# Health IT Certification Program Overview

## 1. Introduction

The Office of the National Coordinator for Health Information Technology (ONC) operates the ONC Health IT Certification Program (Program) under the authority granted by section 3001(c)(5) of the Public Health Service Act (PHSA) and as defined in the Health Information Technology for Economic and Clinical Health (HITECH) Act. The voluntary Program is a third-party conformity assessment program for health information technology (health IT) based on the principles within the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) framework. ONC does not directly perform conformance testing or issue certifications itself. Rather, ONC collaborates with other organizations that it evaluates, approves, and authorizes to perform these functions on its behalf. The Program defines the requirements for health IT and the process by which health IT may become tested, certified, and maintain its certification.

Launched in 2010, the Program supports the Promoting Interoperability Programs (previously Medicare and Medicaid EHR Incentive Programs) administered by the Centers for Medicare & Medicaid Services (CMS). While the Promoting Interoperability Programs continue to require the use of certified health IT, the use of certified health IT has expanded to other government and non-government programs. The Program has released three editions of certification criteria and regulations for new/expanded Program requirements. These new editions of certification criteria include more robust technical and interoperability requirements, ONC-Authorized Certification Body (ONC-ACB) in-the-field surveillance expectations, and cost transparency and disclosure requirements for health IT developers' certified health IT. These additional disclosure requirements have been adopted to ensure users of certified health IT are fully informed about certain types of limitations and additional costs associated with the ability to implement or use certified health IT in a manner consistent with its certification.

The Enhanced Oversight and Accountability final rule (81 FR 72404) permits the Program to provide enhanced oversight for safety and health IT developer accountability. Specifically, the final rule stands up a focused ONC direct review regulatory framework, aligns the testing lab oversight with the existing processes for ONC-ACBs, and makes a more comprehensive set of ONC-ACB surveillance results publicly available. The rule emphasizes the importance of protecting public health and safety while also strengthening transparency and accountability in the Program. It also enables the Program to better support providers and hospitals – the vast majority of whom use health IT.

## 2. Program Participants

**ONC** works with the following agencies and entities as part of Program operations:

- **NIST** (National Institute of Standards and Technology): Per the HITECH Act, NIST, a federal agency within the Department of Commerce, and ONC collaborated to establish the voluntary certification program and continue to work together to develop the necessary functional and conformance testing requirements, test cases, and test tools in support of the Program.
- **NVLAP** (National Voluntary Laboratory Accreditation Program): Administered by NIST, the Program specifies that only test results from a NVLAP-accredited testing laboratory could be used as the basis for a certification determination by an ONC-ACB.
- **ONC-ATL** (ONC-Authorized Testing Laboratory): A NVLAP-accredited testing laboratory that performs health IT testing to determine conformance with ONC's standards and certification criteria according to the ONC-approved test method.
- **ONC-AA** (ONC-Approved Accreditor): Selected by ONC to serve a three-year term to accredit and oversee ONC-ACBs under the Program requirements.
- **ONC-ACB** (ONC-Authorized Certification Body): Certifies health IT based on test results supplied by ONC-ATLs; posts results on the Certified Health IT Product List (CHPL); and is responsible for conducting surveillance of certified health IT.
- **Health IT Developer**: Presents health IT to be tested and certified under the Program.

## 3. Policy Making, Certification Criteria, and Standards Adoption

ONC manages the rulemaking process for the development and issuance of policy and regulations for the Program. Through the rulemaking process, ONC establishes the Program requirements, capabilities, standards, and interoperability requirements for certified health IT. This process includes review and input from within the federal government as well as public and private stakeholders.

The most common rulemaking process begins with ONC issuing a notice of proposed rulemaking (NPRM) and requesting public comments on the NPRM, which is followed by a review of the comments. ONC then drafts the final rule with consideration of public comment and issues a final rule on behalf of the Department of Health and Human Services (HHS) Secretary. Through this rulemaking process, ONC establishes Program requirements as well as requirements for health IT developers and health IT, the latter which are referred to as "certification criteria." Based on these certification criteria, ONC develops a test method (to include test procedures and test tools (including associated test data)) that is approved by the National Coordinator for Health Information Technology (National Coordinator). Draft test method are available for public feedback simultaneously with the NPRM. Only test procedures and test tools approved by the National Coordinator may be used to test health IT under the Program for the purposes of certification. Test procedures and test tools developed outside ONC may be submitted to the National Coordinator, as outlined in 75 FR 36168, for review and approval.

