§170.315(h)(1) Direct Project

2015 Edition Test Procedure

Version 1.4 Updated on 05-26-2017

Revision History

Version #	Description of Change	Version Date
1.0	Final Test Procedure	01-29-2016
1.1	Updated documentation icon. Corrected reference to TTT to ETT for section (h)(1)(i) – Receive System Under Test step 6. Removed all the XDR related delivery notification tests. (h)(1)(ii) – Send – removed negative test SMTP/IMAP/POP MT Test 22.	03-21-2016
1.2	Removed XDR notification test cases. Updated XDR MT test cases to reflect correct SMTP MT test cases. Removed Applicability Statement text from criteria paragraph header language for paragraph (h)(1)(ii).	04-12-2016
1.3	Removed message tracking tests that require Edge protocols.	05-17-2016

1.4	Corrected Reject Receive of Direct Messages in paragraph (h)(1)(i): • Removed Invalid Trust Anchor from the list of test. This is considered a duplicate of Invalid Trust Relationship (Different Trust Anchor). Reformatted the test procedures for readability. The System Under Test aligns closer to the to the Test Lab section. • Several numbering and narrative formatting changes. Removed the link for DCDT; provided navigation instructions instead.	05-26-2017

Regulation Text

Regulation Text

§170.315 (h)(1) *Direct Project—*

(i) *Applicability Statement for Secure Health Transport.* Able to send and receive health information in accordance with the standard specified in §170.202(a)(2), including formatted only as a "wrapped" message.

(ii) *Delivery Notification in Direct.* Able to send and receive health information in accordance with the standard specified in §170.202(e)(1).

Standard(s) Referenced

Paragraph (h)(1)(i)

§ 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, Version 1.2, August 2015

Paragraph (h)(1)(ii)

§ 170.202(e)(1) Delivery Notification - Implementation Guide for Delivery Notification in Direct v1.0

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.

Testing components

Paragraph (h)(1)(i) - Send

System Under Test

Discover Certificates

1. The user performs setup tasks to discover 2015 Direct Certificate Discovery Tool (DCDT) certificates by downloading the DCDT Trust Anchor, uploading it into the Health IT Module's Direct instance, and mapping the Direct address to a non-Direct email address for receiving results so that the user can discover and use address-bound and domain-bound certificates hosted in both DNS and LDAP in DCDT using identified health IT function(s).

Register Direct Address

2. The user selects "Register Direct" within the Edge Testing Tool (ETT): Direct Testing and registers a Direct address within the ETT and corresponding Contact Email address for receipt of the ETT validation report.

Send Health Information Using Direct

3. The user identifies the payload for sending to the ETT. ONC-supplied payloads are available for download from the ETT-Direct home page.
4. The user sends encrypted and signed health information to a third party (ETT) using Direct in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2 using identified health IT function(s).
5. Based upon the types of Direct messages the Health IT Module supports for sending of information ("wrapped" RFC-5751 messages required), the user sends health information to a third party using Direct in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2.

Test Lab Verification

Discover Certificates

1. The tester verifies the Health IT Module can discover and use address-bound and domain-bound certificates hosted in both DNS and LDAP in order to create and store a listing of Direct recipients using the Direct Certificate Discovery Tool. All listed certificates listed in both DNS and LDAP must be tested corresponding to the standard at § 170.202(a)(2).

Register Direct Address

2. The tester verifies that the Health IT Module can register a Direct email address using the ETT and has supplied a corresponding Contact Email address for receipt of the ETT validation report.

Send Health Information Using Direct

3. Using the ETT validation report, the tester verifies the payload sent to the ETT is encrypted using the ETT's Public Key and signed using the Health IT Module's Private Key.
4. Using the ETT validation report, the tester verifies the identified health information is successfully transmitted to a third party using Direct, in accordance with the standard specified at § 170.202(a)(2), and using the RFC-5751 "wrapped" message format.
5. Using the validation report, the tester verifies that the payload was successfully received by the ETT, and that the ETT was able to successfully decrypt the message.

Paragraph (h)(1)(i) - Receive

System Under Test

Hosting Certificates

1. The user performs setup tasks to test hosting of certificates (by entering the Health IT Module's Direct address within DCDT) and executes test cases based upon whether the Health IT Module is able to host either address-bound or domain-bound certificates in either DNS or LDAP servers using the DCDT.

SUT Connection

2. The user selects "Send Direct Message" within the ETT-Direct Testing and performs setup tasks to enable the receipt of Direct Messages including:
   - Completion of the required information, identifying the Direct Address for testing receipt and digital signing of health information in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport v1.2.
   - Installation of the ETT's Valid Trust Anchor within the Health IT Module.
   - Identification of the Health IT Module's Public Key for encryption of messages to be sent by ETT to the Health IT Module.

Receive Direct Message

3. The user receives RFC-5751 "wrapped" health information sent from ETT using Direct in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport v1.2 and sends corresponding Message Delivery Notifications (MDNs).

Reject Receipt of Direct Message (Negative Testing)

4. The user rejects health information that is not in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2 sent from the ETT to the Health IT Module using the following tool option: Invalid Certificate.
5. The user rejects health information that is not in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2 sent from the ETT to the Health IT Module using the following tool option: Expired Certificate.
6. The user rejects health information that is not in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2 sent from the ETT to the Health IT Module using the following tool option: Invalid Trust Relationship (Different Trust Anchor).
7. The user rejects health information that is not in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2 sent from the ETT to the Health IT Module using the following tool option: No Authority Information Access (AIA) Extension.
8. The user rejects health information that is not in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2 sent from the ETT to the Health IT Module using the following tool option: Invalid Message Digest.

