

2015 Edition §170.315(h)(2) Direct Project, Edge Protocol, and XDR-XDM

Testing Components:



Gap







ONC
Supplied
Test Data

Test Procedure Version 1.0 – Last Updated 1/29/16

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

(h)(2)(i) Able to send and receive health information in accordance with:

(i)(A) The standards specified in § 170.202(a)(2), including formatted only as a “wrapped” message;

Standards:

§ 170.202(a)(2): [Applicability Statement for Secure Health Transport v1.2](#) (incorporated by reference in [§ 170.299](#)).

Tools:

[2015 Direct Certificate Discovery Tool \(DCDT\)](#)

[Edge Testing Tool \(ETT\)](#)

(i)(A) – Send

Criteria ¶	System Under Test	Test Lab Verification
(i)(A), Send	<p><u>Discover Certificates</u></p> <ol style="list-style-type: none"> 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. 2. 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). <p style="text-align: right; font-size: 8px;">Continued on next page</p>	<p><u>Discover Certificates</u></p> <ol style="list-style-type: none"> 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 certificates listed in both DNS and LDAP must be tested corresponding to the ONC Applicability Statement for Secure Health Transport v1.2. <p style="text-align: right; font-size: 8px;">Continued on next page</p>

Criteria ¶	System Under Test	Test Lab Verification
<p>(i)(A), Send continued</p>	<p>Continued from previous page</p> <p><u>Register Direct Address</u></p> <ol style="list-style-type: none"> 3. The user selects “Direct Testing” within the Edge Testing Tool (ETT). 4. The user registers a Direct address within the ETT and corresponding Contact Email address for receipt of the ETT validation report within the “Register Direct” tab. <p><u>Send Health Information Using Direct</u></p> <ol style="list-style-type: none"> 5. The user identifies the payload for sending to the ETT. ONC-supplied payloads are available for download from the ETT-Direct home page. 6. 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): Applicability Statement for Secure Health Transport v1.2 using identified health IT function(s). 7. 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) ONC Applicability Statement for Secure Health Transport. 	<p>Continued from previous page</p> <p><u>Register Direct Address</u></p> <ol style="list-style-type: none"> 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. <p><u>Send Health Information Using Direct</u></p> <ol style="list-style-type: none"> 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), 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.

(i)(A) – Receive

Criteria ¶	System Under Test	Test Lab Verification
<p>(i)(A) Receive</p>	<p><u>Hosting Certificates</u></p> <ol style="list-style-type: none"> The user performs setup tasks to test hosting of certificates, by entering the Health IT Module’s Direct address within DCDT. The user 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. <p><u>Receive Direct Message</u></p> <ol style="list-style-type: none"> The user selects “Direct Testing” within the ETT. The user selects the “Send Direct Message” tab and completes 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): Applicability Statement for Secure Health Transport v1.2. The user installs the ETT’s Valid Trust Anchor within the Health IT Module. The user identifies the Health IT Module’s Public Key for encryption of messages to be sent by TTT to the Health IT Module. The user receives RFC-5751 “wrapped” health information sent from ETT using Direct in accordance with the standard specified at §170.202(a)(2) Applicability Statement for Secure Health Transport v1.2 and sends corresponding MDNs. <p style="text-align: right;">Continued on next page</p>	<p><u>Hosting Certificates</u></p> <ol style="list-style-type: none"> The tester verifies that the Health IT Module’s hosted certificates are discoverable as displayed on screen for the DCDT test cases executed. <p><u>Receive Direct Message</u></p> <ol style="list-style-type: none"> 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. The tester verifies that an MDN from the Health IT Module was received from the ETT for all messages in Step 2. <p><u>Reject Receipt of Direct Message (Negative Testing)</u></p> <ol style="list-style-type: none"> Negative Test: The tester verifies that the Health IT Module rejects Direct messages received with an invalid Trust Anchor and no corresponding MDN was received by the ETT from the Health IT Module. Negative Test: The tester verifies that the Health IT Module rejects Direct messages received with an invalid Trust Anchor and invalid certificate. The tester verifies that no corresponding MDN was received by the ETT from the Health IT Module. Negative Test: The tester verifies that the Health IT Module rejects Direct messages received with an expired certificate. The tester verifies that no corresponding MDN was received by the ETT from the Health IT Module. <p style="text-align: right;">Continued on next page</p>

Criteria ¶	System Under Test	Test Lab Verification
<p>(i)(A), Receive continued</p>	<p>Continued from previous page Reject Receipt of Direct Message (Negative Testing) 8. Negative Test: The user rejects health information that is not in accordance with the standard specified at §170.202(a)(2) Applicability Statement for Secure Health Transport v1.2 sent from the ETT to the Health IT Module using the following tool options:</p> <ul style="list-style-type: none"> • Invalid Certificate • Invalid Trust Anchor • Expired Certificate • Invalid Trust Relationship (Different Trust Anchor) • No Authority Information Access (AIA) Extension • Invalid Message Digest 	<p>Continued from previous page</p> <ol style="list-style-type: none"> 7. Negative Test: The tester verifies that the Health IT Module rejects Direct messages received with an invalid Trust Relationship. The tester verifies that no corresponding MDN was received by the ETT from the Health IT Module. 8. Negative Test: The tester verifies that the Health IT Module rejects Direct messages received without an Authority Information Access (AIA) extension. The tester verifies that no corresponding MDN was received by the ETT from the Health IT Module. 9. Negative Test: The tester verifies that the Health IT Module rejects Direct messages received with an invalid message digest. The tester verifies that no corresponding MDN was received by the ETT from the Health IT Module.

(i)(B) The standard specified in § 170.202(b), including support for both limited and full XDS metadata profiles.

Standards:

§ 170.202(b): [ONC XDR and XDM for Direct Messaging Specification](#) (incorporated by reference in § 170.299), including support for both limited and full XDS metadata profiles: IHE ITI: [IHE IT Infrastructure Technical Framework Volume 3 \(ITI TF-3\)](#)

Tools:

- [2015 Direct Certificate Discovery Tool \(DCDT\)](#)
- [Edge Testing Tool \(ETT\)](#)
- [Transport Testing Tool \(TTT\)](#)

(i)(B) – Send using Direct + XDM

Criteria ¶	System Under Test	Test Lab Verification
<p>(i)(B)</p>	<p><u>Discover Certificates</u></p> <ol style="list-style-type: none"> The user performs setup tasks to discover 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. The user can discover and use address-bound and domain-bound certificates hosted in both DNS and LDAP in DCDT using developer-identified health IT function(s). <p><u>Register Direct Address</u></p> <ol style="list-style-type: none"> The user selects “Direct Testing” within the ETT to access the Direct testing functions. The user registers a Direct address within the ETT and corresponding Contact Email address for receipt of the ETT validation report within the “Register Direct” tab. The user identifies the payload for sending to the ETT via Direct with XDM Validation. ONC-supplied payloads are available for download from the Home Page of the ETT. <p><u>Send Health Information Using Direct with XDR/XDM</u></p> <ol style="list-style-type: none"> The user sends encrypted and signed health information to a third party in accordance with the standard specified at §170.202(b): ONC XDR and XDM for Direct Messaging Specification using limited metadata, using RFC-5751 “wrapped” messages. The user sends encrypted and signed health information to a third party, in accordance with the standard specified at §170.202(b): ONC XDR and XDM for Direct Messaging Specification using full metadata, using RFC-5751 “wrapped” messages. <p style="text-align: right;">Continued on next page</p>	<p><u>Discover Certificates</u></p> <ol style="list-style-type: none"> 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 certificates listed in both DNS and LDAP must be tested corresponding to the ONC Applicability Statement for Secure Health Transport v1.2. <p><u>Register Direct Address</u></p> <ol style="list-style-type: none"> The tester verifies 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. <p><u>Send Health Information Using Direct with XDR/XDM</u></p> <ol style="list-style-type: none"> 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. Using the ETT validation report, the tester verifies the identified health information is successfully transmitted to a third party using Direct with XDR/XDM in accordance with the standard specified at §170.202(b), using RFC-5751” wrapped” messages. Using the validation report, the tester verifies the payload using limited XDS metadata was successfully received by the ETT, and that the ETT was able to successfully decrypt the message. Using the validation report, the tester verifies the payload using full XDS metadata was successfully received by the ETT, and that the ETT was able to successfully decrypt the message. <p style="text-align: right;">Continued on next page</p>