# 4. Operations

## Program Structure

The Program's operational structure is informed by ISO/IEC 17067 and operated within the ISO framework and concepts for third-party conformity assessment programs. The requirements defined in the adopted regulations are built on these concepts and are implemented as described in this section.

ONC has collaborated with NVLAP to develop and maintain the Healthcare Information Technology Testing Laboratory Accreditation Program. NVLAP, in accordance with ISO/IEC 17025, Handbook 150 and 150-31, and other requirement documents, accredits and oversees testing laboratories that perform functional and conformance testing. Once NVLAP accredits a testing laboratory, the testing laboratory must submit to ONC an application to become an authorized testing laboratory (ONC-ATL) to begin testing health IT in the Program. ONC specifies the processes and requirements for retaining, suspending, or revoking ONC-ATL status under the Program. ONC-ATLs operate under a three-year authorization cycle and must remain in good standing by adhering to the Principles of Proper Conduct and requirements under subpart E of Part 170.

For certification of health IT under the Program, through an application process, ONC selects an ONC approved accreditor (ONC-AA) to accredit and oversee the Program's certification bodies. Similar to testing laboratory requirements, certification bodies must be accredited by the ONC-AA to ISO/IEC 17065 and the ONC-AA accreditation program requirements to perform certification activities for health IT successfully tested by an ONC-ATL. Once the ONC-AA accredits the certification body, the certification body submits an application to ONC to become an authorized certification body (ONC-ACB) to begin certifying health IT under the Program. ONC-ACBs operate under a three-year authorization cycle and must remain in good standing by adhering to the Principles of Proper Conduct and other requirements under subpart E of Part 170.

## Surveillance of Certified Health IT

Health IT certified under the Program is subject to surveillance activities as a condition of certification and a required ONC-ACB activity. Surveillance of certified health IT ensures the continued conformance of the functionalities and standards specifications required by certification. Surveillance is also a requirement set forth in ISO/IEC 17065 and must be performed by ONC-ACBs to maintain their accreditation and ONC authorization. The purpose of surveillance is to ensure that certified health IT capabilities meet certification requirements, not just in a controlled testing environment, but also when they are used "in the field" (for example, in a clinician's office or a hospital). Surveillance activities can include randomized and reactive complaint based surveillance.

When an ONC-ACB determines that a health IT module does not comply with certification requirements, the health IT module is considered non-conformant. Developers must work with their ONC-ACB on an appropriate corrective action plan (CAP) to correct the identified deficiency(ies) that led to the finding(s) of non-conformity and bring the certified health IT module(s) back into compliance. All CAPs must include certain required elements per 45 CFR § 170.556(d)(3), including:

- A description of the non-conformities or deficiencies;
- How widespread the problem may be across the developer's other customers and users;

- How the developer will address the problem for all potentially affected customers and users;
- How the developer will ensure that all potentially affected customers and users are alerted and that their issues are resolved;
- The timeframe in which all corrective action will be completed; and
- An attestation by the developer that it has completed all elements of the approved CAP.

Under ONC's 2015 Edition final rule (80 FR 62601), ONC posts an initial finding of a non-conformity and updated aspects of CAPs on the CHPL **weekly**—including the date and a description of how the non-conformity was resolved. If the developer does not resolve the non-conformity(ies) and fulfill the terms of the CAP, an ONC-ACB will follow its procedures to suspend and withdraw the certification, which may include a Certification Ban. Note that not all certified health IT modules have been surveilled. Thus, it is important for all stakeholders to ***immediately report any potential issues that may warrant surveillance to an ONC-ACB or to ONC's Health IT Feedback Form and to check the CHPL regularly for the latest information.*** Users of certified health IT should be familiar with the ONC recommended process for filing complaints concerning certified health IT.

To provide more complete information that illuminates whether certified health IT has been surveilled and continues to conform with Program requirements, ONC-ACBs are required to make "identifiable surveillance results" (those NOT resulting in a non-conformity) publicly available on the CHPL on a quarterly basis. This will further enhance transparency and provide customers and users of certified health IT with valuable information about the overall conformity of certified health IT to Program requirements.

## ONC Direct Review of Certified Health IT

The Enhanced Oversight and Accountability final rule (81 FR 72404) articulates a regulatory framework for ONC to directly review certified health IT if there is a reasonable belief that: (1) the certified health IT may present a serious risk to public health or safety; or (2) a review of certified health IT could present practical challenges for ONC-ACBs, such as when 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. This review will be complementary to surveillance conducted by ONC-ACBs and will promote health IT developer accountability for the performance, reliability, and safety of health IT.

