§170.315(d)(9) Trusted connection

2015 Edition Test Procedure

Version 1.1 Updated on 09-21-2017

Revision History

Version #	Description of Change	Version Date
1.0	Final Test Procedure	01-08-2016
1.1	As of September 21, 2017, Test Procedure has been moved to Attestation/Developer self-declaration only.	09-21-2017

Regulation Text

Regulation Text

§170.315 (d)(9) *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).

Standard(s) Referenced

Applies to entire criterion

§ 170.210(a)(2) *General.* 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, Security Requirements for Cryptographic Modules, 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, Secure Hash Standard, 180-4 (August 2015)

Testing components

Self-Declaration: As of September 21, 2017, the testing approach for this criterion is satisfied by self-declaration.

The archived version of the Test Procedure is attached below for reference.

System Under Test	Test Lab Verification
The health IT developer submits their self-declaration to the ONC-ATL.	The Tester verifies the self-declaration document contains all of the required data elements.

Archived Version:

§170.315(d)(9) Test Procedure

Content last reviewed on September 21, 2018