The Office of the National Coordinator for
Health Information Technology

ONC HEALTH IT CERTIFICATION PROGRAM
Program Policy Guidance #15-01A
November 5, 2015

I. Introduction

Program Policy Guidance #15-01A updates ONC's annual surveillance guidance to ONC-Authorized Certification Bodies (ONC-ACBs) for the calendar year 2016 (CY16) surveillance period. ONC-ACBs are required to perform surveillance of health information technology (health IT) they have certified.[1] We issue annual surveillance guidance to assist ONC-ACBs in developing their annual surveillance plans, to clarify surveillance requirements under the ONC Health IT Certification Program, and to identify topics and specific elements of ONC-ACBs' surveillance that ONC considers a priority.

This guidance replaces Program Policy Guidance #15-01,[2] which was issued on July 16, 2015. At that time, we had proposed but not finalized certain modifications to the ONC Health IT Certification Program that could affect ONC-ACBs' surveillance responsibilities.[3] We recommended that ONC-ACBs familiarize themselves with the proposed modifications and be prepared to update their CY16 surveillance plans in the event that such modifications were finalized.[4] Subsequently, on October 16, 2015, we published the 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications final rule (80 FR 62601) ("2015 Edition Final Rule"). The 2015 Edition Final Rule establishes additional surveillance requirements under the ONC Health IT Certification Program, most of which take effect on January 14, 2016. This guidance will assist ONC-ACBs to update their CY16 surveillance plans in accordance with these new requirements in the 2015 Edition Final Rule and existing requirements articulated in previous years' guidance.

As outlined in greater detail below, CY16 surveillance plans must address many of the same topics and elements as in previous years while incorporating improvements and addressing new requirements. We expect CY16 surveillance plans to incorporate substantial improvements and refinements over previous years' based on ONC-ACBs' individual and collective experience developing and implementing their CY14 and CY15 plans, and based on feedback from the ONC-Approved Accreditor (ONC-AA) and ONC. In addition, we have identified certain new priority areas for surveillance in CY16, including the 2014 Edition "data portability" certification criterion and health IT developer transparency and disclosures. We believe these priority areas are critical to advancing interoperability and deterring information blocking and other problematic business practices.

CY16 surveillance plans must reflect changes to certification criteria and program requirements adopted in the 2015 Edition Final Rule and the 2014 Edition Release 2 Electronic Health Record (EHR)

[1] See Program Policy Guidance #13-01 (July 2013), http://www.healthit.gov/sites/default/files/onc-acb_2013annualsurveillanceguidance_final_0.pdf. See also 45 CFR § 170.556.

[2] ONC Health IT Certification Program, Program Policy Guidance #15-01 (July 16, 2015), http://healthit.gov/sites/default/files/policy/onc-acb_cy16annual_surveillance_guidance.pdf.

[3] See 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications proposed rule, 80 FR 16804 (March 30, 2015).

[4] See Program Policy Guidance #15-01, supra n.2. We also stated that we would issue additional guidance, as needed, to assist ONC-ACBs to update their surveillance plans in accordance with any new or modified requirements. Id.

Certification Criteria and the ONC Health IT Certification Program; Regulatory Flexibilities, Improvements, and Enhanced Health Information Exchange; Final Rule (79 FR 54430) (2014 Edition Release 2 Final Rule). In particular, in developing and prior to submitting their CY16 surveillance plans, ONC-ACBs are expected to carefully review the extensive discussion of "In-the-field Surveillance and Maintenance of Certification" and "Transparency and Disclosure Requirements" in the preamble to the 2015 Edition Final Rule.

II. Submission of CY16 Surveillance Plans

ONC-ACBs must submit annual surveillance plans to the National Coordinator as required by 45 CFR § 170.523(i). Annual surveillance plans must describe in detail an ONC-ACB's surveillance approach for the following calendar year. CY16 surveillance plans were due to ONC on September 30, 2015; however, given the additional surveillance requirements established by the subsequently-published 2015 Edition Final Rule, we are extending the submission deadline to allow ONC-ACBs additional time to revise and resubmit their plans to address these new requirements. Thus, final CY16 surveillance plans must be submitted to ONC by **December 5, 2015**. Extensions may be granted in limited circumstances and must be requested in writing with accompanying rationale no later than **November 24, 2015**. ONC will only accept electronic submissions of surveillance plans and requests for extensions. Plans and requests for extensions must be submitted via ONC-ACB@hhs.gov.

III. ONC-ACB Surveillance Approach

We believe there are additional factors and circumstances that an ONC-ACB will be unable to assess at the time the health IT was initially certified based on tests completed by the developer in a controlled environment. Therefore, ONC-ACBs must conduct surveillance (including in-the-field surveillance) to assess whether certified health IT not only meets the requirements of certification in a controlled testing environment but continues to do so when implemented and used in a production environment. Similarly, ONC-ACBs must conduct surveillance to assess whether developers of certified health IT comply with program requirements under the ONC Health IT Certification Program.

