module that they currently use is terminated. We anticipate that health care providers impacted by certification termination will transition to a new certified health IT product due to eventually needing certified health IT to participate in other HHS programs requiring the use of certified health IT (*e.g.,* the EHR Incentive Programs[25]). We calculated the estimated upfront cost for health care providers using the number of known EPs that report under the Medicare EHR Incentive Program using certified Complete EHRs and certified Health IT Modules that would have their certifications terminated multiplied by an estimated average cost per product per provider to implement a new certified health IT product. The estimated average cost per product per provider to implement a new certified health IT product is approximately $33,000. This estimate is consistent with other analyses on average costs.[26]

This analysis and cost estimates does not include sunk costs during the transition year, such as ongoing maintenance for the health IT product that had its certification(s) terminated and any upfront costs the provider paid for the health IT product. The transition by a health care provider to a new certified health IT product could also include non-sunk costs associated with unwinding contractual matters and technological connectivity, replacement/implementation efforts, training of workforce, and the potential for an operational shut down to effectuate a transition to a replacement technology. In regard to contractual matters, we acknowledge that transitioning to a new certified health IT product following a certification termination may be further complicated by the fact that health care providers may have entered multi-year transactions for a Complete EHR or Health IT Module(s). These costs would likely vary significantly based on the contract and specific situation. Conversely, unlike the cost categories just mentioned, which would tend to make our estimates understate the costs to providers due to a termination of certification, some aspects of certified health IT implementation may be similar across products, thus reducing the costs of transitioning to a new product below the costs incurred in association with the original implementation.

We used the following formula to calculate the estimated upfront costs for health care providers to transition to a new product:

1. Number of EPs reporting with a certified Complete EHR or certified Health IT Module that could potentially have its certification terminated
2. #1 multiplied by the average upfront cost per product per health care provider
3. Result of #2 equals the estimated cost for health care providers to replace the certified Complete EHR or certified Health IT Module

Applying this formula, we calculated the upper and lower threshold impacts as well as the median and mean impacts of terminating certifications issued to a Complete EHR or Health IT Module(s). We calculated the upper and lower thresholds from the certified Complete EHR and certified Health IT Modules with the greatest and least number of reported attestations to the Medicare EHR Incentive Program, respectively.[27] The median and mean impacts also were calculated using the number of reported attestations for each product (*see* table 3 (Cost Impact to Health Care Providers)). We calculated the estimated cost to those health care providers assuming all the health care providers would transition to a new certified health IT product.

[23] *http://www.hhs.gov/news/press/2015pres/09/20150902c.html.*

[24] *http://www.hhs.gov/about/news/2013/04/25/certification-for-electronic-health-record-product-revoked.html.*

[25] For health care provider guidance regarding circumstances and options when the health IT they are using to participate in the EHR Incentive Programs has its certification terminated or withdrawn, please see CMS EHR Incentive Programs FAQ 12657: *https://questions.cms.gov/faq.php?isDept=0&search=decertified&searchType=keyword&submitSearch=1&id=5005.*

[26] A Health Affairs study (*http://content.healthaffairs.org/content/30/3/481.abstract*) estimated the average cost for EHR implementation at a five-physician practice as $162,000. Dividing by five, the estimated cost per physician is $32,400, which is close to our estimated cost of $33,000 to implement an in-office health IT product.

[27] As of November 30, 2015.

TABLE 3—COST IMPACT TO HEALTH CARE PROVIDERS

	Lower	Median	Mean	Upper
Number of EP Attestations	1	24	190	19,692
Calculated Cost	$33,000	$792,000	$6,270,000	$649,836,000

We estimate the cost impact of certification termination on health care providers will range from $33,000 to $649,836,000 with a median cost of $792,000 and a mean cost of $6,270,000.

(5) Costs to ONC–ATLs and ONC Associated With ONC–ATL Accreditation, Application, Renewal, and Reporting Requirements

Costs to the Applicant/ONC–ATL

An applicant for ONC–ATL status will be required to submit an application and must be accredited in order to be a qualified ONC–ATL applicant. We estimate there will be between five and eight applicants, five of which are already accredited by NVLAP to ISO/IEC 17025 and up to three new applicants. Any new applicants for ONC–ATL status under the Program will first be required to become accredited by NVLAP to ISO/IEC 17025.