(i)(B) – Send using Direct + XDM, continued

Criteria ¶	System Under Test	Test Lab Verification
(i)(B), continued	Continued from previous page 7. The XDM package sent by the Health IT Module is able to be successfully validated using the Transport Testing Tool (TTT) Message Validator.	Continued from previous page 7. Using the XDM payload available for download within the validation report, the tester uploads the XDM payloads (sent using both limited and full metadata) to the TTT's XDM Message Validator. The tester reviews the TTT validation report to verify the XDM package is valid.

(i)(B) – Send using SOAP + XDR

Criteria ¶	System Under Test	Test Lab Verification
(i)(B)	<ol style="list-style-type: none"> 1. The user can generate a SOAP endpoint for XDR for each payload that will be sent to the TTT and provide a name for each TTT connection. 2. The user sends the payload to the TTT using SOAP Protocols with XDR Validation with limited metadata to the TTT's SOAP endpoint. 3. The user sends the payload to the TTT using SOAP Protocols with XDR Validation with full metadata to the TTT's SOAP endpoint. 	<ol style="list-style-type: none"> 1. Using the validation report, the tester verifies the payload using limited XDS metadata was successfully received by the TTT. 2. Using the validation report, the tester verifies the payload using full XDS metadata was successfully received by the TTT.

(i)(B) – Receive using Direct + XDM

Criteria ¶	System Under Test	Test Lab Verification
<p>(i)(B)</p>	<p><u>Hosting Certificates</u></p> <ol style="list-style-type: none"> 1. The user performs setup tasks to test hosting of certificates by entering the Health IT Module’s Direct address within DCDT. 2. The user 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. <p><u>Receive Direct + XDR/XDM Message</u></p> <ol style="list-style-type: none"> 3. The user selects “Direct Testing” within the ETT to access the Direct testing functions. 4. The user selects the “Send Direct Message” tab and completes 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(b): ONC XDR and XDM for Direct Messaging Specification. 5. The user installs the ETT’s Valid Trust Anchor within the Health IT Module. 6. The user identifies the Health IT Module’s Public Key for encryption of messages to be sent by ETT to the Health IT Module. 7. The user receives health information that is sent from ETT using Direct in accordance with the standard specified at §170.202(b) ONC XDR and XDM for Direct Messaging Specification with limited metadata and sends corresponding MDNs, using RFC-5751 “wrapped” messages. 8. The user receives health information that is sent from ETT using Direct in accordance with the standard specified at §170.202(b) ONC XDR and XDM for Direct Messaging Specification with full metadata and sends corresponding MDNs. <p style="text-align: right;">Continued on next page</p>	<p><u>Hosting Certificates</u></p> <ol style="list-style-type: none"> 1. The tester verifies that the Health IT Module’s hosted certificates are discoverable as displayed on screen for the DCDT test cases executed. <p><u>Receive Direct + XDR/XDM Message</u></p> <ol style="list-style-type: none"> 2. The tester verifies health information can be successfully received by the Health IT Module from the ETT in accordance with the standard specified at §170.202(b), using the limited XDS metadata profile, using RFC-5751 “wrapped” messages. 3. The tester verifies health information can be successfully received by the Health IT Module from the ETT in accordance with the standard specified at §170.202(b), using the full XDS metadata profile and using RFC-5751 “wrapped” messages. 4. The tester verifies that an MDN from the Health IT Module was received by the ETT for all messages in Step 2 and Step 3. <p><u>Validate XDM Package</u></p> <ol style="list-style-type: none"> 5. Using the TTT validation report, the tester verifies the XDM payload received by the Health IT Module and uploaded to the TTT successfully passes XDM validation. <p><u>Negative Testing</u></p> <ol style="list-style-type: none"> 6. Negative Test: The tester verifies that the Health IT Module rejects Direct messages received with an invalid Trust Anchor and no corresponding MDN was received by the ETT. 7. Negative Test: The tester verifies that the Health IT Module rejects Direct messages received with an invalid Trust Anchor and invalid certificate. The tester verifies that no corresponding MDN was received by the ETT. <p style="text-align: right;">Continued on next page</p>

(i)(B) – Receive using Direct + XDM, continued

Criteria ¶	System Under Test	Test Lab Verification
<p>(i)(B), continued</p>	<p>Continued from previous page</p> <p><u>Validate XDM Package</u></p> <p>9. The user uploads the XDM payload received from the ETT to the Transport Testing Tool (TTT) to perform validation of the XDM package.</p> <p><u>Reject Receive of Direct Message (Negative Testing)</u></p> <p>10. The user rejects health information that is not in accordance with the standard specified at §170.202(a)(2) ONC XDR and XDM for Direct Messaging Specification sent from the ETT to the Health IT Module using the following tool options:</p> <ul style="list-style-type: none"> • Expired Certificate • Invalid Trust Relationship (Different Trust Anchor) • No Authority Information Access (AIA) Extension • Invalid Message Digest 	<p>Continued from previous page</p> <p>8. Negative Test: The tester verifies that the Health IT Module rejects Direct messages received with an expired certificate. The tester verifies that no corresponding MDN was received by the ETT.</p> <p>9. Negative Test: The tester verifies that the Health IT Module rejects Direct messages received with an invalid Trust Relationship. The tester verifies that no corresponding MDN was received by the ETT.</p> <p>10. Negative Test: The tester verifies that the Health IT Module rejects Direct messages received without an Authority Information Access (AIA) extension. The tester verifies that no corresponding MDN was received by the ETT.</p> <p>11. Negative Test: The tester verifies that the Health IT Module rejects Direct messages received with an invalid message digest. The tester verifies that no corresponding MDN was received by the ETT.</p>

(i)(B) – Receive using SOAP + XDR

Criteria ¶	System Under Test	Test Lab Verification
(i)(B)	<ol style="list-style-type: none"> 1. The user performs setup by providing a Site Name and a separate endpoint used by the Health IT Module in the TTT for each XDR message. 2. The user shall define and identify an Actor Simulator in the ETT terminology (as described in the ETT User Guide). 3. The Health IT Module receives health information from the TTT using SOAP Protocols with XDR Validation with limited metadata. 4. The Health IT Module receives health information from the TTT using SOAP Protocols with XDR Validation with full metadata. 5. The Health IT Module receives health information from the TTT using SOAP Protocols with XDR Validation with both NHIN SAML and TLS selected, to the Health IT Module’s SOAP endpoint. 	<ol style="list-style-type: none"> 1. The tester verifies that health information can be successfully received by the Health IT Module from the TTT in accordance with the standard specified at §170.202(b), using SOAP Protocols with XDR Validation with limited XDS metadata. 2. The tester verifies that health information can be successfully received by the Health IT Module from the TTT in accordance with the standard specified at §170.202(b), using SOAP Protocols with XDR Validation with full XDS metadata. 3. The tester verifies that health information can be successfully received by the Health IT Module from the TTT in accordance with the standard specified at §170.202(b), using SOAP Protocols with XDR Validation using NHIN SAML and TLS.