CY16 surveillance plans must explain an ONC-ACB's overall approach to surveillance. An ONC-ACB's overall approach must address how the ONC-ACB will conduct both proactive and reactive surveillance of certified health IT, including in-the-field surveillance, as required by 45 CFR § 170.556(a)–(c). ONC-ACBs must also explain how they will administer the corrective action procedures specified by 45 CFR § 170.556(d) and how they will meet the reporting requirements at 45 CFR § 170.556(e). Further, ONC-ACBs must describe how they will address the specific aspects of surveillance prioritized below in Part IV of this guidance. CY16 surveillance plans must include a detailed discussion of all of these elements, which are further explained below.

A. <u>In-the-field Surveillance</u>

Consistent with their accreditation to ISO/IEC 17065 and the requirements of the ONC Health IT Certification Program, ONC-ACBs must perform surveillance of certified health IT "in the field" to determine whether the technology continues to conform to the requirements of its certification once implemented and in use in a production environment. In-the-field surveillance is a key part of both an ONC's proactive and reactive approaches to surveillance. 45 CFR § 170.556(a)–(c). It is therefore important that CY16 surveillance plans provide a full discussion of ONC-ACBs' in-the-field surveillance procedures and methodologies.

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**. While testing is an important part of an ONC-ACB's overall analysis of health IT under the ONC Health IT Certification Program, it 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 subject to an ONC-ACB's ongoing surveillance, including the ONC-ACB's evaluation of certified capabilities in the field. The 2015 Edition Final Rule discusses at length certain circumstances under which health IT would no longer conform to the requirements of its certification, including several examples of non-conformities in the field that would not occur during testing in a controlled environment.[5] Accordingly, when evaluating certified capabilities in the field, 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. 80 FR 62601, 62709. We expect CY16 surveillance plans to explain how ONC-ACBs will evaluate these case-specific factors, including:

- What criteria and methodologies the ONC-ACB will apply in determining whether and under what circumstances to initiate in-the-field surveillance of certified health IT (including how the ONC-ACB will decide which capabilities and/or program requirements to evaluate in the field).
- What methodologies and techniques the ONC-ACB will employ when actually observing and evaluating the use of certified capabilities and developers' compliance with certification program requirements in the field.
- What other investigative and diagnostic techniques the ONC-ACB will use to supplement its in-the-field observations (e.g., user feedback, reviewing developers' complaint logs and resolution of complaints, replicating reported problems in a controlled environment, and other appropriate techniques).
- How the ONC-ACB will engage and work with developers and end-users to analyze and determine the causes of issues.
- How the ONC-ACB will evaluate potential non-conformities resulting from implementation or business practices of the health IT developer that could affect the performance of certified capabilities in the field.[6]
- How the ONC-ACB will evaluate potential non-conformities resulting from the non-disclosure of material information about limitations or additional types of costs associated with certified health IT.[7]
- How the ONC-ACB will document its findings, analysis, and conclusions.

[5] For example, an ONC-ACB would find a non-conformity were it to determine that a developer had imposed restrictions or limitations on its technology (or the use of its technology) that substantially interfered with users' ability to access or use certified capabilities for any purpose within the scope of the technology's certification. Additional examples and discussion of such non-conformities are provided in the 2015 Edition Final Rule. 80 FR 62601, 62709–11.

[6] See supra note 5 and accompanying text.

[7] See infra Parts III.C and V.A. The failure to disclose known material information about certified health IT is a violation of an explicit certification program requirement (45 CFR § 170.523(k)(1)) and thus constitutes a non-conformity. 80 FR 62601, 62711. In addition, the disclosure violation may also give rise to a separate non-conformity in the event that the failure to disclose the required information has substantially impaired, or would be likely to substantially impair, the ability of one or more users (or prospective users) to implement or use the developer's certified health IT in a manner consistent with its certification. Id.

B. Randomized and Other Proactive Surveillance

ONC-ACBs are required to perform ongoing proactive surveillance of certified Complete EHRs and Health IT Modules. CY16 surveillance plans must describe how an ONC-ACB will proactively select health IT developers and products for surveillance, what certification criteria and certification requirements it will assess, and what procedures it will follow when proactively conducting surveillance of certified health IT. Among other topics, ONC-ACBs must describe in detail how they will proactively assess:

- Developers' compliance with the mandatory disclosure requirements at 45 CFR § 170.523(k)(1).
- Health IT's conformity to the prioritized certification criteria described in Part IV of this guidance.
- The adequacy of developers' user complaint processes.
- Appropriate use of the ONC Certification Mark.

