

2015 Edition Certification Companion Guide

Trusted Connection - 45 CFR 170.315(d)(9)

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

Version 1.1 – Last Updated 1/29/2016

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)
New	No	No	No	N/A

This certification criterion at § 170.315(d)(9) is required as part of the 2015 Edition privacy & security approach for the certification criteria at § [170.315\(e\)\(1\)](#), [\(e\)\(2\)](#), [\(e\)\(3\)](#), [\(g\)\(7\)](#), [\(g\)\(8\)](#), and [\(g\)\(9\)](#). This certification criterion at § 170.315(d)(9) must be explicitly demonstrated with § 170.315(e)(1) and (e)(2) because of the specific capabilities for secure electronic transmission and secure electronic messaging included in each of these two criteria, respectively. For the other certification criteria (§ 170.315(e)(3), (g)(7), (g)(8), and (g)(9)), this criterion at § 170.315(d)(9) only needs to be demonstrated once as part of the overall scope of the certificate sought.

Certification Requirements

- [Quality management system \(§ 170.315\(g\)\(4\)\)](#) and [accessibility-centered design \(§ 170.315\(g\)\(5\)\)](#) must be certified as part of the overall scope of the certificate issued to the product.
- 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.

Regulation Text

Trusted connection. Establish a trusted connection using one of the following methods:

- (i) Message-level. Encrypt and integrity protect message contents in accordance with the standards specified in § 170.210(a)(2) and (c)(2).
- (ii) Transport-level. Use a trusted connection in accordance with the standards specified in § 170.210(a)(2) and (c)(2).

Criterion Subparagraph	Technical Explanations and Clarifications	Standard(s) Referenced
Applies to entire criterion	<p>Clarifications:</p> <ul style="list-style-type: none"> Health IT needs to provide a level of trusted connection using either 1) encrypted and integrity message protection <u>or</u> 2) a trusted connection for transport. Either of these methods must be demonstrated in accordance with the following standards: Annex A: FIPS Publication 140-2, Security Requirements for Cryptographic Modules <u>and</u> FIPS PUB 180-4, Secure Hash Standard, 180-4. A “trusted connection” means the link is encrypted/integrity protected according to § 170.210(a)(2) or (c)(2). As such, we do not believe it is necessary to specifically name HTTPS and/or SSL/TLS as this standard already covers encryption and integrity protection for data in motion. [see also 80 FR 62676] 	<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>
(i)	<p>Technical outcome – The health IT offers a user encrypted and integrity message protection.</p> <p>Clarifications</p> <ul style="list-style-type: none"> No additional clarifications available. 	See standards listed above.
(ii)	<p>Technical outcome – The health IT provides the user a trusted connection for transport.</p> <p>Clarifications</p> <ul style="list-style-type: none"> The tester is required to view the encryption handshake to ensure that the digital certificates, where used, are being invoked during the connection. Developers have freedom to demonstrate the encryption handshake based on the technology they are using. For example, if a developer has a browser-based module that uses HTTP, the developer could demonstrate the "lock" icon in the browser that indicates that HTTP is present and working properly. 	See standards listed above.

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 30, 2015
1.1	Clarification added on what must be demonstrated during testing of the trusted connection for transport.	Jan 29, 2016