PRIVACY AND SECURITY

CERTIFICATION COMPANION GUIDE

(Version 4.0; Last updated: February 20, 2025)

This certification companion guide (CCG) provides clarifications for the privacy and security certification framework. Guidance specific to an individual privacy and security criterion is provided in the respective CCG for that criterion.

Privacy and Security Certification Criteria
§ 170.315(d)(1) Authentication, access control, authorization
§ 170.315(d)(2) Auditable events and tamper-resistance
§ 170.315(d)(3) Audit report(s)
§ 170.315(d)(4) Amendments
§ 170.315(d)(5) Automatic access time-out
§ 170.315(d)(6) Emergency access
§ 170.315(d)(7) End-user device encryption
§ 170.315(d)(8) Integrity
§ 170.315(d)(9) Trusted connection
§ 170.315(d)(10) Auditing actions on health information
§ 170.315(d)(11) Accounting of disclosures
§ 170.315(d)(12) Encrypt authentication credentials
§ 170.315(d)(13) Multi-factor authentication

The ONC Health IT Certification Program (Certification Program) specifies at 45 CFR 170.550(h) the privacy and security certification framework for Health IT Modules. Section 170.550(h) identifies a mandatory minimum set of the certification criteria that ONC-Authorized Certification Bodies (ONC-ACBs) must ensure are also included as part of specific Health IT Modules that are presented for certification.

Certification Requirements

Under the Certification Program, a Health IT Module presented for certification must be tested to a mandatory minimum set of identified privacy and security certification criteria for an ONC-ACB to issue the Health IT Module a certification.

ASTP/ONC permits Certified Health IT developers to use one of two approaches to demonstrate conformance to the privacy and security certification criteria:

- **Approach 1:** The Health IT Module technically demonstrates the privacy and security certification criteria during testing.

- **Approach 2:** For each applicable privacy and security certification criterion not certified using Approach 1, the Certified Health IT Developer submits system documentation that is sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces for each applicable privacy and security certification criterion that enable the Health IT Module to access external services necessary to meet the requirements of the privacy and security certification criterion.

Regulation Text

§ 170.550(h) *Privacy and security certification framework—*

1) *General rule.* When certifying a Health IT Module to the ONC Certification Criteria for Health IT, an ONC–ACB can only issue a certification to a Health IT Module if the privacy and security certification criteria in paragraphs (h)(3)(i) through (ix) of this section have also been met (and are included within the scope of the certification).
2) *Testing*. In order to be issued a certification, a Health IT Module would only need to be tested once to each applicable privacy and security criterion in paragraphs (h)(3)(i) through (ix) of this section so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification, except for the following:
    (i) A Health IT Module presented for certification to § 170.315(e)(1) must be separately tested to § 170.315(d)(9); and
    (ii) A Health IT Module presented for certification to § 170.315(e)(2) must be separately tested to § 170.315(d)(9).
3) *Applicability*.
    (i) Section 170.315(a)(1) through (3), (5), (12), (14) and (15) are also certified to the certification criteria specified in § 170.315(d)(1) through (7), d(12) and (d)(13).
    (ii) Section 170.315(a)(4), (10) and (13) and, on and after January 1, 2028, (b)(11), are also certified to the certification criteria specified in § 170.315(d)(1) through (3), and (d)(5) through (7), and d(12), and, for the time period up to and including December 31, 2027, (d)(13);
    (iii) Section 170.315(b)(1) through (b)(3) and (6) through (9) are also certified to the certification criteria specified in § 170.315(d)(1) through (3) and (d)(5) through (8), (12) and (13);
    (iv) Section 170.315(c) is also certified to the certification criteria specified in § 170.315(d)(1) (d)(2)(i)(A), (B), (d)(2)(ii) through (v), (d)(3), (5), (12) and (13);
    (v) Section 170.315(e)(1) is also certified to the certification criteria specified in § 170.315(d)(1) through (3), (5), (7), (9), (12) and (13);
    (vi) Section 170.315(e)(2) and (3) is also certified to the certification criteria specified in § 170.315(d)(1), (d)(2)(i)(A), (B), (d)(2)(ii) through (v), (d)(3), (5), (9), (12) and (13); Section 170.315(f) is also certified to the certification criteria specified in § 170.315(d)(1) through (3), (7), (12) and (13);
    (vii) Section 170.315(g)(7) through (10) is also certified to the certification criteria specified in § 170.315(d)(1), (9), (12) and (13); and (d)(2)(i)(A) and (B), (d)(2)(ii) through (v), or (10);
    (viii) Section 170.315(h) is also certified to the certification criteria specified in § 170.315(d)(1), (d)(2)(i)(A), (B), (d)(2)(ii) through (v), (d) (3), (12) and (13); and

4) *Methods to demonstrate compliance with each privacy and security criterion*. One of the following methods must be used to meet each applicable privacy and security criterion listed in paragraph (h)(3) of this section:
   (i) Directly, by demonstrating a technical capability to satisfy the applicable certification criterion or certification criteria; or
   (ii) Demonstrate, through system documentation sufficiently detailed to enable integration, that the Health IT Module has implemented service interfaces for each applicable privacy and security certification criterion that enable the Health IT Module to access external services necessary to meet the privacy and security certification criterion.

§ 170.550(h)(2) Testing

Technical outcome – In order to be issued a certification, a Health IT Module would only need to be tested once to each applicable privacy and security criterion.