Test Lab Verification

Hosting Certificates

1. The tester verifies that the Health IT Module's hosted certificates are discoverable as displayed on screen for the DCDT test cases executed.

SUT Connection

2. No action required.

Receive Direct Message

3. The tester verifies that health information can be successfully received by the Health IT Module from the ETT, in accordance with the standard specified at § 170.202(a)(2), using "wrapped" RFC-5751 messages and that a MDN from the Health IT Module was received from the ETT for all messages the system received.

Reject Receipt of Direct Message (Negative Testing)

4. Invalid Certificate: The tester verifies that the Health IT Module rejects a Direct message received with an invalid Trust Anchor and that no corresponding MDN was received by the ETT from the Health IT Module.
5. Expired Certificate: The tester verifies that the Health IT Module rejects a Direct message received with an expired certificate and that no corresponding MDN was received by the ETT from the Health IT Module.
6. Invalid Trust Relationship (Different Trust Anchor): The tester verifies that the Health IT Module rejects a Direct message received with an invalid Trust Relationship. The tester verifies that no corresponding MDN was received by the ETT from the Health IT Module.
7. No Authority Information Access (AIA) extension: The tester verifies that the Health IT Module rejects a Direct message received without an Authority Information Access (AIA) extension and that no corresponding MDN was received by the ETT from the Health IT Module.
8. Invalid Message Digest: The tester verifies that the Health IT Module rejects a Direct message received with an invalid message digest that no corresponding MDN was received by the ETT from the Health IT Module.

Paragraph (h)(1)(ii) – Message Disposition Notification: Processed

System Under Test

Disposition-Notification-Options Header

1. Using the ETT: HISP Testing & Delivery Notification "Message Tracking" using "Your system as "Receiver", the Health IT Module is able to receive and successfully process a message from the ETT (as Sending HISP) that contains a valid Disposition-Notification-Options Header and includes it in the message to the destination via SMTP MT Test 39.
2. Negative Testing: The Health IT Module is able to receive and successfully process a message from the ETT (as Sending HISP) that contains an invalid Disposition-Notification-Options Header and includes it in the message to the destination via SMTP MT Test 40.

Test Lab Verification

Disposition-Notification-Options Header

1. The ETT test results for SMTP MT Test 39 are successful.
2. The ETT test results for SMTP MT Test 40 are successful.

Paragraph (h)(1)(ii) – Message Disposition Notification: Failed

System Under Test

Failure Notification

1. Using the ETT: HISP Testing & Delivery Notification “Message Tracking” using “Your system as “Receiver”, the Health IT Module successfully validates security and trust returning a Processed MDN, but cannot deliver the message to its final destination (mail box full, unavailable, mailbox does not exist) - generating a MDN failed or a failure Delivery Status Notification via SMTP MT Test 41.

Test Lab Verification

Failure Notification

1. The ETT test results for SMTP MT Test 41 are successful.

Required Enhanced Testing

The Health IT Module submits evidence of multi-partner testing with three different and unrelated partner HISPs using Direct v1.2 (in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2), formatted only as a “wrapped” message.

Paragraph (h)(1)(i) – Required Enhanced Testing, Send

System Under Test

The Health IT Module provides evidence and demonstration of successful send of encrypted and signed health information from the Health IT Module to 3 partners (e.g., other vendor Health IT Modules (HISPs) that have implemented (h)(1) or (h)(2) capabilities), using Direct v1.2 in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2, which includes:

- Documentation of the Health IT Module sending “Wrapped” RFC-5751 messages to 3 partner HISPs; and
- Documentation of the Health IT Module receiving processed MDNs from each of the 3 partner HISPs, generated by the partner HISPs upon receiving the Direct message from the Health IT Module.

Test Lab Verification

The tester verifies that the Health IT Module has successfully sent encrypted and signed health information to 3 partner HISPs using Direct v1.2 in accordance with the standard specified at § 170.202(a)(2). The verification includes:

- Indication through documentation that the Health IT Module sent “Wrapped” RFC-5751 messages to 3 separate and unrelated HISP partners.
- Indication through documentation of the Health IT Module receiving processed MDNs from each of the 3 partner HISPs, generated upon receiving the Direct message from the Health IT Module.

Paragraph (h)(1)(i) – Required Enhanced[1] Testing, Receive

[1] Partners the Health IT Module chooses to test with do not have to be certified at the time of testing as long as the testing uses the Direct v1.2 (in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2), formatted only as a “wrapped” message.

System Under Test

The user provides evidence of successful receipt of encrypted and signed health information from 3 partners (e.g., other vendor Health IT Modules (HISPs) that have implemented (h)(2) capabilities) using Direct v1.2 in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2. The evidence includes:

- Documentation of the Health IT Module receiving “Wrapped” RFC-5751 messages from 3 partner HISPs; and
- Documentation that the Health IT Module generates and sends processed MDNs that are transmitted to each of the 3 partner HISPs, generated upon successfully receiving a Direct message from the Health IT Module.

Test Lab Verification

The tester verifies that the Health IT Module has received encrypted and signed health information from 3 partner HISPs using Direct v1.2 in accordance with the standard specified at § 170.202(a)(2). The documentation includes:

- Indication that the Health IT Module successfully received “Wrapped” RFC-5751 messages from 3 separate and unrelated HISP partners; and
- Indication of the Health IT Module generating and transmitting processed MDNs to each of the 3 partner HISPs, generated upon receiving the Direct message from each partner HISP.

Content last reviewed on December 6, 2018