As a key aspect of proactive surveillance, ONC-ACBs must conduct randomized surveillance of certified health IT in the field. 45 CFR § 170.556(c). Over the course of CY16, ONC-ACBs must randomly select and perform in-the-field surveillance of 2% of all certified Complete EHRs and/or Health IT Modules for which the ONC-ACB is responsible. For each such certified Complete EHR and/or Health IT Module, the ONC-ACB must perform in-the-field surveillance of each capability (where applicable) prioritized by the National Coordinator below in Part IV.

CY16 surveillance plans must describe ONC-ACBs' sampling and selection methodologies and their procedures for conducting randomized surveillance. In addition, CY16 surveillance plans must describe how ONC-ACBs will document that they have followed the methodologies and procedures described in their CY16 surveillance plans. We note that under the ONC Health IT Certification Program, it is an ongoing responsibility of the ONC-Approved Accreditor (ONC-AA) to ensure that the surveillance approaches used by ONC-ACBs—including the selection processes and methodologies for randomized surveillance discussed below—include the use of consistent, objective, valid, and reliable methods. § 170.503(e)(2). We expect the ONC-AA to review ONC-ACBs' methodologies and procedures and to verify ONC-ACBs' documented randomized surveillance activities against ONC-ACBs' CY16 surveillance plans.

1. Sampling and Selection

An ONC-ACB's selection process under randomized surveillance must adhere to the following requirements, which must be detailed in an ONC-ACB's CY16 surveillance plan:

- The ONC-ACB must select a minimum of 2% of all of the Complete EHRs and/or Health IT Modules to which the ONC-ACB has issued a certification (i.e., all active certifications). The ONC-ACB must select products at random but is permitted to implement appropriate weighting and sampling considerations. We strongly encourage ONC-ACBs to implement weighting techniques that will account for the number of users of certified products. For example, when selecting certificates for randomized surveillance, the ONC-ACB could assign greater weight to products with certifications that are more widely adopted and used so as to increase the likelihood that the products surveilled will include at least some products with a large number of installations and users, thereby increasing the likelihood of discovering and addressing non-conformities that affect a large number of providers and users.

- ONC-ACBs must exclude from randomized surveillance any product for which randomized surveillance was completed within the last 12 months.
- For each product selected for randomized surveillance, the ONC-ACB must select a random sample of one or more locations at which the ONC-ACB will initiate in-the-field surveillance of the certified Complete EHR or certified Health IT Module. The ONC-ACB must select the location or locations at random but is permitted to implement appropriate weighting and sampling considerations. For example, the ONC-ACB could ensure that no two locations selected are under the common ownership or control of a single person or entity, thereby achieving greater diversity of providers and locations.

2. Prioritized Capabilities

When an ONC-ACB selects a product for randomized surveillance, its evaluation of the certified Complete EHR or certified Health IT Module in the field must include the assessment of any capabilities that are (1) within the scope of the certification criteria to which the technology is certified and (2) associated with any certification criterion prioritized by the National Coordinator, as set forth in Part IV of this guidance. 45 CFR § 170.556(c)(1). CY16 surveillance plans must describe how ONC-ACBs' randomized surveillance will address these prioritized capabilities.

3. Exclusion and Exhaustion

Where, having selected a certified Complete EHR or certified Health IT Module for randomized surveillance, and having made a good faith effort to conduct in-the-field surveillance of such Complete EHR or Health IT Module at a particular randomly-selected location, an ONC-ACB cannot complete in-the-field surveillance of the Complete EHR or Health IT Module at such location for reasons beyond its control, the ONC-ACB may exclude such location and substitute another location that meets the random selection requirements described above. Similarly, in the event that the ONC-ACB exhausts all available locations for a particular certified Complete EHR or certified Health IT Module, the ONC-ACB may exclude that Complete EHR or Health IT Module and substitute another randomly selected Complete EHR or Health IT Module.

In the case of exhaustion, we clarify that the excluded certified Complete EHR or Health IT Module will be counted towards the minimum number of products an ONC-ACB is required to randomly surveil during the calendar year surveillance period. We emphasize, however, that an ONC-ACB must carefully and accurately document its efforts to complete in-the-field surveillance for each product and at each location. The ONC-AA would be expected to review this documentation to ensure that ONC-ACBs have met the required random selection requirement and have made a good faith effort to perform in-the-field surveillance prior to excluding any product or location from randomized surveillance.