## Certification Ban

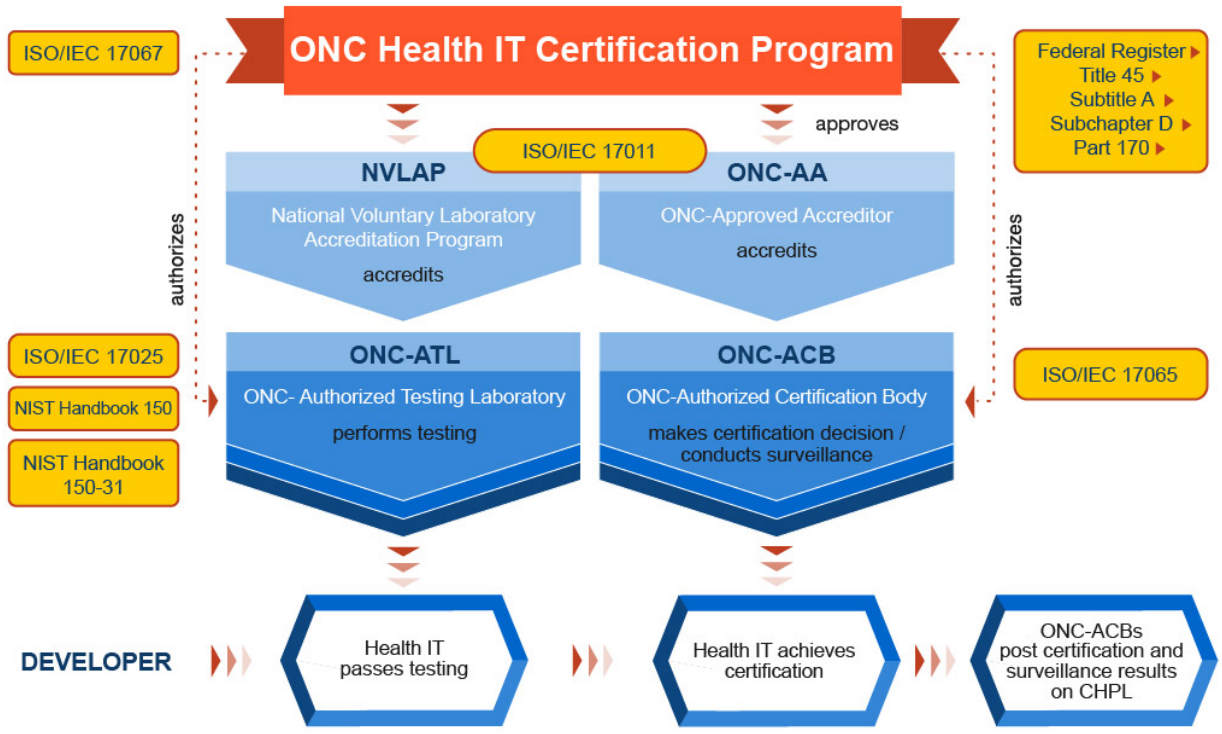
A developer of certified health IT may be prohibited from certification of health IT when one or more of the developer's certified health IT modules is:

1. Terminated by ONC under the Program;
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 under subpart C of part 170 (i.e., Certification Criteria for Health Information Technology); 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 part 170, including notice of pending surveillance.

A list of current banned developers is available on the CHPL. A health IT developer may request in writing to have a certification ban lifted. In order to do this, the developer will need to demonstrate that appropriate remediate has occurred. Further details can be found under our Certification Ban Program Guidance.

## 5. Program Structure




The labels alongside each entity are the ISO/IEC specifications to which that entity must be accredited. The Federal Register reference is the adopted regulation to which ONC operates the Program. Operation of the Program incorporates concepts within ISO/IEC 17067.

Document History

| Version | Description of Change | Date |
|---|---|---|
| **1.0** | Initial Version | September 19, 2016 |
| **1.1** | • Updated after ONC Health IT Certification Program: Enhanced Oversight and Accountability final rule published | January 30, 2016 |
| **1.2** | Updated diagram | April 3, 2017 |
| **1.3** | • Modified the name of the EHR Incentive Program to the Promoting Interoperability Program per the CY2019 IPPS Final Rule.<br>• Added link to the Health IT Feedback form.<br>• Updated links.<br>• Made multiple updates to each section to improve specificity and clarity about the Certification Program.<br>• Removed text elaborating on non-conformities that are better covered in a Health IT Buzz Blog post.<br>• Added text about the Certification Ban. | March 14, 2019 |