(i)(C) Both edge protocol methods specified by the standard in § 170.202(d).

Standards:

§ 170.202(d): [ONC Implementation Guide for Direct Edge Protocols, Version 1.1, June 25, 2014](#) (incorporated by reference in [§ 170.299](#))

Tools:

[Edge Testing Tool \(ETT\)](#)

(i)(C) – Send Using Edge Protocol for IHE XDR profile for Limited Metadata Document Sources, continued

Criteria ¶	System Under Test	Test Lab Verification
(i)(C)	<p><u>SUT Connection</u></p> <ol style="list-style-type: none"> The user shall execute XDR Test Cases using the ETT (HISP & Delivery Notification) for “System as Sender.” The user establishes a Mutual TLS session for the Health IT Module to authenticate to the ETT (XDR Test 16). The user authenticates the Health IT Module to the ETT using an incorrect Mutual TLS session (XDR Test 17). <p><u>Send Payload</u></p> <ol style="list-style-type: none"> The user configures the ETT’s endpoints within the Health IT Module and provides the Health IT Module’s Direct “To” address to generate endpoints for the following types of messages: <ul style="list-style-type: none"> Direct to send to Edge as an XDR message (XDR Test 10); Direct + XDM to send to Edge as an XDR message with Limited Metadata (XDR Test 11); and Direct + XDM to send to Edge as an XDR message with Full Metadata (XDR Test 12). The Health IT Module receives a Direct message from the ETT (as Sending HISP), and translates it to an XDR message sent to the ETT (as Edge) (XDR Test 10). The Health IT Module receives a Direct + XDM message from the ETT (as Sending HISP), and translates it to an XDR message with Limited Metadata sent to the ETT (as Edge) (XDR Test 11). <p style="text-align: right;">Continued on next page</p>	<p><u>SUT Connection</u></p> <ol style="list-style-type: none"> Using the ETT, the tester verifies that the Health IT Module initiates a Mutual TLS session with the ETT. Using the ETT, the tester verifies that the Health IT Module disconnects from the ETT when the certificate received from the ETT is invalid. <p><u>Send Payload</u></p> <ol style="list-style-type: none"> Using the ETT validation report, the tester verifies that the Health IT Module can translate the following using §170.202(d): ONC Implementation Guide for Direct Edge Protocols v1.1: <ul style="list-style-type: none"> Direct Message to Health IT Module to XDR message; Direct + XDM Message to Health IT Module to XDR message with Limited Metadata; and Direct + XDM Message to Health IT Module to XDR message with Full Metadata. <p><u>Message Tracking Using Processed MDNs</u></p> <ol style="list-style-type: none"> Using the ETT, the tester verifies that the Health IT Module successfully performs message tracking using processed MDNs. Using the ETT validation reports, the tester verifies that the Health IT Module has sent failure messages to the ETT (as Edge) for the following tests: <ul style="list-style-type: none"> Bad Address Untrusted Destination HISP <p style="text-align: right;">Continued on next page</p>

(i)(C) – Send Using Edge Protocol for IHE XDR profile for Limited Metadata Document Sources, continued

Criteria ¶	System Under Test	Test Lab Verification
<p>(i)(C), continued</p>	<p>Continued from previous page</p> <p>7. The Health IT Module receives a Direct + XDM message from the ETT (as Sending HISP), and translates it to an XDR message with Full Metadata sent to the ETT (as Edge) (XDR Test 12).</p> <p><u>Message Tracking Using Processed MDNs</u></p> <p>8. The ETT (as Edge) sends a message to the Health IT Module using a bad address, such that the Health IT Module is unable to deliver the message. The Health IT Module delivers a failure message to the ETT (as Edge) using the XDR profile due to a bad address (XDR MT Test 13).</p> <p>9. The ETT (as Edge) sends a message to the Health IT Module using a valid address, but the ETT (as Destination HISP) is not trusted. The Health IT Module delivers a failure message to the ETT (as Edge) using the XDR profile due to an untrusted HISP (ETT as Destination HISP) (XDR MT Test 14).</p> <p>10. The ETT (as Edge) sends a message to the Health IT Module using a valid address, but the ETT’s (as Destination HISP) certificates are not published. The Health IT Module delivers a failure message to the ETT (as Edge) using the XDR profile due to an unpublished HISP certificate (ETT as Destination HISP) (XDR MT Test 15).</p> <p>11. The ETT (as Edge) sends a message to the Health IT Module using a valid address, but the ETT (as Destination HISP) does not respond with a processed MDN. The Health IT Module delivers a failure message to the ETT (as Edge) using the XDR profile, due to exceeded wait period for receiving a processed MDN from the ETT (as Destination HISP) (XDR MT Test 16).</p>	<p>Continued from previous page</p> <ul style="list-style-type: none"> • Unpublished Certificate for Destination HISP • Delivery Failure Timeout

(i)(C) – Send Using Edge Protocol for SMTP

Criteria ¶	System Under Test	Test Lab Verification
(i)(C)	<p><u>SUT Connection</u></p> <ol style="list-style-type: none"> The user shall execute HISP SMTP Tests using the ETT for “System as Sender.” Start TLS Session: The user initiates a TLS session for the Health IT Module with the ETT, using email address wellformed2@edge.nist.gov (SMTP Test 14). The Health IT Module provides documentation of the Health IT module’s ability to reject the connection for a TLS session initiated with an Edge due to an invalid certificate. Authentication to SMTP Server: The user authenticates the Health IT Module to the ETT using PLAIN SASL using email address wellformed1@edge.nist.gov (SMTP Test 18). The Health IT Module provides documentation of the Health IT module’s ability to authenticate using DIGEST-MD5 SASL. <p><u>Send Payload</u></p> <ol style="list-style-type: none"> The user sends a document to the ETT using the email address wellformed1@edge.nist.gov (SMTP Tests 1-8). Message Tracking Using Processed MDNs: The user sends three messages to the ETT with unique message IDs for each message to wellformed14@edge.nist.gov (MU Tracking Step 17). <p><u>Message Tracking Using Processed MDNs</u></p> <ol style="list-style-type: none"> The ETT (as Edge) sends a message to the Health IT Module using a bad address, such that the Health IT Module is unable to deliver the message. The Health IT Module delivers a failure message to the ETT (as Edge) using the following edge protocol due to a bad address: <ul style="list-style-type: none"> SMTP (SMTP MT Test 1) Alternative: SMTP + IMAP (SMTP/IMAP Test 5) Alternative: SMTP + POP (SMTP/POP Test 9) <p style="text-align: right;">Continued on next page</p>	<p><u>SUT Connection</u></p> <ol style="list-style-type: none"> Using the ETT, the tester verifies the Health IT Module initiates a TLS session and can authenticate using PLAIN SASL authentication. The tester verifies evidence of the Health IT Module’s capability to initiate a TLS session, but reject the connection with an Edge due to an invalid certificate. The tester verifies evidence of the Health IT Module’s capability to authenticate using DIGEST-MD5 SASL. <p><u>Send Payload</u></p> <ol style="list-style-type: none"> Using the ETT, the tester verifies that the Health IT Module can send an SMTP Message using the SMTP Edge Protocol with STARTTLS and PLAIN SASL Authentication. <p><u>Message Tracking Using Processed MDNs</u></p> <ol style="list-style-type: none"> Using the ETT, the tester verifies that the Health IT Module successfully performs message tracking using processed MDNs. Using the ETT validation reports, the tester verifies that the Health IT Module has sent failure messages to the ETT (as Edge) for the following tests: <ul style="list-style-type: none"> Bad Address; Untrusted Destination HISP; Unpublished Certificate for Destination HISP; and Delivery Failure Timeout.