4. Developer Customer Lists

CY16 surveillance plans must explain how ONC-ACBs will obtain and integrate health IT developers' customer lists into their randomized sampling and other aspects of proactive surveillance. ONC-ACBs must require, as an ongoing condition of certification, that health IT developers furnish to the ONC-ACB upon its request accurate and complete customer lists, user lists, and other information the ONC-ACB determines necessary to carry out its surveillance responsibilities. Access to accurate customer and user lists is essential to an ONC-ACB's ability to contact users for in-the-field surveillance and to conduct surveys and other activities necessary to obtain and synthesize information about the performance of certified health IT. Therefore, if a health IT developer refuses to provide this information to an ONC-ACB, the ONC-ACB may regard the refusal as a refusal to participate in surveillance under the ONC Health IT Certification Program and institute appropriate procedures, consistent with the ONC-ACB's accreditation to ISO 17065, to suspend or terminate the health IT Module/Complete EHR certification. 80 FR 62601, 62716.

C. Reactive Surveillance

Separate from and in addition to proactive surveillance under Part III.B, an ONC-ACB has a duty to perform ongoing reactive surveillance of certified health IT. 45 CFR § 170.556(b).

An ONC-ACB must initiate surveillance—including, as necessary, in-the-field surveillance—of a certified Complete EHR or certified Health IT Module whenever it becomes aware of facts or circumstances that would cause a reasonable person to question the health IT's continued conformity to the requirements of its certification. 45 CFR § 170.556(b). Such conformity includes the technology's ongoing compliance with applicable certification criteria and the technology developer's ongoing compliance with certification requirements. 80 FR 62601, 62712. Accordingly, CY16 surveillance plans must detail how an ONC-ACB will systematically obtain, synthesize, and act on information concerning ongoing compliance with these requirements, including but not limited to the following information:

- Health IT developers' complaint logs, service tickets, and documentation concerning the analysis and resolution of complaints or issues reported to the developer.
- Complaints and other information about certified health IT submitted directly to an ONC-ACB by customers or users of certified health IT, by the National Coordinator,[8] or by other persons.
- Developers' public and private disclosures regarding certified health IT capabilities.
- Information from publicly available sources (e.g., a developer's website or user forums).
- Repeated inherited certified status requests.[9]
- Other facts and circumstances of which the ONC-ACB is aware.

CY16 surveillance plans must describe the procedures ONC-ACBs will follow for weighing the volume, substance, and credibility of this information in order to determine whether to initiate surveillance for a certified capability or certification program requirement, including how the ONC-ACB will determine if and when certified capabilities or certification program requirements require inspection and evaluation with the technology developer, in-the-field observation of the technology, or other forms of surveillance. See 80 FR 62601, 62713. Whether an ONC-ACB must perform in-the-field surveillance or may employ other methods is governed by the definition and principles for in-the-field surveillance codified at § 170.556(a) and elaborated in our discussion of that section in the 2015 Edition Final Rule. 80 FR 62601, 62708–09. Among other factors, an ONC-ACB must consider the nature of the suspected non-conformity and the adequacy of other forms of surveillance for evaluating the suspected non-

[8] When ONC receives a user complaint about health IT, ONC's general practice is to forward the complaint to the ONC-ACB responsible for performing surveillance for that product under the ONC Health IT Certification Program.

[9] Consistent with prior years' practice, we expect ONC-ACBs to automatically initiate surveillance of a Complete EHR or Health IT Module upon the issuance of 3 or more inherited certified status requests.

conformity under the circumstances.[10] In-the-field surveillance may also be necessary to determine a developer's compliance with certification program requirements, such as the disclosure requirements at 45 CFR § 170.523(k)(1). While non-compliance with these requirements may often be established from complaints and a review of a developer's disclosures, certain kinds of undisclosed limitations or types of costs associated with certified capabilities may need to be confirmed through in-the-field surveillance of the technology, or may not be discovered at all except upon observing the operation of certified capabilities in the field.

Of special importance, ONC-ACBs must specifically outline their approach to weighing complaints and other information indicating that a developer has failed to disclose known material information about certified capabilities, as required by § 170.523(k)(1), and how this information will be used to inform their decisions whether to initiate surveillance, including in-the-field surveillance, of potentially affected certified capabilities.[11] See 80 FR 62601, 62711. In addition, ONC-ACBs must describe in detail what actions they will take to determine whether any failure to disclose material information has prevented users from successfully implementing and using any capability of certified health IT for any use within the scope of the health IT's certification. We note that ONC-ACBs must always review health IT developers' disclosures whenever they perform reactive surveillance. 45 CFR § 170.556(b)(1).

Similarly, ONC-ACBs should explain how they will weigh and act on information about other aspects of surveillance prioritized by the National Coordinator below in Part IV of this guidance.