We note in section V (''Collection of Information Requirements'') of this final rule that we have increased the burden hour estimates by a factor of four from the estimates in the Proposed Rule for requirements in 45 CFR 170.520(b) (ONC–ATL application), 45 CFR 170.524(d) (reporting changes to ONC), and 45 CFR 170.540(c) (ONC–ATL status renewal). As such, the following cost estimates reflect the associated increase in burden hour estimates.

Based on our consultations with NIST, we estimate that it will take approximately 2–5 days for NVLAP to complete a full scope on-site assessment for all criteria required for accreditation at an approximate cost of $11,000. The on-site assessment fee covers the costs incurred by the assessors conducting the on-site assessment such as preparation time, time on-site, and travel costs (*e.g.* flights, hotel, meals, etc.). Section 170.511 will permit the authorization of ONC–ATLs for testing to one or even a partial certification criterion. Based on our consultations with NIST, this will take at least one day to complete and may reduce the necessary scope and cost of the on-site assessment to approximately $8,000. The current five accredited testing labs will each incur the full scope on-site assessment fee of $11,000, as discussed below. We anticipate the potential three new applicants will each incur a limited scope on-site assessment fee of $8,000, as discussed below.

Based on information provided by ONC–ACBs, we estimate the applicant staff time necessary to prepare and participate in the full scope on-site assessment at 130 hours. We estimate the applicant staff time necessary to prepare and participate in the limited scope on-site assessment at 65 hours, which is half the estimate for the full scope on-site assessment. We anticipate that an employee equivalent to a GS–15, Step 1 federal employee will be responsible for preparation and participation in the accreditation assessment. The hourly wage with benefits for a GS–15, Step 1 employee located in Washington, DC is approximately $122.74. Therefore, we estimate the applicant staff cost for the full scope on-site assessment at $15,956 and the applicant staff cost for the limited scope on-site assessment at $7,978.

In comparison, the BLS average hourly wage for a ''Computer and Information Analyst'' under NAICS 541380, Testing Laboratories, is $43.54.[28] The average hourly wage is $87.08 with the inclusion of benefits. Therefore, the BLS estimate for applicant staff cost for the full scope on-site assessment is $17,416 and the BLS estimate for applicant staff cost for the limited scope on-site assessment is $8,708. We emphasize that the problem with using the BLS information for the ATL classifications and wage estimates is that ONC–ATL duties do not easily fall within a particular occupational classification. For instance, there is not a singular occupational classification under NAICS 541380, Testing Laboratories, that would accurately capture the various tasks performed by ONC–ATLs in the processes described in this final rule. Thus, we used a broad occupation category, ''Computer and Information Analysts,'' for this estimate.

We anticipate that ONC–ATLs will incur an estimated $5,000 accreditation administrative/technical support fee each year during the three-year ONC–ATL authorization period.[29] The accreditation administrative/technical support fee covers costs associated with NVLAP staff under the Program. On-site assessments are required prior to initial accreditation, during the first renewal year, and every two years thereafter. As such, we expect the potential three new applicants will each incur the on-site assessment fee twice during their initial three-year ONC–ATL authorization period and the current five accredited testing labs will incur the on-site assessment fee once during the same period. Further, as stated above, we estimate that each full scope on-site assessment for all criteria will cost approximately $11,000 and each limited scope on-site assessment will cost approximately $8,000. We estimate that staff expertise and cost for renewal is likely to remain consistent at approximately $15,956 for a full scope on-site assessment and $7,978 for a limited scope on-site assessment. We expect that each ONC–ATL will renew its status, meaning it will request reauthorization from ONC to be an ONC–ATL, every three years.