(i)(C) – Send Using Edge Protocol for SMTP, continued

Criteria ¶	System Under Test	Test Lab Verification
(i)(C), continued	<p>Continued from previous page</p> <p>9. The ETT (as Edge) sends a message to the Health IT Module using a valid address, but the ETT (as Destination HISP) is not trusted. The Health IT Module delivers a failure message to the ETT (as Edge) using the following edge protocol due to an untrusted HISP (ETT as Destination HISP):</p> <ul style="list-style-type: none"> • SMTP (SMTP MT Test 2) • Alternative: SMTP + IMAP (SMTP/IMAP Test 6) • Alternative: SMTP + POP (SMTP/POP Test 10) <p>10. The ETT (as Edge) sends a message to the Health IT Module using a valid address, but the ETT’s (as Destination HISP) certificates are not published. The Health IT Module delivers a failure message to the ETT (as Edge) using the following edge protocol due to an unpublished HISP certificate (ETT as Destination HISP):</p> <ul style="list-style-type: none"> • SMTP (SMTP MT Test 3) • Alternative: SMTP + IMAP (SMTP/IMAP Test 7) • Alternative: SMTP + POP (SMTP/POP Test 11) <p>11. The ETT (as Edge) sends a message to the Health IT Module using a valid address, but the ETT (as Destination HISP) does not respond with a processed MDN. The Health IT Module delivers a failure message to the ETT (as Edge) using the following edge protocol due to exceeded wait period for receiving a processed MDN from the ETT (as Destination HISP):</p> <ul style="list-style-type: none"> • SMTP (SMTP MT Test 4) • Alternative: SMTP + IMAP (SMTP/IMAP Test 8) • Alternative: SMTP + POP (SMTP/POP Test 12) 	See previous page

(i)(C) – Send Using Edge Protocol for IMAP (SMTP Optional)

Criteria ¶	System Under Test	Test Lab Verification
(i)(C)	<ol style="list-style-type: none"> 1. The user executes HISP IMAP Tests using the ETT for “System as Sender.” 2. Using the ETT, the user initiates an IMAP session to the Health IT Module using the IMAP4 CAPABILITIES command, NOOP command, and LOGOUT command. (IMAP Tests 1-3) 3. Using the ETT, the user initiates an IMAP session to the Health IT Module using the STARTTLS command, AUTHENTICATE command, LOGIN command, SELECT command, and FETCH command. (IMAP Tests 4-8, 11, 15) 4. Negative Test: The user demonstrates the Health IT Module rejects an IMAP4 connection with a bad command syntax by terminating the connection from the ETT. (IMAP Test 9) 5. Negative Test: The user demonstrates the Health IT Module rejects an IMAP4 connections with bad commands using the right syntax based upon the specific state of the connection by terminating the connection from the ETT. (IMAP Test 10) 6. The Health IT Module generates unique identifiers (UIDs) for each message when messages are added/deleted to the Health IT Module mailbox and synchronized multiple times after closing/reopening connections. (IMAP Test 12) 7. The Health IT Module provides documentation of the Health IT module’s ability to process connection requests initiated using STARTTLS with TLS_RSA_WITH_RC4_128_MD5 cipher suite. 8. The Health IT Module provides documentation of the Health IT module’s ability to process connection requests initiated using STARTTLS with TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA cipher suite. 9. The Health IT Module provides documentation of the ability to accept a DIGEST-MD5 authentication mechanism and authenticates the Edge. <p style="text-align: right;">Continued on next page</p>	<ol style="list-style-type: none"> 1. Using the ETT logs, the tester verifies the Health IT Module is has successfully implemented the following commands (IMAP Tests 1-8, 11, 15): <ul style="list-style-type: none"> • IMAP4 CAPABILITY • NOOP • LOGOUT • AUTHENTICATE • STARTTLS • LOGIN • SELECT • FETCH 2. Negative Tests: Using the ETT logs, the tester verifies the Health IT Module rejects commands with the appropriate response and terminates connection with the ETT. (IMAP Tests 9-10) 3. Using the ETT logs, the tester verifies the Health IT Module generates unique identifiers for each message (UIDs). (IMAP Test 12) 4. The tester verifies evidence of the Health IT Module’s capability to process connection requests initiated using STARTTLS with TLS_RSA_WITH_RC4_128_MD5 cipher suite. 5. The tester verifies evidence of the Health IT Module’s capability to process connection requests initiated using STARTTLS with TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA cipher suite. 6. The tester verifies evidence of the Health IT Module’s capability to accept authentication requests using DIGEST-MD5. 7. Negative Test: The tester verifies evidence of the Health IT Module’s capability to reject authentication requests due to bad DIGEST-MD5 values. <p style="text-align: right;">Continued on next page</p>

(i)(C) – Send Using Edge Protocol for IMAP (SMTP Optional), continued

Criteria ¶	System Under Test	Test Lab Verification
<p>(i)(C), continued</p>	<p>Continued from previous page</p> <p>10. Negative Test: The Health IT Module provides documentation of the ability to reject an authentication request from an Edge due to bad DIGEST-MD5 values.</p> <p>11. Negative Test: The Health IT Module rejects authentication requests from the ETT due to an invalid PLAN SASL username/password. (IMAP Test 17)</p> <p>12. The ETT (as Edge) is able to fetch attachments from the Health IT Module using an IMAP4 connection (IMAP Test 32)</p>	<p>Continued from previous page</p> <p>8. Negative Test: Using the ETT logs, the tester verifies the Health IT Module rejects authentication requests due to invalid username/password. (IMAP Test 17)</p> <p>9. Using the ETT logs, the tester verifies the Health IT Module is able to host attachments and make them available for fetching using IMAP. (IMAP Test 32)</p>

(i)(C) – Send Using Edge Protocol for POP3 (SMTP Optional)