IV. Prioritized Elements of Surveillance

For CY16, we have prioritized the following capabilities:

- Interoperability and Information Exchange
  - 45 CFR § 170.314(b)(1) Transitions of care – receive, display and incorporate transition of care/referral summaries.
  - 45 CFR § 170.314(b)(2) Transitions of care – create and transmit transition of care/referral summaries.
  - 45 CFR § 170.314(b)(7) Data portability.
  - 45 CFR § 170.314(b)(8) Optional – transitions of care.

[10] In most cases, the need to evaluate the certified health IT in the field will be obvious from the nature of the suspected non-conformity. For example, if a problem with a certified health IT capability is reported to arise only in connection with a specific local implementation option, an ONC-ACB would likely need to observe the relevant capabilities in the field in order to fully analyze the cause of the problem and determine whether it is the result of a non-conformity. In other cases, the need for in-the-field surveillance may become apparent only after other surveillance methods and techniques have failed to isolate the cause of the problem. 80 FR 62601, 62708–09.

[11] An ONC-ACB's decision to initiate reactive surveillance must take into account complaints and other information indicating whether a health IT developer has disclosed all known material information about certified capabilities, as required by 45 CFR § 170.523(k)(1). 80 FR 62601, 62713. The failure to disclose this information calls into question the continued conformity of those capabilities because it creates a substantial risk that existing and prospective users will encounter problems implementing the capabilities in a manner consistent with the applicable certification criteria. Id. Where an apparent failure to disclose known material information raises these potential concerns regarding the performance of certified health IT capabilities, an ONC-ACB would be required to initiate in-the-field surveillance to determine both whether the developer had failed to disclose the information and, if so, whether the failure to disclose the information prevented users from reasonably implementing and using certified capabilities for any purpose within the scope of the health IT's certification. Id.

  - 45 CFR § 170.314(e)(1) View, download, and transmit to 3rd party.
  - 45 CFR § 170.314(h)(1) Optional – Transmit - Applicability Statement for Secure Health.
  - 45 CFR § 170.314(h)(2) Optional – Transmit - Applicability Statement for Secure Health Transport and XDR/XDM for Direct Messaging.

- Safety-related
  - 45 CFR § 170.314(a)(2) Drug-drug, drug-allergy interaction checks.
  - 45 CFR § 170.314(a)(8) Clinical decision support.
  - 45 CFR § 170.314(a)(16) Inpatient setting only—electronic medication administration record.
  - 45 CFR § 170.314(b)(4) Clinical information reconciliation.
  - 45 CFR § 170.314(b)(9) Optional – Clinical information reconciliation and incorporation.

- Security
  - 45 CFR § 170.314(d)(2) Auditable Events and Tamper-Resistance.
  - 45 CFR § 170.314(d)(7) End-User Device Encryption.

- Population Management
  - 45 CFR § 170.314(c)(2) Clinical quality measures – import and calculate

We expect ONC-ACBs to cumulatively and thoroughly address these capabilities throughout CY16. In addition, and as discussed above in Part III.B, ONC-ACBs must explain how they will address these prioritized capabilities as part of their randomized surveillance activities.

In addition to the above capabilities, we consider the following additional elements to be a priority for surveillance in CY16 and therefore expect ONC-ACBs to specifically address them as part of their CY16 surveillance plans:

- The assessment of developers' disclosures, as required by 45 CFR § 170.523(k), and the evaluation of potential non-conformities resulting from the failure to disclose material information about limitations or additional types of costs associated with certified health IT.[12]
- The assessment of potential non-conformities resulting from implementation or business practices of a health IT developer that could affect the performance of certified capabilities in the field.
- The adequacy of developers' user complaint processes, including customer complaint logs, consistent with ISO/IEC 17065 §4.1.2.2(j).
- Appropriate use of the ONC Certification Mark.

V. Transparency and Disclosure Requirements

A. Surveillance of Developers' Disclosures

[12] For additional discussion of this element and its inclusion in ONC-ACBs' CY16 surveillance plans, see Part III of this guidance.

Developers must make a comprehensive disclosure of all known material information regarding their certified health IT—including limitations and additional types of costs. 45 CFR § 170.523(k)(1). ONC-ACBs must describe in their CY16 surveillance plans how they will ensure adherence to this requirement of the ONC Health IT Certification Program. As explained in more detail in the 2015 Edition Final Rule at 80 FR 62601, 62722–24, to comply with the disclosure requirements, a developer must disclose in plain language—on its website and in all marketing materials, communications statements, and other assertions related to its certified health IT—a detailed description of all **known material information** concerning limitations and additional types of costs that a person may encounter or incur to implement or use certified health IT capabilities, whether to meet meaningful use objectives and measures or to achieve any other use within the scope of the health IT's certification. Such information is "material" (and its disclosure therefore required) if the failure to disclose it could substantially interfere with the ability of a user or prospective user to implement or use certified health IT for any use within the scope of the health IT's certification. Certain kinds of limitations and additional types of costs will always be material and thus, if known, must be disclosed. These include but are not limited to:

- Additional types of costs or fees (whether fixed, recurring, transaction-based, or otherwise) imposed by a developer (or any third-party from whom the developer purchases, licenses, or obtains any technology, products, or services in connection with its certified health IT) to purchase, license, implement, maintain, upgrade, use, or otherwise enable and support the use of capabilities to which health IT is certified; or in connection with any data generated in the course of using any capability to which health IT is certified. 45 CFR § 170.523(k)(1)(iv)(A).
- Limitations, whether by contract or otherwise, on the use of any capability to which technology is certified for any purpose within the scope of the technology's certification; or in connection with any data generated in the course of using any capability to which health IT is certified. 45 CFR § 170.523(k)(1)(iv)(B).
- Limitations, including but not limited to technical or practical limitations of technology or its capabilities, that could prevent or impair the successful implementation, configuration, customization, maintenance, support, or use of any capabilities to which technology is certified; or that could prevent or limit the use, exchange, or portability of any data generated in the course of using any capability to which technology is certified. 45 CFR § 170.523(k)(1)(iv)(C).

We note that developers are not required to disclose information of which they are not and could not reasonably be aware, nor to account for every conceivable type of cost or implementation hurdle that a customer may encounter. "Developers are required, however, to describe **with particularity** the nature, magnitude, and extent of the limitations or types of costs." 80 FR 62601, 62722 (emphasis in original). A developer's disclosure possesses the requisite particularity if it contains sufficient information and detail from which a reasonable person under the circumstances would, without special effort, be able to reasonably identify the specific limitations he may encounter and reasonably understand the potential costs he may incur in the course of implementing and using capabilities for any purpose within the scope of the health IT's certification. Id.

These requirements are explained in more detail in the 2015 Edition Final Rule, which also contains a number of hypothetical scenarios and accompanying analysis that will assist ONC-ACBs in understanding these requirements and incorporating them in their CY16 surveillance plans. We refer ONC-ACBs in particular to the discussion of these requirements at 80 FR 62601, 62722–24. We expect CY16 surveillance plans to contain a detailed and comprehensive approach to administering these new disclosure requirements, which we consider a major focus of the ONC Health IT Certification Program for CY16.

B. Attestation Requirement

CY16 surveillance plans must explain how ONC-ACBs will administer the transparency attestation requirement at 45 CFR § 170.523(k)(2). As a condition of certification, health IT developers must make one of the following attestations:

In the affirmative:

> In support of enhanced marketplace transparency and visibility into the costs and performance of certified health IT products and services, and the business practices of health IT developers, [*Developer Name*] hereby attests that it will provide in a timely manner, in plain writing, and in a manner calculated to inform, any part (including all) of the information required to be disclosed under 45 CFR § 170.523(k)(1) under the following circumstances:
>
> - **To all persons who request such information**.
> - **To all persons who request or receive a quotation**, estimate, description of services, or other assertion or information from [*Developer Name*] in connection with any certified health IT or any capabilities thereof.
> - **To all customers prior to providing or entering into any agreement** to provide any certified health IT or related product or service (including subsequent updates, add-ons, or additional products or services during the course of an on-going agreement).

- OR -

In the negative:

> [*Developer Name]* hereby attests that it has been asked to make the voluntary attestation described by 45 CFR § 170.523(k)(2)(i) in support of enhanced marketplace transparency and visibility into the costs and performance of certified health IT products and services, and the business practices of health IT developers. **[*Developer Name*] hereby declines to make such attestation at this time.**

While developers' adherence to their attestations is voluntary, ONC-ACBs are responsible for ensuring that all developers attest to one or the other of these two statements. Further, ONC-ACBs must include developers' attestations in the information submitted to National Coordinator for inclusion in the CHPL so that the public can determine which developers have attested to taking the additional actions to promote transparency of their technologies and business practices. We note that a developer's attestation under 45 CFR § 170.523(k)(2) does not broaden or change the scope of the information a developer is required to disclose under 45 CFR § 170.523(k)(1).