After becoming accredited by NVLAP, an applicant for ONC–ATL status will incur minimal costs to prepare and submit an application to the National Coordinator. We estimate that it will take 40 minutes to provide the general information requested in the application, 120 minutes to assemble the information necessary to provide documentation of accreditation by NVLAP, and 80 minutes to review and agree to the PoPC for ONC–ATLs. We note that these time estimates are also accurate for an ONC–ATL to complete the proposed status renewal process. Based on our consultations with NIST, we estimate that an employee equivalent to a GS–9, Step 1 federal employee could provide the required general identifying information and documentation of accreditation status. The hourly wage with benefits for a GS–9, Step 1 federal employee located in Washington, DC is approximately $51.20. We estimate that an employee equivalent to a GS–15, Step 1 federal employee would be responsible for reviewing and agreeing to the PoPC for ONC–ATLs. Therefore, our cost estimate per ONC–ATL for these activities is $300. In comparison, the BLS cost estimate for one hour of work with

[28] *See http://www.bls.gov/oes/current/naics5_541380.htm#15-0000.*

[29] *See* NVLAP Fee Structure, *http://www.nist.gov/nvlap/nvlap-fee-policy.cfm.*

benefits by a ''Computer and Information Analyst'' is $348.

Overall, we estimate the total cost of ONC–ATL accreditation, application, and the first proposed three-year authorization period will be approximately $53,128 and the total cost for up to three new applicants will be approximately $159,384. We assume that ONC–ATLs will remain accredited during the three-year ONC–ATL authorization period.

We estimate the total cost for an ONC–ATL to renew its accreditation, application, and authorization during the first three-year ONC–ATL authorization period to be approximately $48,832 and the total renewal cost for all five current ONC–ATLs to be approximately $219,160. Based on our cost estimate timeframe of three years, we estimate the annualized renewal cost to be approximately $73,053.

We explain in § 170.524(d) that ONC–ATLs shall report various changes to their organization within 15 days. We estimate an employee equivalent to the Federal Salary Classification of GS–9, Step 1 could complete the transmissions of the requested information to ONC. As specified in section VI.B of this final rule, we estimate two responses per year at four hours per response for ONC–ATLs to provide updated information to ONC per § 170.524(d). Accordingly, we estimate it will cost each ONC–ATL $409.60 annually to meet this requirement. To estimate the highest possible cost, we assumed that the eight applicants we estimate will apply to become ONC–ATLs will become ONC–ATLs. Therefore, we estimate the total annual cost for ONC–ATLs to meet the requirements of proposed § 170.524(d) to be $3,276. In comparison, using the BLS wages, we estimate the total annual cost for ONC–ATLs to meet the requirements of proposed § 170.524(d) to be $5,573.

We explain in § 170.524(f) that ONC–ATLs shall retain all records related to the testing of Complete EHRs and Health IT Modules to an edition of certification criteria for a minimum of three years from the effective date that removed the applicable edition from the Code of Federal Regulations. Based on our consultations with NIST, we concluded that this time period is in line with common industry practices. Consequently, it does not represent an additional cost to ONC–ATLs.

Costs to ONC

We estimate the cost to develop the ONC–ATL application to be $522 based on the five hours of work we believe it would take a GS–14, Step 1 federal employee to develop an application form. The hourly wage with benefits for a GS–14, Step 1 employee located in Washington, DC is approximately $104.34. We also anticipate that there will be costs associated with reviewing applications under the Program. We expect that a GS–15, Step 1 federal employee will review the applications and ONC (or a designated representative) will issue final decisions on all applications. We anticipate that it will take approximately 20 hours to review and reach a final decision on each application. This estimate assumes a satisfactory application (*i.e.,* no formal deficiency notifications) and includes the time necessary to verify the information in each application and prepare a briefing for the National Coordinator. We estimate the cost for the application review process to be $2,455. As a result, we estimate ONC's overall cost of administering the entire application process to be approximately $2,977. Based on our cost estimate timeframe of three years, we estimate the annualized cost to ONC to be $992. These costs will be the same for a new applicant or ONC–ATL renewal.

As discussed in this final rule's preamble, we will also post the names of applicants granted ONC–ATL status on our Web site. We note that there will be minimal cost associated with this action and estimate the potential cost for posting and maintaining the information on our Web site to be approximately $446 annually. This amount is based on a maximum of six hours of work for a GS–12, Step 1 federal employee. The hourly wage with benefits for a GS–12 Step 1 federal employee located in Washington, DC is $74.

