



# ONC Health IT Certification Program

## OVERVIEW

Last Updated February 8, 2024





|   |    |
|---|----|
| Table of Contents   |    |
| Introduction .....  | 3  |
| Program Participants.....   | 3  |
| Regulatory History.....   | 4  |
| Operations .....  | 4  |
| Program Structure .....   | 4  |
| Certified Health IT Product List (CHPL).....                      | 5  |
| Program Requirements .....  | 6  |
| Certification Criteria .....                                      | 6  |
| Standards Version Advancement Process and Standards Updates ..... | 6  |
| Conditions and Maintenance of Certification .....                 | 7  |
| Information Blocking .....  | 7  |
| Assurances .....  | 7  |
| Communications .....  | 8  |
| Application Programming Interfaces (APIs).....                    | 8  |
| Real World Testing .....  | 9  |
| Attestations .....  | 9  |
| Insights .....  | 9  |
| Surveillance of Certified Health IT .....                         | 9  |
| ONC Direct Review of Certified Health IT .....                    | 10 |
| Certification Ban .....   | 11 |





## INTRODUCTION

The Office of the National Coordinator for Health Information Technology (ONC) governs the administration of the [ONC Health IT Certification Program \(Certification Program\)](#) 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 Certification 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. Conformity assessment is a series of three functions that satisfy a need or demand for demonstration that specified requirements are fulfilled:

1. **Selection** - planning and preparation activities to collect or produce all the information and input needed for the subsequent determination function
2. **Determination** - develop complete information regarding fulfillment of the specified requirements by the object of conformity assessment or its sample
3. **Review and Attestation** –
  - Review is the final stage of checking before the decision is made as to whether the object of conformity demonstrated the specified requirements were met
  - Attestation results in a “statement” in a form that most readily reaches all the potential users

ONC does not directly perform conformance testing or issue certifications itself. Rather, ONC collaborates with other organizations that it evaluates and authorizes to perform these functions on its behalf. The Certification Program defines the requirements for health IT and the process by which health IT may become evaluated, tested (if required) and certified, and maintain its certification.

Launched in 2010, the voluntary Certification Program was established by ONC to provide for the certification of health IT and to support its availability for encouraged and required use under other federal, state, and private programs. The Centers for Medicare & Medicaid Services (CMS) [Promoting Interoperability \(PI\) Programs](#) (previously Medicare and Medicaid EHR Incentive Programs), as an example, requires the use of health IT certified under the Certification Program. Throughout the evolution of the Certification Program, ONC has released multiple editions of certification criteria and regulations for new and expanded Certification Program requirements.

This overview provides summary information to offer a general understanding of the Certification Program structure, requirements, and operations. Where additional information is available in supplementary resources, links to those materials will be provided for further review.

## PROGRAM PARTICIPANTS

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

**National Institute of Standards and Technology (NIST):** 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 Certification Program.

**National Voluntary Laboratory Accreditation Program (NVLAP):** Administered by NIST, accredits testing laboratories as a requirement for ONC authorization to perform testing under the Certification Program.

**Accreditation Body:** Accredits certification bodies as a requirement for ONC authorization to perform





certification activities under the Certification Program. Certification Bodies may choose any Accreditation Body, with an appropriate scope, that is a signatory of the Multilateral Recognition Arrangement (MLA) with the International Accreditation Forum (IAF) to become accredited.

**ONC-Authorized Testing Laboratory (ONC-ATL):** A NVLAP-accredited testing laboratory that has been authorized by ONC to perform health IT testing to determine conformance with ONC's standards and certification criteria according to the [ONC-approved test method](#). Successfully tested products can be submitted to an ONC-ACB for certification.

**ONC Authorized Certification Body (ONC-ACB):** Certifies health IT based on information gathered and provided by ONC- ATLS that demonstrates fulfillment of the specified requirements for certification. ONC-ACBs provide ONC with a current list of certified health IT on a weekly basis, including relevant information associated with the certified health IT required for reporting, on the [Certified Health IT Product List \(CHPL\)](#). ONC-ACBs are also responsible for conducting ongoing oversight and surveillance of certified health IT.

