The Office of the National Coordinator for
Health Information Technology

2015 Edition §170.315(d)(9) Trusted Connection

Testing Components:

Test Procedure Version 1.0 – Last Updated 1/08/16

Please consult the Final Rule entitled: *2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications* for a detailed description of the certification criterion with which these testing steps are associated. We also encourage developers to consult the Certification Companion Guide in tandem with the test procedure as they provide clarifications that may be useful for product development and testing.

Note: The order in which the test steps are listed reflects the sequence of the certification criterion and does not necessarily prescribe the order in which the test should take place.

Required Tests

(d)(9)(i) Message-level - Encrypt and integrity protect message contents in accordance with the standards specified in § 170.210(a)(2) and (c)(2).

Standards: § 170.210(a)(2): Any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2, October 8, 2014
§ 170.210(c)(2): A hashing algorithm with a security strength equal to or greater than SHA-2 as specified by NIST in FIPS Publication 180-4 (August 2015)

Testing must be conducted of one Alternative outlined below to satisfy the requirements for this criteria.

Criteria ¶	System Under Test	Test Lab Verification
(i) (Alternative)	1. The health IT developer identifies the encryption algorithm and hashing algorithm to be used to send/receive secure messages. 2. The Health IT Module or user sends at least one message that is encrypted and integrity protected using the algorithms identified in step 1. 3. The Health IT Module encrypts and integrity protects message contents in accordance with the standards specified in § 170.210(a)(2), any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2, October 8, 2014, AND § 170.210 (c)(2), and a hashing algorithm with a security strength equal to or greater than SHA-2 as specified by NIST in FIPS Publication 180-4 (August 2015). Following the exchange of the message, the Health IT Module creates a message digest on the receiving system of the electronic health information that has been received to ensure that the content has not been altered.	1. The tester verifies that the message(s) sent are in conformance with the named encryption and hashing algorithm standards specified in § 170.210(a)(2) and (c)(2) using Documentation. 2. Alternately, the tester verifies via visual inspection that the message(s) sent are in conformance with the named encryption and hashing algorithm standards specified in § 170.210(a)(2) and (c)(2). 3. The tester compares the electronically exchanged message digest and the message digest created on the receiving system to verify that the electronically received health information has not been altered using visual inspection.

(ii) Transport-level - Use a trusted connection in accordance with the standards specified in § 170.210(a)(2) and (c)(2).

Standard(s):§ 170.210(a)(2):Any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2, October 8, 2014
§ 170.210(c)(2):A hashing algorithm with a security strength equal to or greater than SHA-2 as specified by NIST in FIPS Publication 180-4 (August 2015)

Criteria ¶	System Under Test	Test Lab Verification
(ii) (Alternative)	1. The health IT developer identifies the connection's encryption algorithm and hashing algorithm to be used for the trusted connection. 2. The Health IT Module establishes at least one trusted connection in accordance with the standards specified in § 170.210(a)(2), "any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2, October 8, 2014," and § 170.210(c)(2), "a hashing algorithm with a security strength equal to or greater than SHA-2 as specified by NIST in FIPS Publication 180-4 (August 2015)."	1. The tester verifies that the Health IT Module uses a trusted connection in accordance with the standards specified in § 170.210(a)(2) and (c)(2) using Documentation. 2. Where used, the tester requires to see the encryption handshake to ensure that the digital certificates are being invoked during the connection.

Document History

Version Number	Description of Change	Date
1.0	Final Test Procedure	January 08, 2016

Dependencies: For all related and required criteria, please refer to the Master Table of Related and Required Criteria.