ONC HEALTH IT CERTIFICATION PROGRAM
Program Policy Guidance #15-01
July 16th, 2015

I.   Introduction

Program Policy Guidance #15-01 contains 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 IT they have certified.[1] Annual guidance is issued to assist ONC-ACBs in developing their annual surveillance plans, clarify required aspects of surveillance under the ONC Health IT Certification Program, and identify topics and specific elements of ONC-ACBs' surveillance that ONC considers a priority.

As outlined in greater detail below, while CY16 surveillance plans must address many of the same topics and elements as previous years, ONC-ACB CY16 surveillance plans must incorporate substantial improvements and refinements based on the ONC-ACBs' accumulated experience developing and implementing their CY14 and CY15 plans, including the feedback received from the ONC-Approved Accreditor (ONC-AA) and ONC. CY16 plans must also be revised as necessary to reflect changes to certification criteria and other program requirements adopted in the 2014 Edition Release 2 Electronic Health Record (EHR) Certification Criteria and the ONC HIT Certification Program; Regulatory Flexibilities, Improvements, and Enhanced Health Information Exchange; Final Rule" ([79 FR 54430](#)) (2014 Edition Release 2 final rule).. In addition, we have identified two new priority areas for surveillance (data portability and health IT developer product transparency) that we believe are particularly important to advance interoperability and deter information blocking. As such, ONC-ACBs must specifically address these new priority areas as part of their CY16 surveillance plans.

This guidance supplements but does not replace other surveillance plan guidance issued under the ONC Health IT Certification Program. In particular, we refer ONC-ACBs to Program Policy Guidance #13-01[2] and #14-1,[3] which clarifies many of the core requirements of surveillance under the program.[4] ONC-ACBs should also be aware of 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 Notice of proposed with comment period ([80 FR 16804](#)) (2015 Edition proposed rule), which includes several proposals that would affect ONC-ACBs' surveillance responsibilities. In the event that such proposals are finalized and ONC-ACBs' surveillance responsibilities change, we will update this guidance accordingly.

---

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

[2] Id.

[3] Program Policy Guidance #14-01 (July 2014), available at http://www.healthit.gov/sites/default/files/onc-acb_cy15annualsurveillanceguidance.pdf.

[4] See also 45 CFR Part 170; Establishment of the Permanent Certification for Health Information Technology; Final Rule, 76 FR 1262, 1281-1285 (Jan. 7, 2011).

II. Submission of Annual Surveillance Plan

ONC-ACBs must submit annual surveillance plans as required by 45 CFR 170.523(i). Annual surveillance plans must describe in sufficient detail an ONC-ACB's surveillance approach for the following calendar year. CY16 surveillance plans must be submitted to ONC by **September 30, 2015**. Extensions may be granted in limited circumstances and must be requested in writing with accompanying rationale no later than **September 15, 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 Plan Content

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 routinely and proactively conduct 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 by health care providers and staff.

A. ONC-ACB Surveillance Approach

An ONC-ACB's surveillance approach must include the assessment of whether the products (i.e., Complete EHRs and EHR Modules) it has certified continue to conform to the requirements of certification once implemented and in use "in the field" (i.e., in a production environment).[5],[6] Guidance #13-01 describes certain kinds of "reactive" surveillance that we expect ONC-ACBs to include as part of their approach. These include:

- Conducting surveillance initiated by complaints received from users of products the ONC-ACB has certified.[7]

---

[5] In-the-field surveillance is a requirement of the ONC Health IT Certification Program. We explicitly recognized this requirement in the Proposed Establishment of Certification Programs for Health Information Technology; Proposed Rule, 75 FR 11328 (Mar 10, 2010), wherein we proposed that an ONC–ACB would be required to "evaluate and reevaluate previously certified Complete EHRs and/ or EHR Modules to determine whether [they] continued to perform in an acceptable, if not the same, manner in the field as they had performed when they were certified." 75 FR 11349 (emphasis added). We later finalized this requirement in the Establishment of the Permanent Certification for Health Information Technology; Final Rule, 76 FR 1262 (Jan. 7, 2011) (hereinafter "PCP Final Rule"). Subsequently, we issued initial and annual guidance to ONC-ACBs clarifying our interpretation of the requirements for in-the-field surveillance under the ONC Health IT Certification Program, the preparation and submission of ONC-ACBs' annual surveillance plans, and the reporting of surveillance results to the National Coordinator on an annual basis. See Program Guidance #13-01, supra n.1, and Program Guidance #14-01, supra n.3.