**Health IT Developer:** Presents health IT products to ONC-ATL to be tested. Once the developer's product satisfies all applicable certification requirements, the developer then contacts an ONC-ACB to have their product certified.

## REGULATORY HISTORY

ONC manages the rulemaking process for the development and issuance of policy and regulations for the Certification Program. Through the rulemaking process, ONC establishes the Certification Program requirements, capabilities, standards, and interoperability requirements for certified health IT. This process begins with ONC issuing a notice of proposed rulemaking (NPRM) and a request for public comments and is followed by ONC's review and response to this input. 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 Certification 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 conformance 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 conformance methods are made available for public feedback simultaneously with the NPRM. Only test procedures, test tools, and conformance methods approved by the national coordinator may be used to test and evaluate health IT under the Certification 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 as alternative test methods for the Certification Program](#). Please refer to [Certification Standards and Regulations page](#) for information on specific rules that have informed the Certification Program.

## OPERATIONS

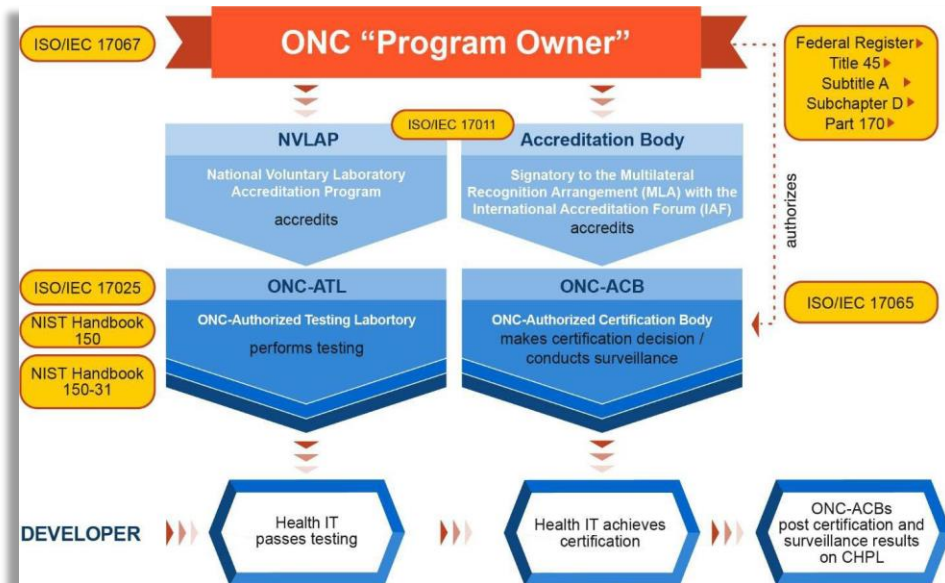
### Program Structure

The Certification 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](#), [Handbook 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 ONC-ATL to begin testing health IT in the Certification Program. ONC specifies the processes and requirements for retaining, suspending, or revoking ONC-ATL status under the Certification 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 Certification Program, similar to testing laboratory requirements, certification bodies must provide documentation, with an appropriate scope, that confirms that the applicant has been accredited to [ISO/IEC 17065](#) by any accreditation body that is a signatory to the Multilateral Recognition Arrangement (MLA) with the International Accreditation Forum (IAF). The certification body provides this documentation when it submits an application to ONC to become an ONC-ACB to begin certifying health IT under the Certification 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](#). To renew its status, an ONC-ACB is required to submit a renewal request, which contains any updates to the information requested in the initial application to the National Coordinator, 60 days prior to the expiration of its status.

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 Certification Program. Operation of the Certification Program incorporates concepts within ISO/IEC 17067.

### Certified Health IT Product List (CHPL)

The CHPL provides an authoritative, comprehensive listing of Health IT Modules that have been tested and certified through the Certification Program. The CHPL is updated, at minimum, once per week.