Criteria ¶	System Under Test	Test Lab Verification
(i)(C)	<ol style="list-style-type: none"> 1. The user executes HISP POP Tests using the ETT for “System as Sender.” 2. Using the ETT, the user initiates an POP session to the Health IT Module using the POP3 CAPA command, NOOP command, and QUIT command. (POP Tests 1-2) 3. Using the ETT, the user initiates an IMAP session to the Health IT Module using the POP3 STAT command, STARTTLS command, RETR command, LIST command, and RSET command. (POP Tests 3-5, 11, 15) 4. Negative Test: The user demonstrates the Health IT Module rejects an POP3 connection with a bad command syntax by terminating the connection from the ETT. (POP Test 9) 5. Negative Test: The user demonstrates the Health IT Module rejects an POP3 connections with bad commands using the right syntax based upon the specific state of the connection by terminating the connection from the ETT. (POP Test 10) 6. The Health IT Module generates unique identifiers for each message when messages are added/deleted to the Health IT Module mailbox and synchronized multiple times after closing/reopening connections. (POP Test 12) 7. The Health IT Module provides documentation of the ability to process connection requests initiated using STARTTLS with TLS_RSA_WITH_RC4_128_MD5 cipher suite. 8. The Health IT Module provides documentation of the ability to processes connection requests initiated using STARTTLS with TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA cipher suite. 9. Negative Test: The Health IT Module rejects authentication requests from the ETT due to an invalid PLAN SASL username/password. (POP Test 17) 10. The ETT (as Edge) is able to fetch attachments from the Health IT Module using an IMAP4 connection (POP Test 32) 	<ol style="list-style-type: none"> 1. Using the ETT logs, the tester verifies the Health IT Module is has successfully implemented the following commands (POP Tests 1-5, 11, 15): <ol style="list-style-type: none"> a. POP3 CAPA b. NOOP c. QUIT d. POP3 STAT e. STARTTLS f. RETR g. LIST h. RSET 2. Negative Tests: Using the ETT logs, the tester verifies the Health IT Module rejects commands with the appropriate response and terminates connection with the ETT. (POP Tests 9-10) 3. Using the ETT logs, the tester verifies the Health IT Module generates unique identifiers for each message. (POP Test 12) 4. The tester verifies evidence of the Health IT Module’s ability to process connection requests initiated using STARTTLS with TLS_RSA_WITH_RC4_128_MD5 cipher suite. 5. The tester verifies evidence of the Health IT Module’s ability to process connection requests initiated using STARTTLS with TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA cipher suite. 6. Negative Test: Using the ETT logs, the tester verifies the Health IT Module rejects authentication requests due to invalid username/password. (POP Test 17) 7. Using the ETT logs, the tester verifies the Health IT Module is able to host attachments and make them available for fetching using POP. (POP Test 32)

(i)(C) – Receive Using Edge Protocol for IHE XDR profile for Limited Metadata Document Sources

Criteria ¶	System Under Test	Test Lab Verification
(i)(C)	<p><u>SUT Connection</u></p> <ol style="list-style-type: none"> The user executes HISP XDR Tests using the ETT for “System as Receiver.” The user establishes authentication from the ETT to the Health IT Module using Mutual TLS correctly (XDR Test 18). The user establishes authentication from the ETT to the Health IT Module using bad certificates (incorrect Mutual TLS configuration (XDR Test 19). <p><u>Receive Payload</u></p> <ol style="list-style-type: none"> The user enters the Health IT Module’s endpoints for receiving an XDR message from the ETT (as Edge) for Limited Metadata (XDR Test 13) and Full Metadata (XDR Test 14). The Health IT Module receives a properly formatted XDR message with limited metadata from the ETT (as Edge) and translates it to a Direct message sent to the ETT (as Destination HISP) (XDR Test 13). The Health IT Module receives a properly formatted XDR message with limited metadata from the ETT (as Edge) and translates it to a Direct message sent to the ETT (as Destination HISP) (XDR Test 14). <p><u>Incorrect XDR Message Receive</u></p> <ol style="list-style-type: none"> The Health IT Module returns errors when the following incorrect messages are received from the ETT (XDR Test 15): <ul style="list-style-type: none"> Invalid SOAP envelope details; Invalid SOAP body details; Missing metadata elements; Missing associations between ebRIM constructs; or Missing Direct Address block. 	<p><u>SUT Connection</u></p> <ol style="list-style-type: none"> Using the ETT, the tester verifies that the Health IT Module is capable of accepting and validating a Mutual TLS session when authenticating to the ETT. Using visual inspection of the logs, the tester verifies that the Health IT Module does not accept connections due to incorrect Mutual TLS configuration and an invalid certificate published by the ETT. <p><u>Receive Payload</u></p> <ol style="list-style-type: none"> Using visual inspection of the logs, the tester verifies that the Health IT Module is capable of receiving and processing a valid XDR message with limited metadata. Using visual inspection of the logs, the tester verifies that the Health IT Module is capable of receiving and processing a valid XDR message with full metadata. Using visual inspection of the logs, the tester verifies that the Health IT Module does not accept invalid messages sent from the ETT. <p><u>Incorrect XDR Message Receive</u></p> <ol style="list-style-type: none"> Using logs, the tester verifies that the Health IT Module recognizes that the messages sent from the ETT are invalid messages and rejects the bad messages.

(i)(C) – Receive Using Edge Protocol for SMTP

Criteria ¶	System Under Test	Test Lab Verification
(i)(C)	<p><u>SUT Connection</u></p> <ol style="list-style-type: none"> The user executes HISP SMTP Tests using the ETT for “System as Receiver.” Start TLS Session: The user initiates a TLS session for the Health IT Module with the ETT sent from email address wellformed3@edge.nist.gov to welformed1@edge.nist.gov (SMTP Test 16). Start TLS Session: The user initiates a TLS session for the Health IT Module with the ETT sent from badcommands4@edge.nist.gov to wellformed1@edge.nist.gov (SMTP Test 17). Authentication: The user authenticates the ETT with the Health IT Module using PLAIN SASL as an SMTP server from wellformed3@edge.nist.gov to wellformed1@edge.nist.gov (SMTP Test 20). The Health IT Module provides documentation of the ability to authenticate to an Edge using DIGEST-MD5 SASL as an SMTP server and reject authentication due to an invalid DIGEST-MD5 value. Authentication: The Health IT Module receives an authentication from the ETT using an Invalid PLAIN SASL username/password as an SMTP server from wellformed3@edge.nist.gov to wellformed1@edge.nist.gov (SMTP Test 22). <p><u>Receive Payload</u></p> <ol style="list-style-type: none"> The user receives a document from the ETT using valid SMTP commands from wellformed3@edge.nist.gov and establishes a connection with the ETT (SMTP Test 9). The user receives a document from the ETT using invalid data as part of the DATA command from badcommands@edge.nist.gov to wellformed1@edge.nist.gov (SMTP Test 10). <p style="text-align: right;">Continued on next page</p>	<p><u>SUT Connection</u></p> <ol style="list-style-type: none"> Using the ETT, the tester verifies all HISP SMTP test cases for “System as Receiver” are successful and valid. Using the ETT, the tester verifies a secure session was established with the Health IT Module based upon TLS initiation using correct syntax. Using the ETT, the tester verifies the Health IT Module does not accept the TLS session based upon incorrect syntax used. Using the ETT with a predetermined username and password, the tester verifies a secure session was established with the Health IT Module with PLAIN SASL authentication. The tester verifies evidence of the capability to establish a secure session with the Health IT Module based upon successful DIGEST-MD5 authentication. The tester verifies evidence of the capability to reject an authentication request due to an invalid DIGEST-MD5 value. Using the ETT, the tester verifies the Health IT Module does not accept an authentication request due to an invalid PLAIN SASL username and password. <p><u>Receive Payload</u></p> <ol style="list-style-type: none"> Using the ETT, the tester verifies the Health IT Module can receive an SMTP Message using §170.202(d): ONC Implementation Guide for Direct Edge Protocols v1.1, and the Validation Report indicates the successful sequence of commands for SMTP protocols. Using the ETT Logs, the tester verifies a secure connection cannot be established based upon invalid data provided and does not accept the data by using appropriate responses: <p style="text-align: right;">Continued on next page</p>