Clarifications:

- ONC-ACBs must ensure before they issue a certificate that the scope includes the appropriate "(d) criteria" (i.e., 45 CFR § 170.315(d)(1) through (13)) based on the other letter paragraphs in scope (e.g., (a), (b)). The regulation is silent as to what capabilities the (d) certification criteria are associated with during *testing*, so long as the ultimate scope of a certification requested by a developer includes the (d) criteria associated with the other criteria included in the certification. [See also 80 FR 25710]
- Except for § 170.315(e)(1) View, download and transmit (VDT) to 3rd party, and (e)(2) Secure messaging, (d) criteria are NOT required to be repetitively applied to each separate letter paragraph, as long as the Certified Health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification. For example, if a developer demonstrates (d)(1) through (d)(7), (d)(12) and (d)(13) during testing for the paragraph (a)(1) through (3), (5), (12), (14) and (15) criteria, the developer does NOT have to separately demonstrate those same (d) criteria for an (f) capability, because the required (d) criteria associated with the (f) capabilities are included within those required for certification to the (a) capabilities.
- For Health IT Modules certifying to § 170.315(e)(1) VDT to 3rd party and (e)(2) Secure messaging, a Health IT Module must be separately tested for each criterion to § 170.315(d)(9) because of the specific capabilities for secure electronic transmission and secure electronic messaging included in each criterion, respectively. [See also 80 FR 25710]
- Certification can proceed for the audit log process without the Health IT Module demonstrating that it can record an encryption status in accordance with § 170.315(d)(2)(i)(C). Paragraph § 170.315(d)(2)(i)(C) is not applicable for the privacy and security testing and certification of a Health IT Module required by §170.550(h)(3)(iii), (v), (vii), and (viii). [See also 80 FR 25710]
- Health IT Modules presented for certification do not have to demonstrate the capabilities required by the certification criterion, §170.315(d)(4) Amendments, unless the Health IT Module is presenting for certification to another criterion that requires certification to the "Amendments" criterion under the privacy and security certification framework. [See also 80 FR 25709]

§ 170.550(h)(3) Applicability

Clarifications:

- Only the privacy and security criteria and the criteria specified in § 170.315(b)(10) and (g)(1) through (6) are completely exempt from the privacy and security certification framework. [See also 80 FR 25709]
- § 170.550(h)(3)(ii) includes reference to an expiring requirement for the certification to § 170.315(d)(13). This inclusion was related to a revision to the (d)(13) criterion in the HTI-2 Proposed Rule that was not included in the HTI-2 Final Rule that went into effect on January 15, 2025. ASTP expects a correction to be issued in the future to remove this expiration from the applicability requirements outlined in this section.

§ 170.550(h)(4)(ii) Methods to demonstrate compliance

Technical outcome – "Approach 2" demonstration through system documentation

Clarifications:

- Under Approach 2, Certified Health IT developers may submit documentation that demonstrates that the Health IT Module has implemented service interfaces for each applicable privacy and security criterion to enable the Health IT Module to access external services necessary to meet the privacy and security requirements. For these purposes, the term "access" includes as applicable, bi-directional interfaces with external services. For example, system documentation could detail how integration establishes a bi-directional interface that meets the requirements of the § 170.315(d)(3) "Audit report(s)" certification criterion. [See also 80 FR 76870]
- External services simply mean services outside the scope of the capabilities within the Health IT Module being presented for certification. External services could be, but are not limited to, those provided by another certified Health IT Module, another software program such as Microsoft Active Directory, or a hospital enterprise-wide infrastructure. [See also 80 FR 76870]
- A Health IT Module is not required to be paired with the other services for the purposes of certification (e.g., a Health IT Module does not have to seek certification with another Certified Health IT Module that performs the privacy and security capability or specify the external services as "relied upon software"). [See also 80 FR 76870]
- System documentation may consist of "screenshots" illustrating integration with external services necessary to meet the applicable privacy and security criteria. However, this approach of demonstrating implementation is not required. Rather, only a clear description of how the external services necessary to meet the applicable privacy and security criteria would be deployed and used is necessary for the purposes of testing and certification. [See also 80 FR 62707]

Note: This Certification Companion Guide (CCG) is an informative document designed to assist with health IT product certification. The CCG is not a substitute for the requirements outlined in regulation and related ASTP/ONC final rules. It extracts key portions of ASTP/ONC final rules' preambles and includes subsequent clarifying interpretations. To access the full context of regulatory intent please consult the Certification Regulations page for links to all ASTP/ONC final rules or consult other regulatory references as noted. The CCG is for public use and should not be sold or redistributed.

Revision History

Version #	Description of Change	Version Date
1.0	Initial Publication	July 7, 2017
1.1	Clarification of system documentation requirements for testing and certification under Approach 2.	August 25, 2017
1.2	Removed table columns regarding Certified EHR Technology Definition and Associated EHR Incentive Program Objective(s). Added text indicating when the P&S framework applies to the Base EHR definition and CMS objectives or measures.	December 31, 2019
2.0	Cures Update–Updated the Regulation Text; Removed the column indicating the Gap Certification. This is now part of each of the individual criterion. Modified the Security Criteria comparisons to indicate updates from the 2015 Edition. Added clarifications for § 170.550(h)(2) per the ONC Cures Act Final Rule Addition.	June 16, 2020
3.0	Updated to remove reference to 2015 Cures Act Final Rule	May 7, 2024
4.0	Updated to reflect addition of § 170.315(b)(11) to applicable criteria as outlined in the HTI-2 Final Rule and offer clarification on changes to § 170.550(h)(3) as outlined in that rule.	February 20, 2025