**CHPL**  
Explore information on certified products and developers.

Each Certified Health IT Module on the CHPL has a “CHPL Product Number” assigned to it by the ONC- ACB that certified the product. The CHPL also generates the CMS EHR Certification Identification Number that represents a Health IT Module or combination of Health IT Modules, which are used for reporting to the PI Programs. Additional details on each product including criteria to which it certifies, certification status, mandatory disclosures and compliance activities can be found on specific product pages. [Step-by-step instructions](#) for navigating CHPL and obtaining a CMS EHR Certification ID are available on the [CHPL website](#).



## PROGRAM REQUIREMENTS

ONC establishes the program requirements which include HHS adoption of standards, implementation specifications, and certification criteria for health IT, often referred to as “certification criteria.” Other Certification Program requirements address ONC-ATL and ONC-ACB responsibilities, developer reporting and disclosures requirements, and ONC enhanced oversight. In addition, the ONC Cures Act Final Rule established seven Conditions of Certification with accompanying Maintenance of Certification requirements for health IT developers.

### Certification Criteria

The Certification Program is composed of functional requirements known as “certification criteria.” ONC defines certification criteria for health IT through regulation and publishes conformance methods to provide procedural steps for evaluating conformance with these criteria. Developers certify their Health IT Modules by demonstrating conformance to these criteria, using conformance methods (that may have associated testing, test tools and/or test data) approved by the National Coordinator. Additionally, ONC provides clarifications to certification criteria through Certification Companion Guides (CCG) designed to assist with health IT product development.

#### [ONC Certification Criteria for Health IT](#)

Explore all criteria and their associated requirements and conformance methods.

### Standards Version Advancement Process and Standards Updates

The Standards Version Advancement Process (SVAP) allows developers to update their Certified Health IT Modules to use more advanced versions of standards and implementation specifications than the version(s) incorporated by reference in the regulation for the certification criteria, provided such versions are approved by the national coordinator for use in health IT certified under the Certification Program. All Certified Health IT developers voluntarily opting to avail themselves of the SVAP flexibility must ensure that their annual Real World Testing plans and Real World Testing results submissions address all the versions of all the standards and implementation specifications to which each Health IT Module is certified.

A deeper dive into requirements and timelines related to [Standards Version Advancement Process \(SVAP\)](#).

In addition to SVAP, the Certification Program addresses situations when a voluntary consensus standards organization issues a correction to a standard or implementation specification included in the Certification Program. In the event that the adopted version of the standard or implementation specification is corrected by a voluntary consensus standards organization (or steward) after it has been adopted by ONC in a final rule, ONC follows a specific approach to determine whether, even if not yet formally adopted by the Secretary, the correction(s) should be incorporated into the testing, certification, and surveillance of health IT to the adopted standard or implementation specification.

In general, ONC reviews corrections to the length, data type, data type descriptions, usage, cardinality and/or value sets for various message elements, as well as corrections to conformance statements where they were mistakenly omitted or not clearly specified by the author of the standard or implementation specification. Each of these examples of corrections, if not implemented by the health IT industry, could lead to interoperability errors as well as the inconsistent implementation of the standard or implementation specification, which may impede electronic health information exchange.

If ONC determines that a correction(s) creates the concern described above, ONC will update the appropriate Certification Companion Guide(s) (CCG) to incorporate the correction and provide an interpretative explanation. These CCG notations will include a 90-day delayed effective date for the use of



the correction(s) in testing and certification. ONC expects already certified health IT to include any such identified correction(s) without the need for further testing and certification under the Certification Program. For the purposes of surveillance, there will be an 18-month delayed effective date from the CCG notations before a finding of an identified correction's absence during surveillance would constitute a non-conformity under the Certification Program.

