

2015 Edition Certification Companion Guide

Secure Messaging - 45 CFR 170.315(e)(2)

Links will be updated as available: [Final Rule Preamble](#) – [Test Procedure](#) – [MU Specification Sheet](#)

Version 1.1 – Last Updated 1/5/2016

New/Revised/Unchanged Compared to 2014 Edition	Gap Certification Eligible	Base EHR Definition	In Scope for Certified EHR Technology Definition	Associated EHR Incentive Program Objective(s)
Revised	No	No	Yes	Objective 6

Certification Requirements

Privacy and Security: This certification criterion was adopted at § 170.315(e)(2). As a result, an ONC-ACB must ensure that a product presented for certification to a § 170.315(e) “paragraph (e)” criterion includes the privacy and security criteria (adopted in § 170.315(d)) within the overall scope of the certificate issued to the product.

- The privacy and security criteria (adopted in § 170.315(d)) do not need to be explicitly tested with this specific paragraph (e) criterion unless it is the only criterion for which certification is requested.
- As a general rule, a product presented for certification only needs to be tested once to each applicable privacy and security criterion (adopted in § 170.315(d)) 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. However, exceptions exist for § 170.315(e)(1) “VDT” and (e)(2) “secure messaging,” which are explicitly stated.

Design and Performance: The following design and performance certification criteria (adopted in § 170.315(g)) must also be certified in order for the product to be certified.

- When a single quality management system (QMS) is used, the QMS only needs to be identified once. Otherwise, the QMS’ need to be identified for every capability to which it was applied.
- When a single accessibility-centered design standard is used, the standard only needs to be identified once. Otherwise, the accessibility-centered design standards need to be identified for every capability to which they were applied; or, alternatively the developer must state that no accessibility-centered design was used.

Privacy and Security (§ 170.315(d))	Design and Performance (§ 170.315(g))
<ul style="list-style-type: none"> • If choosing Approach 1: <ul style="list-style-type: none"> ○ Authentication, access control, and authorization (§ 170.315(d)(1)) ○ Auditable events and tamper-resistance (§ 170.315(d)(2)) ○ Audit reports (§ 170.315(d)(3)) ○ Automatic access time-out (§ 170.315(d)(5)) ○ Trusted Connection (§ 170.315(d)(9)) must be explicitly demonstrated with this criterion. • If choosing Approach 2: <ul style="list-style-type: none"> ○ For each applicable P&S certification criterion not certified for approach 1, the health IT developer may certify for the criterion (with the exception of (§ 170.315(d)(9)) using system documentation which provides a clear description of how the external services necessary to meet the P&S criteria would be deployed and used. Please see the 2015 Edition final rule correction notice at 80 FR 76870 for additional clarification. 	<ul style="list-style-type: none"> • Quality management system (§ 170.315(g)(4)) • Accessibility-centered design (§ 170.315(g)(5))

Regulation Text

Secure messaging.

(i) Enable a user to send messages to, and receive messages from, a patient in a secure manner.

Criterion Subparagraph	Technical Explanations and Clarifications	Standard(s) Referenced
Applies to entire criterion	<p>Technical outcome – A user can send messages to, and receive messages from a patient in a secure manner.</p> <p>Clarifications:</p> <ul style="list-style-type: none"> • A Health IT Module presented for certification to this criterion <u>must</u> be separately tested to the privacy and security criterion for <u>“trusted connection” at § 170.315(d)(9)</u>. [see also 80 FR 62707] • A health IT developer can choose between message-level or transport-level “trusted connection” certification in accordance with § 170.315(d)(9). [see also 80 FR 62661] • The encryption requirements of this certification criterion <u>only apply to the message content</u> and not to the patient’s device(s). [see also 80 FR 62661] • This criterion is <u>not</u> eligible for gap certification as the new hashing standard (a hashing algorithm with a security strength equal to or greater than SHA-2) applies to this criterion per the standard required at § 170.210(c)(2). [see also 80 FR 62661]. • Secure email, a secure portal, even some type of mobile application could all be examples for secure messaging methods that could potentially meet this certification criterion. [see also 77 FR 54193] • We will test that the health IT has the capability as a whole to <u>send and receive</u> secure messages for certification in order for providers to have assurance that health IT can enable bidirectional communication. [see also 77 FR 54194] • As noted in Annex A: FIPS 140-2, only encryption and hashing algorithms are in scope for this certification criterion. Random number generator standards are not in scope. [see also 77 FR 54194] 	<p>Standards required for § 170.315(d)(9) Trusted connection:</p> <p>170.210(a)(2) Annex A: Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, October 8, 2014</p> <p>170.210(c)(2) FIPS PUB 180-4, Secure Hash Standard, 180-4 (August 2015)</p>

Note: This Certification Companion Guide (CCG) is an informative document designed to assist with health IT product development. The CCG is not a substitute for the 2015 Edition final regulation. It extracts key portions of the rule’s preamble and includes subsequent clarifying interpretations. To access the full context of regulatory intent please consult the 2015 Edition final rule or other included regulatory reference. The CCG is for public use and should not be sold or redistributed.

Version History

Version #	Change(s) Summary	Date Made
1.0	Initial Publication	Oct 22, 2015
1.1	Revised to indicate this certification criterion is in scope for the Certified EHR Definition.	Jan 5, 2016