2015 Edition Certification Companion Guide

Privacy and Security

Version 1.1 – Last Updated 8/25/2017

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.

Regulation Text Citation	New/Revised/Unchanged Compared to 2014 Edition	Gap Certification Eligible	Certified EHR Technology Definition	Associated EHR Incentive Program Objective(s)
§ 170.315(d)(1)	Revised	No	Not Included	N/A
§ 170.315(d)(2)	Revised	No	Not Included	N/A
§ 170.315(d)(3)	Revised	No	Not Included	N/A
§ 170.315(d)(4)	Unchanged	Yes	Not Included	N/A
§ 170.315(d)(5)	Unchanged	Yes	Not Included	N/A
§ 170.315(d)(6)	Unchanged	Yes	Not Included	N/A
§ 170.315(d)(7)	Unchanged	Yes	Not Included	N/A
§ 170.315(d)(8)	Revised	No	Not Included	N/A
§ 170.315(d)(9)	New	No	Not Included	N/A
§ 170.315(d)(10)	New	No	Not Included	N/A
§ 170.315(d)(11)	Unchanged	Yes	Not Included	N/A

The 2015 Edition includes a new approach to the certification of health IT for applicable privacy and security (P&S) capabilities as compared to the 2014 Edition.

Certification Requirements

Under the ONC Health IT Certification Program, a Health IT Module presented for certification to the 2015 Edition must be tested to a mandatory minimum set of identified P&S certification criteria in order for an ONC-Authorized Certification Body (ONC-ACB) to issue the Health IT Module a certification. The 2015 Edition permits health IT developers to use one of two approaches to demonstrate conformance to the P&S certification criteria:

- Approach 1: The Health IT Module technically demonstrates the P&S certification criteria during testing.
- Approach 2: For each applicable P&S certification criterion not certified using Approach 1, the 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 P&S certification criterion that enable the Health IT Module to access external services necessary to meet the requirements of the P&S certification criterion.

Regulation Text

(h) *Privacy and security certification framework— (1) General rule.*

When certifying a Health IT Module to the 2015 Edition health IT certification criteria, 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 (viii) of this section have also been met (and are included within the scope of the certification).

(2) 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 (viii) 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) is also certified to the certification criteria specified in § 170.315(d)(1) through (7);

(ii) Section 170.315(b) is also certified to the certification criteria specified in § 170.315(d)(1) through (3) and (d)(5) through (8);

(iii) Section 170.315(c) is also certified to the certification criteria specified in § 170.315(d)(1) through (3), and (5);

(iv) Section 170.315(e)(1) is also certified to the certification criteria specified in § 170.315(d)(1) through (3), (5), (7), and (9);

(v) Section 170.315(e)(2) and (3) is also certified to the certification criteria specified in § 170.315(d)(1) through (3), (5), and (9);

(vi) Section 170.315(f) is also certified to the certification criteria specified in § 170.315(d)(1) through (3) and (7);

(vii) Section 170.315(g)(7), (8) and (9) is also certified to the certification criteria specified in § 170.315(d)(1) and (9); and (d)(2) or (10);

(viii) Section 170.315(h) is also certified to the certification criteria specified in § 170.315(d)(1) through (3); 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.

Criterion Subparagraph	Technical Explanations and Clarifications	Standard(s) Referenced
§ 170.550(h)(2)	• 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 ***Clarification:*** • ONC-ACBs must ensure that before they issue a certificate the scope includes the appropriate "(d) criteria" (i.e., 45 CFR 170.315(d)(1) through (11)) 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 62706]. • With the exception of § 170.315(e)(1) "VDT" and (e)(2) "secure messaging,"(d) criteria are *NOT* required to be repetitively applied to each separate letter paragraph, as long as the health IT developer attests that such P&S capabilities apply to the full scope of capabilities included in the requested certification. For example, if a developer demonstrates (d)(1) through (d)(7) during testing for the paragraph (a) 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" 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 62707].	
§ 170.550(h)(3)	• Technical outcome – Applicability ***Clarifications:*** • Only the P&S criteria and the criteria specified in § 170.315(g)(1) through (6) are completely exempt from the P&S certification framework [see also 80 FR 62706].	

Criterion Subparagraph	Technical Explanations and Clarifications	Standard(s) Referenced
§ 170.550(h)(4)(ii)	• Technical outcome – "Approach 2" demonstration through system documentation ***Clarifications:*** • 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 2015 Edition "audit report(s)" certification criterion [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 [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 P&S capability or specify the external services as "relied upon software") [80 FR 76870]. • System documentation may consist of "screenshots" illustrating integration with external services necessary to meet the applicable P&S 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 P&S criteria would be deployed and used is necessary for the purposes of testing and certification [80 FR 62707].	

Version History

Version #	Change(s) Summary	Date Made
1.0	Initial Publication	Jul 7, 2017
1.1	Clarification of system documentation requirements for testing and certification under Approach 2.	Aug 25, 2017