We note that there will be minimal cost associated with recording and maintaining updates and changes reported by the ONC–ATLs. We estimate an annual cost to the federal government of $743. This amount is based on ten hours of yearly work of a GS–12, Step 1 federal employee.

(6) Costs for ONC–ATLs and ONC Related To Revoking ONC–ATL Status

Costs to the ONC–ATL

We have revised § 170.565 to apply the same process for ONC–ATL status revocation as applies to ONC–ACBs. We estimate that an ONC–ATL may commit, on average and depending on complexity, between 20 and 160 hours of staff time to provide responses and information requested by ONC. We assume that the expertise of the employee(s) needed to comply with ONC's requests will be equivalent to a GS–15, Step 1 federal employee. The hourly wage with benefits for a GS–15, Step 1 employee located in Washington, DC, is approximately $122.74. Therefore, we estimate the cost for an ONC–ATL to comply with ONC requests per § 170.565 will, on average, range from $2,455 to $19,638. In comparison, the BLS cost estimate for a ''Computer and Information Analyst'' would, on average, range from $1,742 to $13,933. We note that in some instances the costs may be less and in other instances the costs may exceed this estimated cost range.

Costs to ONC

We estimate that ONC would commit, on average and depending on complexity, between 40 and 320 hours of staff time to conducting actions under § 170.565 related to ONC–ATLs. We assume that the expertise of a GS–15, Step 1 federal employee(s) would be necessary. Therefore, we estimate the cost for ONC would, on average, range from $4,910 to $39,277. We note that in some instances the costs may be less and in other instances the costs may exceed this estimated cost range.

(7) Costs for ONC–ACBs To Submit Identifiable Surveillance Results to the CHPL

In this final rule, we require ONC–ACBs to submit identifiable surveillance results to the CHPL quarterly. We estimate that it will take an employee 20 hours annually to submit these identifiable surveillance results quarterly to the CHPL. The hourly wage with benefits for a GS–9, Step 1 federal employee located in Washington, DC, is approximately $51.20. Therefore, we estimate the annual cost for each ONC–ACB to report surveillance results to be $1,024 and the total cost for all three ONC–ACBs to be $3,072. In comparison, the average hourly wage with benefits for a ''Computer Support Specialist'' under NAICS 541380, Testing Laboratories, is $55.90.[30] Therefore, the BLS estimate for the annual cost for each ONC–ACB to report identifiable surveillance results quarterly is $1,118 and the total cost for all three ONC–ACBs is $3,354.

We note that ONC may incur a cost for hosting the CHPL, but we have not estimated this cost because ONC already hosts the CHPL and any additional cost associated with this final rule is nominal. Similarly, we note that ONC may incur a cost for updating the CHPL due to the new requirements in this final rule, but we have not estimated

[30] *http://www.bls.gov/oes/current/naics5_541380.htm#15-0000.*

these costs because the CHPL has already been updated for the current posting of non-conforming findings and CAPs. As such, any additional cost associated with this final rule will be nominal.

(8) Total Annual Cost Estimate

We estimate the overall annual cost for this final rule, based on the cost estimates outlined above, will range from $171,011 to $650,352,050 with an average annual cost of $6,597,033.

b. Benefits

The final rule's provisions for ONC direct review of certified health IT will promote health IT developers' accountability for the performance, reliability, and safety of certified health IT; and facilitate the use of safer and more reliable health IT by health care providers and patients. Specifically, ONC's direct review of certified health IT will facilitate ONC's assessment of non-conformities and ability to require comprehensive corrective actions for health IT developers to address non-conformities determined by ONC, including notifying affected customers. We emphasize that our first and foremost goal is to work with health IT developers to remedy any non-conformities with certified health IT in a timely manner and across all customers. If ONC ultimately suspends and/or terminates a certification issued to a Complete EHR or Health IT Module under the provisions in this final rule, such action will serve to protect the integrity of the Program and users of health IT. While we do not have available means to quantify the benefits of ONC direct review of certified health IT, we note that ONC direct review supports and enables the National Coordinator to fulfill his or her responsibilities under the HITECH Act, instills public confidence in the Program, and protects public health and safety.