(i)(C) – Receive Using Edge Protocol for SMTP, continued

Criteria ¶	System Under Test	Test Lab Verification
(i)(C), continued	<p>Continued from previous page</p> <p>9. The user receives a document from the ETT using invalid SMTP commands as part of the DATA command from badcommands@edge.nist.gov to wellformed1@edge.nist.gov (SMTP Test 11).</p> <p>10. The user receives a document from the ETT using data beyond allowable size limits from badcommands@edge.nist.gov to wellformed1@edge.nist.gov (SMTP Test 12 – cannot be tested as these are not invalid per specification as RFC 2821 does not mandate any failure on large sizes).</p> <p>11. The user receives a document from the ETT from badcommands@edge.nist.gov to wellformed1@edge.nist.gov beyond the allowable time period (SMTP Test 13).</p>	<p>Continued from previous page</p> <ul style="list-style-type: none"> • Invalid DATA command; • Invalid SMTP commands; or • Invalid size limits of SMTP commands. <p>10. Using the ETT, the tester verifies the Health IT Module has kept the transaction open for beyond the specified time constraints found with RFC 2821, Section 4.5.3.2, and therefore cannot accept the incoming message.</p>

(h)(2)(ii) Applicability Statement for Secure Health Transport and Delivery Notification in Direct

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

Standards:

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

Tools:

[Edge Testing Tool \(ETT\)](#)

(ii) Send

(ii) Send

Criteria ¶	System Under Test	Test Lab Verification
<p>(ii) Send</p>	<ol style="list-style-type: none"> The user selects “HISP Testing & Delivery Notification” within the ETT. The user selects the “Message Tracking” tab and selects the option for Your system as “Sender”. <p><u>Disposition-Notification-Options Header</u></p> <ol style="list-style-type: none"> The Health IT Module is able to successfully process the Disposition-Notifications-Options-Header received from the ETT (as Sending Edge) and include it in the message to the destination (ETT as Destination HISP): <ul style="list-style-type: none"> Using SMTP: SMTP MT Test 21 Using IMAP: SMTP/IMAP MT Test 21 (Alternative) Using POP3: SMTP/POP MT Test 21 (Alternative) Negative Test: The Health IT Module is able to successfully process an invalid Disposition-Notifications-Options-Header received from the ETT (as Sending Edge) and sends a successful handoff status to the ETT (as Sending Edge). The ETT (as Destination HISP) will send an error/failure to the Health IT Module: <ul style="list-style-type: none"> Using SMTP: SMTP MT Test 22 Using IMAP: SMTP/IMAP MT Test 22 (Alternative) Using POP3: SMTP/POP MT Test 22 (Alternative) <p><u>Delivery Failure Due to Bad Destination Address</u></p> <ol style="list-style-type: none"> The Health IT Module is able to successfully process a message from the ETT (as Sending Edge) with a bad address (non-existent) for the destination, send the message to the ETT (as Destination HISP), which will return an error as it will be unable to deliver the message to the address. The Health IT Module sends the ETT (as Sending Edge) a negative delivery status notification message via: <ul style="list-style-type: none"> SMTP MT Test 23 SMTP/IMAP MT Test 23 (Alternative) SMTP/POP MT Test 23 (Alternative) <p style="text-align: right;">Continued on next page</p>	<p><u>Disposition-Notification-Options Header</u></p> <ol style="list-style-type: none"> The ETT test results for the following tests are successful: <ul style="list-style-type: none"> SMTP MT Test 21 SMTP/IMAP MT Test 21 (Alternative) SMTP/POP MT Test 21 (Alternative) Negative Test: The ETT test results for the following tests are successful: <ul style="list-style-type: none"> SMTP MT Test 22 SMTP/IMAP MT Test 22 (Alternative) SMTP/POP MT Test 22 (Alternative) <p><u>Delivery Failure Due to Bad Destination Address</u></p> <ol style="list-style-type: none"> The ETT test results for the following tests are successful: <ul style="list-style-type: none"> SMTP MT Test 23 SMTP/IMAP MT Test 23 (Alternative) SMTP/POP MT Test 23 (Alternative) <p><u>Delivery Failure Due to Untrusted Destination HISP</u></p> <ol style="list-style-type: none"> The ETT test results for the following tests are successful: <ul style="list-style-type: none"> SMTP MT Test 24 SMTP/IMAP MT Test 24 (Alternative) SMTP/POP MT Test 24 (Alternative) <p><u>Delivery Failure Due to Unpublished Certificate for Destination HISP</u></p> <ol style="list-style-type: none"> The ETT test results for the following tests are successful: <ul style="list-style-type: none"> SMTP MT Test 25 SMTP/IMAP MT Test 25 (Alternative) SMTP/POP MT Test 25 (Alternative) <p style="text-align: right;">Continued on next page</p>

(ii) Send, continued

Criteria ¶	System Under Test	Test Lab Verification
<p>(ii) Send, continued</p>	<p>Continued from previous page</p> <p><u>Delivery Failure Due to Untrusted Destination HISP</u></p> <p>6. The Health IT Module is able to successfully process a message from the ETT (as Sending Edge) with a valid address for the destination, send the message to the ETT (as an untrusted Destination HISP). The Health IT Module sends the ETT (as Sending Edge) a negative delivery status notification message via:</p> <ul style="list-style-type: none"> • SMTP MT Test 24 • SMTP/IMAP MT Test 24 (Alternative) • SMTP/POP MT Test 24 (Alternative) <p><u>Delivery Failure Due to Unpublished Certificate for Destination HISP</u></p> <p>7. The Health IT Module is able to successfully process a message from the ETT (as Sending Edge) with a valid address for the destination, send the message to the ETT (as Destination HISP). Due to the unpublished certificate, security and trust processing fails. The Health IT Module sends the ETT (as Sending Edge) a negative delivery status notification message via:</p> <ul style="list-style-type: none"> • SMTP MT Test 25 • SMTP/IMAP MT Test 25 (Alternative) • SMTP/POP MT Test 25 (Alternative) <p><u>Delivery Failure Timeout for Processed MDN</u></p> <p>8. The Health IT Module is able to successfully process a message from the ETT (as Sending Edge) with a valid address for the destination, send the message to the ETT (as Destination HISP). The wait time for the Health IT Module to receive a Processed MDN from the Destination HISP is exceeded. The Health IT Module sends the ETT (as Sending Edge) a negative delivery status notification message via:</p> <p style="text-align: right;">Continued on next page</p>	<p>Continued from previous page</p> <p><u>Delivery Failure Timeout for Processed MDN</u></p> <p>6. The ETT test results for the following tests are successful:</p> <ul style="list-style-type: none"> • SMTP MT Test 26 • SMTP/IMAP MT Test 26 (Alternative) • SMTP/POP MT Test 26 (Alternative) <p><u>Delivery Failure for Dispatched MDN</u></p> <p>7. The ETT test results for the following tests are successful:</p> <ul style="list-style-type: none"> • SMTP MT Test 27 • SMTP/IMAP MT Test 27 (Alternative) • SMTP/POP MT Test 27 (Alternative) <p><u>Delivery Failure Timeout for Dispatched MDN</u></p> <p>8. The ETT test results for the following tests are successful:</p> <ul style="list-style-type: none"> • SMTP MT Test 28 • SMTP/IMAP MT Test 28 (Alternative) • SMTP/POP MT Test 28 (Alternative) <p><u>Delivery Failure Timeout for Dispatched MDN</u></p> <p>9. The ETT test results for the following tests are successful:</p> <ul style="list-style-type: none"> • SMTP MT Test 29 • SMTP/IMAP MT Test 29 (Alternative) • SMTP/POP MT Test 29 (Alternative) <p><u>Requesting Delivery Notification for XDR Edge HISP</u></p> <p>10. The ETT test results for XDR MT Test 30 are successful.</p> <p>11. The ETT test results for XDR MT Test 31 are successful.</p> <p><u>XDR Delivery Failure: Bad Address</u></p> <p>12. The ETT test results for XDR MT Test 32 are successful.</p> <p><u>XDR Delivery Failure: Untrusted Destination HISP</u></p> <p>13. The ETT test results for XDR MT Test 33 are successful.</p> <p style="text-align: right;">Continued on next page</p>