[6] In consultation with the HHS Office for Civil Rights, we clarified that ONC-ACBs meet the definition of a "health oversight agency" under the HIPAA Privacy Rule when they conduct surveillance in accordance with the requirements of their accreditation and the ONC Health IT Certification Program rules at 45 CFR 170 Subpart E. See ONC Regulation FAQ #45 [12-13-045-1] (available at http://www.healthit.gov/policy-researchers-implementers/45-question-12-13-045).

[7] 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.

- Conducting surveillance upon the issuance of a repeated number of inherited certified status requests, with surveillance being required upon the issuance of 3 or more inherited certified status requests.
- Systematically obtaining and synthesizing feedback from users of products the ONC-ACB has certified (e.g., through various surveys/questionnaires) to determine if certain capabilities should be evaluated with the technology developer, or with health care providers and staff in the field, or both.

In addition, we expect ONC-ACBs to engage in "proactive" surveillance. For example, ONC-ACBs must explain in their surveillance plans how the ONC-ACB will proactively assess:

- Compliance with the mandatory disclosure requirements at 45 CFR 170.523(k).
- The adequacy of developers' user complaint processes.
- Appropriate use of the ONC Certification Mark.

CY16 surveillance plans must describe in detail how the ONC-ACB will address these and other aspects of surveillance for the CY16 surveillance period. Within their overall approach, ONC-ACBs must describe how they will address, at a minimum, the detailed aspects of surveillance prioritized below in section III.B.

B. CY 2016 (CY16) Proactive Surveillance Plan Elements

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.
  - 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 the entire calendar year. Because these capabilities are of substantial interest to ONC, CY16 surveillance plans must specifically address these prioritized capabilities in addition to describing an overall approach to surveillance. ONC-ACBs should refer to Guidance #13-01 for more detailed guidance regarding how prioritized capabilities should be incorporated in annual surveillance plans.

In addition to these prioritized capabilities, we consider the following elements a priority for surveillance in CY16:

- The assessment of developers' disclosures, as required by 45 CFR 170.523(k).
- 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.

IV. Submission of Annual Surveillance Results

ONC-ACBs must annually report surveillance results to the National Coordinator as required by 45 CFR 170.523(i). We expect that the procedures developed by ONC-ACBs for performing surveillance will provide health IT developers with an opportunity to give input to an ONC-ACB, where appropriate, regarding surveillance results prior to reporting the results to the National Coordinator. We strongly encourage ONC-ACBs to work with health IT developers to review and validate surveillance results prior to submission to ONC.

Guidance #13-01 describes the information we expect ONC-ACBs to document and report annually as part of their surveillance results, including information about health IT developers' complaint processes, identifying information about the products that the ONC-ACB surveilled during the surveillance period, and, where applicable, the reasons for the failure of such products to function properly. CY16 surveillance plans must provide for the accurate recordation and reporting of this information, as described more fully in Guidance #13-01.

A. Due Date and Submission Method

CY16 surveillance results are due to ONC by **February 28, 2017**. Extensions may be granted in limited circumstances and must be requested in writing with accompanying rationale no later than **February 15, 2017**. ONC will only accept electronic submissions of surveillance

results and requests for extensions. Surveillance results and requests for extensions must be submitted via ONC-ACB@hhs.gov.

V.   ONC Health IT Certification Program Transparency

ONC-ACBs should make their annual surveillance plans and surveillance results publicly available after submission to ONC. We believe making this information publicly available will help strengthen the overall value stakeholders will receive from the ONC Health IT Certification Program. We will continue to work with ONC-ACBs and the ONC-AA to mature and refine this portion of the ONC Health IT Certification Program and may issue additional guidance as necessary.