This final rule's provisions will provide other benefits as well. The provisions for ONC to authorize and oversee testing labs (ONC–ATLs) will facilitate further public confidence in testing and certification by facilitating ONC's ability to timely and directly address testing issues for health IT. The public availability of identifiable surveillance results will enhance transparency and the accountability of health IT developers to their customers. We note that this will provide customers and users of certified health IT with valuable information about the continued conformity of certified health IT. Further, the public availability of identifiable surveillance results will likely benefit health IT developers by providing a more complete context of surveillance in the health IT industry and illuminating good performance and the continued conformity of certified health IT with Program requirements. Again, while we do not have available means to quantify these benefits, we maintain that these approaches will improve Program conformity and compliance as well as further public confidence in certified health IT.

We note that we do not have data to establish how often we will need to exercise direct review, the extent of existing and future non-conformities, and the likely outcomes of ONC review, including up to preventing the loss of life. We also note that we do not have data to establish that the provisions for direct oversight of testing labs and the public availability of identifiable surveillance results would actually result in greater public confidence in certified health IT and increased adoption of certified health IT.

c. Accounting Statement and Table

When a rule is considered an economically significant rule under Executive Order 12866, we are required to develop an accounting statement indicating the classification of the expenditures associated with the provisions of this final rule. Monetary annualized benefits are presented as discounted flows using 3 percent and 7 percent factors in table 4 below. We are not able to explicitly define the universe of all costs, but have provided an average of likely costs of this final rule as well as a high and low range of likely costs. This final rule requires no federal annualized monetized transfers.

TABLE 4—ACCOUNTING STATEMENT

							Source
BENEFITS							
Qualitative, but not monetized	Expected qualitative benefits include: health IT developer accountability for the performance, reliability, and safety of certified health IT; the use of safer and more reliable health IT by health care providers and patients; and further public confidence in testing and certification.						RIA
COSTS							
Annualized monetized costs	Year dollar	Estimates (in millions)			Unit discount rate	Period covered	
		Low	Mean	High			
	2015	.17	6.60	650.35	7%	One year	RIA
		.17	6.60	650.35	3%		
TRANSFERS							
From Whom To Whom?	N/A						

2. Regulatory Flexibility Act

The Regulatory Flexibility Act (RFA) requires agencies to analyze options for regulatory relief of small businesses if a rule has a significant impact on a substantial number of small entities. The Small Business Administration (SBA) establishes the size of small businesses for federal government programs based on average annual receipts or the average employment of a firm.[31] The entities that are likely to be

[31] The SBA references that annual receipts means ''total income'' (or in the case of a sole proprietorship, ''gross income'') plus ''cost of goods sold'' as these terms are defined and reported on Internal Revenue Service tax return forms.

directly affected by this final rule are applicants for ONC–ATL status and health IT developers.

We estimate up to eight applicants for ONC–ATL status. These applicants are classified under the North American Industry Classification System (NAICS) codes 541380 (Testing Laboratories) specified at 13 CFR 121.201 where the SBA publishes ''Small Business Size Standards by NAICS Industry.'' [32] The SBA size standard associated with this NAICS code is set at $15 million annual receipts or less. As specified in section VI.C.(5) of this final rule's preamble, we estimate minimal costs for applicants for ONC–ATL status to apply and participate in the Program as ONC–ATLs. We have finalized the minimum amount of requirements necessary to accomplish our goal of enhanced oversight of testing under the Program. As discussed in section VI.B of this final rule, we emphasize that there are also no appropriate regulatory or non-regulatory alternatives that could be developed to lessen the compliance burden associated with this final rule. We further note that we expect all of the estimated costs to be recouped by those applicants that become ONC–ATLs through the fees they charge for testing health IT under the Program.