(ii) Send, continued

Criteria ¶	System Under Test	Test Lab Verification
<p>(ii) Send, continued</p>	<p>Continued from previous page</p> <ul style="list-style-type: none"> • SMTP MT Test 26 • SMTP/IMAP MT Test 26 (Alternative) • SMTP/POP MT Test 26 (Alternative) <p><u>Delivery Failure for Dispatched MDN</u></p> <p>9. The Health IT Module is able to successfully process a message from the ETT (as Sending Edge) with a valid address for the destination, send the message to the ETT (as Destination HISP) which provides a Processed MDN but does not provide a Dispatched MDN to the Health IT Module. The Health IT Module sends the ETT (as Sending Edge) a negative delivery status notification message via:</p> <ul style="list-style-type: none"> • SMTP MT Test 27 • SMTP/IMAP MT Test 27 (Alternative) • SMTP/POP MT Test 27 (Alternative) <p><u>Delivery Failure Timeout for Dispatched MDN</u></p> <p>10. The Health IT Module is able to successfully process a message from the ETT (as Sending Edge) with a valid address for the destination, send the message to the ETT (as Destination HISP) which provides a Processed MDN to the Health IT Module. The Health IT Module receives a Dispatched MDN after the expected wait time is exceeded. The Health IT Module sends the ETT (as Sending Edge) a negative delivery status notification and does not forward the dispatched MDN to the ETT (as Sending Edge) message via:</p> <ul style="list-style-type: none"> • SMTP MT Test 28 • SMTP/IMAP MT Test 28 (Alternative) • SMTP/POP MT Test 28 (Alternative) <p style="text-align: right;">.Continued on next page</p>	<p>Continued from previous page</p> <p><u>XDR Delivery Failure: Unpublished Destination HISP Certificate</u></p> <p>14. The ETT test results for XDR MT Test 34 are successful.</p> <p><u>XDR Delivery Failure: No Processed MDN</u></p> <p>15. The ETT test results for XDR MT Test 35 are successful.</p> <p><u>XDR Delivery Failure: No Dispatched MDN</u></p> <p>16. The ETT test results for XDR MT Test 36 are successful.</p> <p><u>XDR Delivery Failure: Timeout for Dispatched MDN</u></p> <p>17. The ETT test results for XDR MT Test 37 are successful.</p> <p><u>XDR Positive Delivery Notification</u></p> <p>18. The ETT test results for XDR MT Test 38 are successful.</p>

(ii) Send, continued

Criteria ¶	System Under Test	Test Lab Verification
<p>(ii) Send, continued</p>	<p>Continued from previous page</p> <p><u>Positive Delivery Notification</u></p> <p>11. The Health IT Module is able to successfully process a message from the ETT (as Sending Edge) with a valid address for the destination, send the message to the ETT (as Destination HISP) which provides a Processed MDN and Dispatched MDN to the Health IT Module. The Health IT Module only sends the ETT (as Sending Edge) a positive delivery status notification (dispatched MDN) message via:</p> <ul style="list-style-type: none"> • SMTP MT Test 29 • SMTP/IMAP MT Test 29 (Alternative) • SMTP/POP MT Test 29 (Alternative) <p><u>Requesting Delivery Notification for XDR Edge HISP</u></p> <p>12. The Health IT Module is able to successfully process a message from the ETT (as Sending Edge) that includes a valid Direct address block header and valid destination. The Health IT Module includes the header in the message to the ETT (as Destination HISP) within SMTP headers via XDR MT Test 30.</p> <p>13. The Health IT Module is able to successfully process a message from the ETT (as Sending Edge) that includes a valid Direct address block header and invalid destination. The Health IT Module is able to process the header handle an invalid delivery notification request via XDR MT Test 31.</p> <p><u>XDR Delivery Failure: Bad Address</u></p> <p>14. The Health IT Module is able to successfully process a message from the ETT (as Sending Edge) that includes an invalid (non-existent) address. The Health IT Module sends a negative delivery status notification message to the ETT (as Sending Edge) using XDR profile via XDR MT Test 32.</p> <p style="text-align: right;">Continued on next page</p>	<p>See previous page</p>

(ii) Send, continued

Criteria ¶	System Under Test	Test Lab Verification
<p>(ii) Send, continued</p>	<p>Continued from previous page</p> <p><u>XDR Delivery Failure: Untrusted Destination HISP</u></p> <p>15. The Health IT Module is able to successfully process a message from the ETT (as Sending Edge) to a valid address. The ETT (as Destination HISP) is not trusted and the Health IT Module sends a negative delivery status notification message to the ETT (as Sending Edge) using XDR profile via XDR MT Test 33.</p> <p><u>XDR Delivery Failure: Unpublished Destination HISP Certificate</u></p> <p>16. The Health IT Module is able to successfully process a message from the ETT (as Sending Edge) to a valid address. The ETT (as Destination HISP) does not have published certificates, and security and trust processing fails. The Health IT Module sends a negative delivery status notification message to the ETT (as Sending Edge) using XDR profile via XDR MT Test 34.</p> <p><u>XDR Delivery Failure: No Processed MDN</u></p> <p>17. The Health IT Module is able to successfully process a message from the ETT (as Sending Edge) to a valid address. The ETT (as Destination HISP) does not respond with a Processed MDN. The Health IT Module sends a negative delivery status notification message to the ETT (as Sending Edge) using XDR profile via XDR MT Test 35.</p> <p><u>XDR Delivery Failure: No Dispatched MDN</u></p> <p>18. The Health IT Module is able to successfully process a message from the ETT (as Sending Edge) to a valid address. The ETT (as Destination HISP) responds with a Processed MDN, but no Dispatched MDN. The Health IT Module sends a negative delivery status notification message to the ETT (as Sending Edge) using XDR profile via XDR MT Test 36.</p> <p style="text-align: right;">Continued on next page</p>	<p>See previous page</p>

(ii) Send, continued

Criteria ¶	System Under Test	Test Lab Verification
<p>(ii) Send, continued</p>	<p>Continued from previous page</p> <p><u>XDR Delivery Failure: Timeout for Dispatched MDN</u></p> <p>19. The Health IT Module is able to successfully process a message from the ETT (as Sending Edge) to a valid address. The ETT (as Destination HISP) responds with a Processed MDN, but the Dispatched MDN is received after the expected wait time has exceeded. The Health IT Module sends a negative delivery status notification message to the ETT (as Sending Edge) using XDR profile via XDR MT Test 37.</p> <p><u>XDR Positive Delivery Notification</u></p> <p>20. The Health IT Module is able to successfully process a message from the ETT (as Sending Edge) to a valid address. The ETT (as Destination HISP) responds with a Processed MDN and Dispatched MDN within the expected time period. The Health IT Module sends only one positive delivery status notification message to the ETT (as Sending Edge) using XDR profile via XDR MT Test 38.</p>	