## CONDITIONS AND MAINTENANCE OF CERTIFICATION

The 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule (ONC Cures Act Final Rule) (85 FR 25642) adopted new Certification Program requirements, including the introduction of the Conditions and Maintenance of Certification suite of requirements. \

The Conditions and Maintenance of Certification requirements express initial requirements and ongoing requirements for health IT developers and their Certified Health IT Module(s). The Conditions and Maintenance of Certification requirements, except for the Information Blocking and Assurances Conditions and Maintenance of Certification requirements, apply only to actions and behaviors of health IT developers related to their certified health IT as well as to the certified health IT itself. The Information Blocking and Assurances Conditions and Maintenance of Certification require that a health IT developer be responsible to ensure that all of its health IT and related actions and behaviors do not constitute information blocking or inhibit the appropriate access, exchange, and use of electronic health information (EHI).

### Information Blocking

This requirement prohibits any Certified Health IT developer with at least one health IT product certified under the Certification Program from taking any action that constitutes information blocking as defined by section 3022(a) of the PHSA and codified in 45 CFR 171.103. ONC outlines eight categories of exemptions where reasonable and necessary activities would not be considered information blocking.

**Companion Resource:**  
[Information Blocking  
Fact Sheet](#)

If a developer is found to have committed information blocking, it may be subject to termination of their Health IT Module(s)' certification, a certification ban, and subject to civil monetary penalties.

### Assurances

This requirement outlines that Certified Health IT developers must provide assurances that:

- they will not take any actions that constitutes information blocking or may inhibit the appropriate exchange, access and use of EHI;
- they are in full compliance with and unrestricted implementation of certification criteria capabilities;
- they did not take any action to interfere with a user's ability to access or use certified capabilities;
- their Certified Health IT Module, as part of a health IT product that electronically stores EHI, is certified to § 170.315(b)(10) criterion; and
- must not inhibit its customer's timely access to interoperable health IT certified under the Program.

As part of efforts to maintain their certification, developers must:





- retain all records and information necessary to demonstrate initial and ongoing compliance with Certification Program requirements for a period of 10 years beginning from the date of certification or a period of three years from the effective date that removes criteria from the Code of Federal Regulations;
- within, on and after December 31, 2023, if they meet applicable requirements, they must provide all customers with health IT certified to § 170.315(b)(10) criterion; and
- must update certified Health IT Modules to all applicable revised criteria and provide those updates to their customers by the timeframes outlined in regulation.

## Communications

This requirement prevents Health IT developers from prohibiting or restricting communications about certain aspects of the performance of health IT and related business practices. Health IT developers are able to impose certain types of limited prohibitions and restrictions that strike a balance between the need to promote open communication about health IT with the need to protect the legitimate business interests of Health IT developers and others.

## Application Programming Interfaces (APIs)

Developers with Health IT Modules certified to any certification criteria in § 170.315(g)(7) through (g)(10) must:

- publish APIs and allow health information from such technology to be accessed, exchanged, and used without special effort;
- publish complete business and technical documentation, via a publicly accessible hyperlink;
- publish all terms and conditions for its certified API technology including material information and API Fees;
- abide by permitted/prohibited API fees and keep for inspection detailed records of any fees charged with respect to the certified API technology; and
- abide by openness and pro-competitive conditions.

**Companion Resource:**  
[API Resource Guide](#)

As part of their API Maintenance of Certification requirements at § 170.404, developers with Health IT Modules certified to § 170.315(g)(10) specifically must:

- follow requirements for authenticity verification and registration for production use; and
- by December 31, 2024, publish, at no charge, the service base URLs and related organization details in a standard FHIR format that can be used by patients to access their EHI.





## Real World Testing

As a Condition and Maintenance of Certification requirement, Certified Health IT Developers must successfully test the real-world use of health IT for interoperability in the type(s) of setting(s) in which such technology would be marketed. To meet the requirements, developers must submit publicly available annual Real World Testing plans, as well as annual Real World Testing results reports for health IT certified to certain criteria. All Certified Health IT developers voluntarily opting to use the SVAP flexibility must ensure that their annual Real World Testing plans and Real World Testing results submissions address all the versions of all the standards and implementation specifications to which each Health IT Module is certified.