While health IT developers that pursue certification of their health IT under the Program represent a small segment of the overall information technology industry, we believe that many health IT developers impacted by this final rule most likely fall under NAICS code 541511 ''Custom Computer Programming Services.'' [33] The SBA size standard associated with this NAICS code is set at $27.5 million annual receipts or less. There is enough data generally available to establish that between 75% and 90% of entities that are categorized under NAICS code 541511 are under the SBA size standard. We also note that with the exception of aggregate business information available through the U.S. Census Bureau and the SBA related to NAICS code 541511, it appears that many health IT developers that pursue certification of their health IT under the Program are privately held or owned and do not regularly, if at all, make their specific annual receipts publicly available. As a result, it has been difficult to locate empirical data related to many of these health IT developers to correlate to the SBA size standard. However, although not perfectly correlated to the size standard for NAICS code 541511, we do have information indicating that over 60% of health IT developers that have had Complete EHRs and/or Health IT Modules certified to the 2011 Edition have less than 51 employees.

We estimate that this final rule will have effects on health IT developers, some of which may be small entities, that have certified health IT or are likely to pursue certification of their health IT under the Program. This is because health IT developers may need to reassess their health IT to verify conformity with the Program requirements outlined in this final rule and they may have their certified health IT subjected to corrective action, suspension, and/or termination under the provisions of this final rule. We have, however, finalized the minimum amount of requirements necessary to accomplish our primary policy goals of enhancing Program oversight and health IT developer accountability for the performance, reliability, and safety of certified health IT. Further, as discussed in section VI.B of this final rule, there are no appropriate regulatory or non-regulatory alternatives that could be developed to lessen the compliance burden associated with this final rule.

We do not believe that this final rule will create a significant impact on a substantial number of small entities. Additionally, the Secretary certifies that this final rule will not have a significant impact on a substantial number of small entities.

3. Executive Order 13132—Federalism

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a proposed rule (and subsequent final rule) that imposes substantial direct requirement costs on state and local governments, preempts state law, or otherwise has federalism implications. Nothing in this final rule imposes substantial direct compliance costs on state and local governments, preempts state law, or otherwise has federalism implications. We are not aware of any state laws or regulations that are contradicted or impeded by any of the provisions in this final rule.

4. Unfunded Mandates Reform Act of 1995

Section 202 of the Unfunded Mandates Reform Act of 1995 requires that agencies assess anticipated costs and benefits before issuing any rule that imposes unfunded mandates on state, local, and tribal governments or the private sector requiring spending in any one year of $100 million in 1995 dollars, updated annually for inflation. The current inflation-adjusted statutory threshold is approximately $144 million. While our estimated potential cost effects of this final rule reach the statutory threshold, we do not believe this final rule imposes unfunded mandates on state, local, and tribal governments or the private sector. We estimate the *potential* monetary costs for the private sector (health IT developers and health care providers) and note that the costs will be the result of a health IT developer not maintaining its certified health IT product's conformity with voluntary Program requirements and having its product's Complete EHR or Health IT Modules' certification(s) terminated. We further state that the minimal monetary cost estimates for ONC–ATLs derive from voluntary participation in the Program and will be recouped through fees charged for the testing of health IT under the Program.

OMB reviewed this final rule.

List of Subjects in 45 CFR Part 170

Computer technology, Electronic health record, Electronic information system, Electronic transactions, Health, Health care, Health information technology, Health insurance, Health records, Hospitals, Incorporation by reference, Laboratories, Medicaid, Medicare, Privacy, Reporting and recordkeeping requirements, Public health, Security.

For the reasons set forth in the preamble, 45 CFR subtitle A, subchapter D, part 170, is amended as follows:

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

■ 1. The authority citation for part 170 continues to read as follows:

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

■ 2. Amend § 170.299 by revising paragraph (a) to read as follows:

§ 170.299 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

[32] *https://www.sba.gov/sites/default/files/files/Size_Standards_Table.pdf.*

[33] *https://www.sba.gov/sites/default/files/files/Size_Standards_Table.pdf.*

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 sources 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.*

* * * * *

■ 3. Revise § 170.501 to read as follows:

§ 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 Complete EHRs, 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 Complete EHRs and Health IT Modules in accordance with the applicable certification criteria adopted by the Secretary in subpart C of this part.

(c) This subpart establishes the processes accreditation organizations must follow to request approval from the National Coordinator to be an ONC–AA and that the National Coordinator will follow to approve an accreditation organization under the ONC Health IT Certification Program as well as certain ongoing responsibilities for an ONC–AA.

(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.