(ii) – Receive

Criteria ¶	System Under Test	Test Lab Verification
<p>(ii) Receive,</p>	<ol style="list-style-type: none"> 1. The user selects “HISP Testing & Delivery Notification” within the ETT. 2. The user selects the “Message Tracking” tab and selects the option for Your system as “Receiver”. <p><u>SMTP: Disposition-Notification-Options Header</u></p> <ol style="list-style-type: none"> 3. 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 include it in the message to the destination via SMTP/IMAP MT Test 39. 4. Negative Test: 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 include it in the message to the destination via SMTP/IMAP MT Test 40. <p><u>SMTP: Failure Notification (Configurable Wait Time Exceeded)</u></p> <ol style="list-style-type: none"> 5. The Health IT Module receives a message from the ETT (as Sending HISP) and is unable to deliver the message to its final destination (ETT as Destination Edge). The Health IT Module delivers a Processed MDN to the ETT (as Sending HISP) followed by a delivery failure message to the ETT (as Sending HISP) after the wait time has exceeded for delivering the message to its final destination via SMTP/IMAP MT Test 41. <p><u>SMTP: Failure Notification</u></p> <ol style="list-style-type: none"> 6. The Health IT Module receives a message from the ETT (as Sending HISP), and is unable to deliver the message to its final destination (ETT as Destination Edge) due to a bad address. The Health IT Module delivers a Processed MDN to the ETT (as Sending HISP) followed by a delivery failure message to the ETT (as Sending HISP) due to the bad address via SMTP/IMAP MT Test 42. <p style="text-align: right;">Continued on next page</p>	<p><u>SMTP: Disposition-Notification-Options Header</u></p> <ol style="list-style-type: none"> 1. The ETT test results for XDR MT Test 39 are successful. 2. The ETT test results for XDR MT Test 40 are successful. <p><u>SMTP: Failure Notification (Configurable Wait Time Exceeded)</u></p> <ol style="list-style-type: none"> 3. The ETT test results for XDR MT Test 41 are successful. <p><u>SMTP: Failure Notification</u></p> <ol style="list-style-type: none"> 4. The ETT test results for XDR MT Test 42 are successful. <p><u>XDR: Failure Notification (Configurable Wait Time Exceeded)</u></p> <ol style="list-style-type: none"> 5. The ETT test results for XDR MT Test 43 are successful. <p><u>XDR: Failure Notification</u></p> <ol style="list-style-type: none"> 6. The ETT test results for XDR MT Test 43 are successful.

(ii) – Receive, continued

Criteria ¶	System Under Test	Test Lab Verification
(ii) Receive, continued	<p>Continued from previous page</p> <p><u>XDR: Failure Notification (Configurable Wait Time Exceeded)</u></p> <p>7. The Health IT Module receives a message from the ETT (as Sending HISP) and is unable to deliver the message to its final destination (ETT as Destination Edge). The Health IT Module delivers a Processed MDN to the ETT (as Sending HISP) followed by a delivery failure message to the ETT (as Sending HISP) after the wait time has exceeded for delivering the message to its final destination via XDR MT Test 43.</p> <p><u>XDR: Failure Notification</u></p> <p>8. The Health IT Module receives a message from the ETT (as Sending HISP), and is unable to deliver the message to its final destination (ETT as Destination Edge) due to a bad address. The Health IT Module delivers a Processed MDN to the ETT (as Sending HISP) followed by a delivery failure message to the ETT (as Sending HISP) due to the bad address via XDR MT Test 44.</p>	

Required Enhanced Testing: Direct v1.2

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): Applicability Statement for Secure Health Transport v1.2, formatted only as a “wrapped” message.

(i)(A) – Send

Criteria ¶	System Under Test	Test Lab Verification
<p>(i)(A) Required Enhanced Testing</p>	<p>The Health IT Module provides evidence and demonstrates 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): Applicability Statement for Secure Health Transport v1.2, which includes:</p> <ul style="list-style-type: none"> • Documentation of the Health IT Module sending “Wrapped” RFC-5751 messages to 3 partner HISPs. • Documentation of the Health IT Module receiving processed Message Disposition Notifications (MDNs) from each of the 3 partner HISPs generated by the partner HISPs upon receiving the Direct message from the Health IT Module. 	<p>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): Applicability Statement for Secure Health Transport v1.2. The verification includes:</p> <ul style="list-style-type: none"> • 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 Message Disposition Notifications (MDNs) from each of the 3 partner HISPs generated upon receiving the Direct message from the Health IT Module.

(i)(A) – Receive

Criteria ¶	System Under Test	Test Lab Verification
<p>(i)(A) Required Enhanced Testing</p>	<p>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): Applicability Statement for Secure Health Transport v1.2. The evidence includes:</p> <ul style="list-style-type: none"> • Documentation of the Health IT Module receiving “Wrapped” RFC-5751 messages from 3 partner HISPs • Documentation of the Health IT Module generates and sends processed Message Disposition Notifications (MDNs) that are transmitted to each of the 3 partner HISPs generated upon successfully receiving a Direct message from the Health IT Module. 	<p>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): Applicability Statement for Secure Health Transport v1.2. The documentation includes:</p> <ul style="list-style-type: none"> • Indication that the Health IT Module successfully received “Wrapped” RFC-5751 messages from 3 separate and unrelated HISP partners. • Indication of the Health IT Module generating and transmitting processed Message Disposition Notification (MDNs) to each of the 3 partner HISPs generated upon receiving the Direct message from each partner HISP.

Required Enhanced Testing: ONC XDR and XDM for Direct

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(b): ONC XDR and XDM for Direct Messaging Specification (incorporated by reference in § 170.299), including support for both limited and full XDS metadata profiles, formatted only as a “wrapped” message.

(i)(B) – Send

Criteria ¶	System Under Test	Test Lab Verification
<p>(i)(B) Required Enhanced Testing</p>	<p>The Health IT Module provides evidence and demonstrates 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(b) ONC XDR and XDM for Direct Messaging Specification which includes:</p> <ul style="list-style-type: none"> • Documentation of the Health IT Module sending “Wrapped” RFC-5751 messages to 3 partner HISPs. • Documentation of the Health IT Module receiving processed Message Disposition Notifications (MDNs) from each of the 3 partner HISPs generated by the partner HISPs upon receiving the Direct message from the Health IT Module. 	<p>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(b) ONC XDR and XDM for Direct Messaging Specification. The verification includes:</p> <ul style="list-style-type: none"> • 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 Message Disposition Notifications (MDNs) from each of the 3 partner HISPs generated upon receiving the Direct message from the Health IT Module.

(i)(B) – Receive

Criteria ¶	System Under Test	Test Lab Verification
<p>(i)(B) Required Enhanced Testing</p>	<p>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 §170.202(b) ONC XDR and XDM for Direct Messaging Specification. The evidence includes:</p> <ul style="list-style-type: none"> • Documentation of the Health IT Module receiving “Wrapped” RFC-5751 messages from 3 partner HISPs • Documentation of the Health IT Module generates and sends processed Message Disposition Notifications (MDNs) that are transmitted to each of the 3 partner HISPs generated upon successfully receiving a Direct message from the Health IT Module. 	<p>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(b) ONC XDR and XDM for Direct Messaging Specification. The documentation includes:</p> <ul style="list-style-type: none"> • Indication that the Health IT Module successfully received “Wrapped” RFC-5751 messages from 3 separate and unrelated HISP partners. • Indication of the Health IT Module generating and transmitting processed Message Disposition Notification (MDNs) to each of the 3 partner HISPs generated upon receiving the Direct message from each partner HISP.

Document History

Version Number	Description of Change	Date
1.0	Released for Comment - NPRM	January 29, 2016

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