VI. Corrective Action Procedures

When an ONC-ACB determines that a Complete EHR or Health IT Module does not conform to the requirements of its certification, the ONC-ACB must notify the developer of its findings and require the developer to submit a proposed corrective action plan for the applicable certification criterion, certification criteria, or certification requirement. 45 CFR § 170.556(d). CY16 surveillance plans must describe the procedures ONC-ACBs will follow for:

- Notifying the developer of its findings and requiring the developer to submit a proposed corrective action plan for the applicable certification criterion, certification criteria, or certification requirement. 45 CFR § 170.556(d)(1).
- Providing direction to the developer as to the required elements of the corrective action plan. 45 CFR § 170.556(d)(2).
- Determining what elements the developer must address as part of its corrective action plan, including an appropriate timeframe for completing corrective action under the circumstances, and evaluating and determining whether to approve, require revisions to, or reject a proposed corrective action plan submitted by a developer. 45 CFR § 170.556(d)(3)–(4).
- Ensuring that proposed and revised corrective action plans are timely submitted and completed, or, if such plans are not timely submitted or completed, taking appropriate action to suspend or terminate the health IT's certification. 45 CFR § 170.556(d)(5)–(6) and 170.556(f).
- Submitting corrective action information to ONC for inclusion on the Certified Health IT Product List (CHPL). 45 CFR § 170.523(f)(1)(xxii) & (f)(2)(xi).

ONC-ACB's must ensure prior to approving any corrective action plan that it contains the following elements:

- A description of the identified non-conformities or deficiencies;
- An assessment of how widespread or isolated the identified non-conformities or deficiencies may be across all of the developer's customers and users of the certified Complete EHR or certified Health IT Module;
- How the developer will address the identified non-conformities or deficiencies, both at the locations under which surveillance occurred and for all other potentially affected customers and users;
- How the developer will ensure that all affected and potentially affected customers and users are alerted to the identified non-conformities or deficiencies, including a detailed description of how the developer will assess the scope and impact of the problem, including identifying all potentially affected customers; how the developer will promptly ensure that all potentially affected customers are notified of the problem and plan for resolution; how and when the developer will resolve issues for individual affected customers; and how the developer will ensure that all issues are in fact resolved.
- The timeframe under which corrective action will be completed.
- Any additional elements specified by the National Coordinator or that the ONC-ACB deems appropriate, consistent with its accreditation.
- A requirement that the developer attest to having completed all elements of the corrective action plan (discussed below).

Finally, ONC-ACBs must outline their approach for verifying that developers have completed all requirements of corrective action specified in the approved corrective action plan. At a minimum, ONC-ACBs must detail an approach under which they will require developers to attest that the developer has completed all required elements of the plan and through which the ONC-ACB will validate that attestation. In this connection, we expect ONC-ACBs to verify that developers have notified all affected and potentially affected customers and users.

VII. Submission of Corrective Action and Surveillance Information

A. Submission of Corrective Action Information

CY16 surveillance plans must describe how ONC-ACBs will document and timely (no less frequently than weekly) submit the following corrective action information to ONC for inclusion in the CHPL, as required by 45 CFR § 170.523(f)(1)(xxii) & (f)(2)(xi):

- Each Complete EHR or Health IT Module that failed to conform to its certification and for which corrective action was instituted under 45 CFR § 170.556. ONC-ACBs must use the CHPL product number to identify the certified Complete EHRs and Health IT Modules.
- The specific certification requirements to which the technology failed to conform, as determined by the ONC-ACB.
- A summary of the deficiency or deficiencies identified by the ONC-ACB as the basis for its determination of non-conformity.
- When available, the health IT developer's explanation of the deficiency or deficiencies.
- The dates surveillance was initiated and completed.
- The results of randomized surveillance, including pass rate for each criterion in instances where the Complete EHR or EHR Module is evaluated at more than one location.
- The number of sites that were used in randomized surveillance.
- The date of the ONC-ACB's determination of non-conformity.
- The date on which the ONC-ACB approved a corrective action plan.
- The date corrective action began (effective date of approved corrective action plan).
- The date by which corrective action must be completed (as specified by the approved corrective action plan).
- The date corrective action was completed.
- A description of the resolution of the non-conformity or non-conformities.

B. Submission of Surveillance Information

1. Surveillance Narratives and Corroborating Documentation

ONC-ACBs must report surveillance results to the National Coordinator on a rolling basis (i.e., no less frequently than quarterly) throughout CY16. 45 CFR § 170.523(i)(2) and § 170.556(e). When submitting annual surveillance results, ONC-ACBs must identify each instance of surveillance performed during CY16 and the results of that surveillance. In each case, the ONC-ACB must submit a detailed narrative and corroborating documentation and evidence to support its determination, including:

- Each certified Complete EHR or Health IT Module, certification criterion, and certification program requirement that was subjected to surveillance during CY16. ONC-ACBs must use the CHPL product number to identify the certified Complete EHRs and Health IT Modules.
- The type of surveillance initiated in each case.

- The grounds for initiating surveillance and for deciding whether or not to evaluate the certified health IT in the field.

- Whether or not the ONC-ACB confirmed a non-conformity.
- The substantial factors that, in the ONC-ACBs assessment, caused or contributed to the apparent non-conformity (e.g., implementation problem, user error, limitations on the use of capabilities in the field, a failure to disclose known material information, etc.).
- The steps the ONC-ACB took to obtain and analyze evidence and to arrive at its conclusions.