**Companion Resource:**  
[Real World Testing](#)

ONC-ACBs must review and confirm that each developer with one or more Health IT Module(s) certified to any of the required criteria submits Real World Testing plans and Real World Testing results in a timeframe that allows for the ONC-ACB to confirm completeness of all plans and results reports by the applicable annual due dates.

## Attestations

The health IT developer must attest compliance with the Conditions and Maintenance of Certification requirements twice a year for purposes of compliance with the Certification Program.

## Insights

Previously referred to as the EHR Reporting Program, the Insights Condition aims to provide transparent reporting on certified health IT in the categories of interoperability, usability and user-centered design, security, conformance to certification testing, and more.

As part of their Insights Maintenance of Certification requirements at § 170.407, Certified Health IT developers must submit responses to reporting criteria outlined by ONC in order to address information gaps in the health IT marketplace and provide insights on the use of health IT. Developers must report on the following measures as applicable to their Health IT Module's capabilities:

- Individuals' access to electronic health information
- C-CDA problems, medications, and allergies reconciliation and incorporation using certified health IT
- Applications supported through certified health IT
- Use of FHIR in apps supported by certified APY technology
- Use of FHIR bulk data access through certified health IT
- Immunization administrations electronically submitted to an immunization information system through certified health IT
- Immunization history and forecasts through certified health IT

## SURVEILLANCE OF CERTIFIED HEALTH IT

Certified health IT is subject to surveillance activities carried out by ONC-ACBs. 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 continues to meet certification requirements, post-certification. [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\(d\)\(3\)](#).

Under the 2015 Edition Final Rule ([80 FR 62601](#)), ONC requires ONC-ACBs post an initial finding of a non-conformity and updated aspects of CAPs on the CHPL weekly including the date the CAP was accepted by the ONC-ACB, the date the CAP was completed, 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/or withdraw the certification, which may include a [certification ban](#) ([80 FR 62601](#)). 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 and Inquiry Portal](#) and to check the CHPL regularly for the latest information. Users should be familiar with the ONC [recommended process](#) for filing complaints concerning their certified health IT products.

**Note:** Stakeholders should immediately report any potential issues with a developer or certified product to an ONC-ACB or to ONC's [Health IT Feedback and Inquiry Portal](#) and to check the CHPL regularly for the latest information.

To provide more complete information that illuminates whether certified health IT has been surveilled and continues to conform with Certification 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 Certification Program requirements.

## ONC DIRECT REVIEW OF CERTIFIED HEALTH IT

The ONC Health IT Certification Program: Enhanced Oversight and Accountability Final Rule (EOA Final Rule) (81 FR 72404) permits the Certification Program to provide enhanced oversight for safety and health IT developer accountability. Specifically, the final rule establishes a focused ONC Direct Review regulatory framework, aligns the testing lab oversight with the existing processes for ONC Authorized Certification Bodies (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 Certification Program. It also enables the Certification Program to better support providers and hospitals – the vast majority of whom use health IT.



The EOA Final Rule establishes 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 Certified Health IT developer accountability for the performance, reliability, and safety of health IT. If Direct Review is initiated, ONC will work with developers to correct the non-conformity by way of a Corrective Action Plan. ONC could take more serious steps of suspending or terminating the affected certification(s), and/or issuing a certification ban to the Certified Health IT developer if identified issues are not corrected.

### Certification 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 Health IT Modules is:

- 1) Terminated by ONC under the Certification Program;
- 2) Withdrawn by an ONC-ACB because the Certified Health IT developer requested it to be withdrawn when the 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 Certified Health IT developer requested it to be withdrawn when the 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 certification ban may also be determined as appropriate by ONC if a Direct Review determines that a developer has not complied with a Condition or Maintenance of Certification requirement.

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 remediation has occurred.

**Companion Resources:**  
[ONC Direct Review Fact Sheet](#)  
[Certification Ban Program](#)  
[Guidance](#)