■ 4. Amend § 170.502 by revising the definitions of ‘‘Applicant’’ and ‘‘Gap certification’’ and by adding the definition of ‘‘ONC-Authorized Testing Lab or ONC–ATL’’ in alphabetical order to read as follows:

§ 170.502 Definitions.

* * * * *

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.

* * * * *

Gap certification means the certification of a previously certified Complete EHR or 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 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 Complete EHRs and Health IT Modules to certification criteria adopted by the Secretary at subpart C of this part.

* * * * *

■ 5. Revise § 170.505 to read as follows:

§ 170.505 Correspondence.

(a) Correspondence and communication with ONC or the National Coordinator shall be conducted by email, unless otherwise necessary or specified. The official date of receipt of any email between ONC or the National Coordinator and an accreditation organization requesting ONC–AA status, the ONC–AA, 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 accreditation organization requesting ONC–AA status, the ONC–AA, 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.

■ 6. Amend § 170.510 by revising the section heading and introductory text to read as follows:

§ 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:

* * * * *

■ 7. Add § 170.511 to read as follows:

§ 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.

■ 8. Revise § 170.520 to read as follows:

§ 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 by the ONC–AA.

(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.

■ 9. Amend § 170.523 by revising paragraphs (h) and (i) and adding paragraph (o) to read as follows:

§ 170.523 Principles of proper conduct for ONC–ACBs.

* * * * *

(h) Only certify health IT (Complete EHRs and/or Health IT Modules) that has been tested, using test tools and test procedures approved by the National Coordinator, by a/an:

(1) ONC–ATL;

(2) NVLAP-accredited testing laboratory under the ONC Health IT Certification Program for no longer than six months from December 19, 2016; or

(3) ONC–ATL, NVLAP-accredited testing laboratory under the ONC Health IT Certification Program, and/or an ONC–ATCB for the purposes of:

(i) Certifying previously certified Complete EHRs and/or Health IT Module(s) if the certification criterion or criteria to which the Complete EHRs and/or Health IT Module(s) was previously certified have not been revised and no new certification criteria are applicable to the Complete EHRs and/or Health IT Module(s); or

(ii) Performing gap certification.

(i) 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.

* * * * *

(o) Be prohibited from reducing the scope of a Complete EHR or Health IT Module's certification when it is under surveillance or under a corrective action plan.

■ 10. Add § 170.524 to read as follows:

§ 170.524 Principles of proper conduct for ONC–ATLs.

An ONC–ATL shall:

(a) Maintain its NVLAP accreditation for the ONC Health IT Certification Program, including accreditation to ISO/IEC 17025 (incorporated by reference, *see* § 170.599);

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

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

(d) 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) 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 Complete EHRs and/or Health IT Modules to an edition of certification criteria for a minimum of 3 years from the effective date that removes the applicable edition 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) Only test health IT using test tools and test procedures approved by the National Coordinator; and

(h) 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 Complete EHRs and/or Health IT Modules.

■ 11. Revise § 170.525 to read as follows:

§ 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.

■ 12. Amend § 170.530 by revising paragraphs (c)(2) and (4) and (d)(2) and (3) to read as follows:

§ 170.530 Review of application.

* * * * *

(c) * * *

(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.

* * * * *

(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) * * *

(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.

■ 13. Amend § 170.535 by revising the section heading and paragraphs (a) and (d)(1) to read as follows:

§ 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.

* * * * *

(d) * * *

(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.

* * * * *

■ 14. Revise § 170.540 to read as follows:

§ 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.

■ 15. Amend § 170.556 by revising paragraph (d)(6) and (e)(1) to read as follows:

§ 170.556 In-the-field surveillance and maintenance of certification for health IT.

* * * * *

(d) * * *

(6) *Withdrawal.* If a certified Complete EHR or certified Health IT Module's certification has been suspended, an ONC–ACB is permitted to initiate certification withdrawal procedures for the Complete EHR or 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) * * *

(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).

* * * * *

■ 16. Revise § 170.557 to read as follows:

§ 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.

■ 17. Revise § 170.560 to read as follows:

§ 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 Complete EHRs and/or 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.