CY16 surveillance plans must describe in detail the process by which ONC-ACBs will collect and submit all of the information described above, including the following procedural aspects:

- Methodologies and techniques the ONC-ACB will employ when determining whether to initiate surveillance, what type of surveillance to perform (e.g., in-the-field surveillance or other forms of surveillance), and how to evaluate suspected non-conformities.
- How the ONC-ACB will engage and work with developers and end-users to analyze and determine the causes of suspected non-conformities and related deficiencies.
- How the ONC-ACB will evaluate potential non-conformities resulting from implementation or business practices of a health IT developer that could affect the performance of certified capabilities in the field.[13]
- How the ONC-ACB will evaluate potential non-conformities resulting from the non-disclosure of material information about limitations or additional types of costs associated with certified health IT.
- How the ONC-ACB will document its findings, analyses, and conclusions.

2. *Review of Developer Complaint Processes*

CY16 surveillance plans must also explain how ONC-ACBs will identify, for each health IT developer whose technology was subject to surveillance during the applicable calendar year, and regardless of the circumstances that triggered surveillance or the type of surveillance performed:

- The extent to which the developer followed its complaint process, and any observed deficiencies with its process.
- The frequency of complaints made to the developer associated with the prioritized elements in Part IV.

C. Due Process and Exclusion of Certain Sensitive Information

1. *Meaningful Opportunity for Input and Comment on ONC-ACB Findings*

Consistent with its accreditation to ISO 17065 and with the Principles of Proper Conduct for ONC-ACBs, we expect an ONC-ACB to complete its review of all relevant facts and circumstances, including those raised by the developer in the course of the ONC-ACB's surveillance, prior to making a

[13] For example, an ONC-ACB would find a non-conformity were it to determine that a developer had imposed restrictions or limitations on its technology (or the use of its technology) that substantially interfered with users' ability to access or use certified capabilities for any purpose within the scope of the technology's certification. Additional examples and discussion of such non-conformities are provided in the 2015 Edition Final Rule. 80 FR 62709–11.

non-conformity or other determination and prior to submitting its surveillance results and, where applicable, corrective action information to the National Coordinator. 80 FR 62601, 62717–18.

Moreover, we expect ONC-ACBs to provide a meaningful opportunity for the developer to explain any deficiencies prior to an ONC-ACB's final non-conformity determination. When the developer has provided an explanation of the deficiencies identified by the ONC-ACB as the basis for its determination, the ONC-ACB must include the developer's explanation (subject to any exclusions described below) in its submission of this information to the National Coordinator. 80 FR 62601, 62718.

2. Exclusion of Certain Information from Submission of Corrective Action Information and Surveillance Results

In submitting corrective action information and surveillance results to the National Coordinator, ONC-ACBs must exclude any information that would identify any customer or user, any health care provider, location, or practice site that participated in or was subject to surveillance, or any person who submitted a complaint or other information to a health IT developer or ONC-ACB.

3. Exclusion of Certain Information from Submission of Corrective Action Information

With respect to the submission of corrective action information to the National Coordinator for inclusion in the CHPL, ONC-ACBs should not submit any information that is in fact legally privileged or protected from disclosure and that therefore should not be listed on a publicly available website. ONC-ACBs may also implement other appropriate safeguards, as necessary, to protect information that, while not legally protected from disclosure, the ONC-ACB believes should not be reported to a publicly available website. We caution, however, that ONC-ACBs must ensure that such safeguards are narrowly tailored and consistent with the goal of promoting the greatest possible degree of transparency with respect to certified health IT and the business practices of certified health IT developers, especially the disclosure of material information about limitations and types of costs associated with certified health IT. ONC-ACBs are required to accurately report the results of their surveillance and to explain in detail the facts and circumstances on which their conclusions are based.[14]

D. <u>Due Date and Submission Method</u>

CY16 surveillance results are due to ONC quarterly in the agreed upon template, beginning March 31, 2016. ONC will only accept electronic submissions of surveillance result via ONC-ACB@hhs.gov.

VIII. Public Accountability

ONC-ACBs should make their annual surveillance plans publicly available after submission to ONC. We believe making this information publicly available will help strengthen the overall value

[14] Health IT developers are required to cooperate with these efforts and may not prevent or seek to discourage an ONC-ACB from reporting the results of its authorized surveillance activities. We note that while the ONC Health IT Certification Program is a voluntary one, developers who choose to participate agree to comply with certification program requirements, including reporting requirements designed to ensure transparency and accountability for all participants and stakeholders. 80 FR 62601, 62718.

stakeholders will receive from the ONC Health IT Certification Program. ONC may at any time publish surveillance information to the extent permitted by law.