■ 18. Revise § 170.565 to read as follows:

§ 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 noncompliance 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 noncompliance 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 Complete EHRs or 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 Complete EHRs or 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 Complete EHRs and 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.

■ 19. Revise § 170.570 to read as follows:

§ 170.570 Effect of revocation on the certifications issued to Complete EHRs and EHR Module(s).

(a) The certified status of Complete EHRs and/or 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 Complete EHRs and/or Health IT Module(s) certifications were based on unreliable testing and/or certification.

(c) If the National Coordinator determines that Complete EHRs and/or Health IT Module(s) certifications were based on unreliable testing and/or certification, the certification status of affected Complete EHRs and/or Health IT Module(s) would only remain intact for 120 days after the National Coordinator publishes the notice.

(1) The certification status of affected Complete EHRs and/or 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 Complete EHRs and/or Health IT Module(s) remains intact as necessary for the proper retesting and recertification of the affected health IT.

■ 20. Add § 170.580 to read as follows:

§ 170.580 ONC review of certified health IT.

(a) *Direct review*—(1) *Purpose.* ONC may directly review certified health IT to determine whether it conforms to the requirements of the ONC Health IT Certification Program.

(2) *Circumstances that may trigger review*—(i) *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.* 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.

(3) *Relationship to ONC–ACBs and ONC–ATLs.* (i) ONC's review of certified health IT is independent of, and may be in addition to, any surveillance 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.

(v) ONC may end all or any part of its review of certified health IT 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.

(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 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 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.

(2) *Notice of non-conformity*—(i) *Circumstances that may trigger notice of non-conformity.* At any time during its review of certified health IT 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 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; and

(ii) Any complaint records related to the certified health IT.

(c) *Corrective action plan and procedures.* (1) If ONC determines that certified health IT 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 Complete EHR or 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 Complete EHR or 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 Complete EHR or 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 Complete EHRs or 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) ONC may propose to terminate a certification issued to a Complete EHR and/or 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) 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; or

(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.

(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 Complete EHR or 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 Complete EHR or Health IT Module if the health IT developer asserts:

(i) ONC incorrectly applied ONC Health IT Certification Program requirements for suspension or termination; or

(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 whose Complete EHR or Health IT Module was 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 termination or notice of suspension.

(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 suspension or notice of termination.

(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 on suspension and termination.* (i) A request for appeal stays the termination of a certification issued to a Complete EHR or Health IT Module, but the Complete EHR or 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 Complete EHR or Health IT Module.

(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 or termination 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.

(A) The written statement and supporting documentation must be included as part of the written record and provided to the health IT developer within 15 days of the health IT developer's filing of an intent to appeal.

(B) Failure of ONC to submit a written statement does not result in any adverse findings against ONC and may not in any way be taken into account by the hearing officer in reaching a determination.

(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.

■ 21. Add § 170.581 to read as follows:

§ 170.581 Certification ban.

(a) *Ban.* The certification of any of a health IT developer's health IT is prohibited when the certification of one or more of the health IT developer's Complete EHRs or Health IT Modules is:

(1) Terminated by ONC under the ONC Health IT Certification Program;

(2) Withdrawn from the ONC Health IT Certification Program by an ONC–ACB because the health IT developer requested it to be withdrawn when the health IT developer's health IT was the subject of a potential non-conformity or non-conformity as determined by ONC;

(3) 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; or

(4) Withdrawn by an ONC–ACB because the health IT developer requested it to be withdrawn 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.

(b) *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 or withdrawal have been provided appropriate remediation.

(3) ONC is satisfied with the health IT developer's demonstration under paragraph (b)(2) of this section that all affected customers have been provided with appropriate remediation and grants reinstatement into the ONC Health IT Certification Program.

■ 22. Revise § 170.599 to read as follows:

§ 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 17065:2012(E)—Conformity assessment—Requirements for bodies certifying products, processes and services (First Edition), 2012, ''ISO/IEC 17065,'' IBR approved for § 170.503.

Sylvia M. Burwell,

Secretary, Department of Health and Human Services.

[FR Doc. 2016–24908 Filed 10–14–16; 8:45 am]

BILLING CODE 4150–45–P