

2015 Edition §170.315(h)(2) Direct Project, Edge Protocol, and XDR-XDM					
Testing Components:					
				Data	
Test Procedure Version 1.1 – Last Updated 12/4/15					

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

Tools:

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

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

(i)(A) – Send

Criteria ¶	System Under Test	Test Lab Verification
(i)(A)	<ol style="list-style-type: none"> 1. Discover Certificates: 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. 2. Discover Certificates: 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). 3. The user selects “2014 Direct” within the Edge Testing Tool (ETT) to access the Direct testing functions. 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. 5. The user identifies the payload for sending to the ETT. ONC-supplied payloads are available for download from the Home page of the ETT. 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): ONC Applicability Statement for Secure Health Transport using the developer-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. 	<ol style="list-style-type: none"> 1. Discover Certificates: 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 ONC Applicability Statement for Secure Health Transport v1.2. 2. 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. 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.

Criteria ¶	System Under Test	Test Lab Verification
	<p>8. The user provides evidence and demonstrates 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, which includes:</p> <ul style="list-style-type: none"> • Documentation of the Health IT module sending “Wrapped” RFC-5751 messages to 3 partner HISPs • Demonstration 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>6. 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. The verification includes:</p> <ul style="list-style-type: none"> • Indication through documentation that the Health IT module sent “Wrapped” RFC-5751 messages • Evidence through demonstration 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
(i)(A)	<ol style="list-style-type: none"> 1. Hosting Certificates: The user performs setup tasks to test hosting of certificates by entering the Health IT module’s Direct address within DCDT. 2. Hosting Certificates: 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. 3. The user selects “2014 Direct” 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 sign of health information in accordance with the standard specified at §170.202(a)(2): ONC Applicability Statement for Secure Health Transport. 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 RFC-5751 “wrapped” health information sent from ETT using Direct in accordance with the standard specified at §170.202(a)(2) ONC Applicability Statement for Secure Health Transport and sends corresponding MDNs. 8. The user rejects health information sent from ETT that is not in accordance with the standard specified at §170.202(a)(2) ONC Applicability Statement for Secure Health Transport. 	<ol style="list-style-type: none"> 1. Hosting Certificates: The tester shall verify that the Health IT module’s hosted certificates are discoverable as displayed on screen for the DCDT test cases executed. 2. The tester verifies that health information can be successfully received by the Health IT module from the ETT accordance with the standard specified at §170.202(a)(2), using “wrapped” RFC-5751 messages. 3. The tester shall verify that an MDN from the Health IT module was received by the ETT for all messages in Step 2. 4. 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 5. 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. 6. 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. 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. 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.

Criteria ¶	System Under Test	Test Lab Verification
	<p>9. 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. The evidence includes documentation of:</p> <ul style="list-style-type: none"> • The Health IT module is receiving “Wrapped” RFC-5751 messages from 3 partner HISPs • The Health IT module is generating and sending processed Message Disposition Notifications (MDNs) that are transmitted to each of the 3 partner HISPs generated upon successfully receiving a Direct message from the partner HISP. 	<p>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.</p> <p>10. 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. The documentation includes:</p> <ul style="list-style-type: none"> • Indication that the Health IT module successfully received “Wrapped” RFC-5751 messages • Evidence of the Health IT module generating and transmitting processed Message Disposition Notifications (MDNs) to each of the 3 partner HISPs generated upon receiving the Direct message from the partner HISP.

(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:

[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
(i)(B)	<ol style="list-style-type: none"> 1. Discover Certificates: 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. 2. Discover Certificates: 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). 3. The user selects “2014 Direct” within the ETT to access the Direct testing functions. 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. 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. 5. 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. 	<ol style="list-style-type: none"> 1. Discover Certificates: 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 ONC Applicability Statement for Secure Health Transport v1.2. 2. 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. 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 with XDR/XDM in accordance with the standard specified at §170.202(b), using RFC-5751 “wrapped” messages. 5. 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.

Criteria ¶	System Under Test	Test Lab Verification
	<p>6. 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> <p>7. The XDM package sent by the Health IT module is able to be successfully validated using the Transport Testing Tool (TTT) Message Validator.</p> <p>8. The user provides evidence 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, which includes:</p> <ul style="list-style-type: none"> • Documentation of the Health IT module sending “Wrapped” RFC-5751 messages to 3 partner HISPs • Demonstration 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>6. 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> <p>7. Using the XDM payload returned by the ETT to the Contact Email address provided by the Health IT module user, the tester uploads the XDM payload to the TTT’s Message Validator to verify the XDM package is valid.</p> <p>8. 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. The verification includes:</p> <ul style="list-style-type: none"> • Indication through documentation that the Health IT module sent “Wrapped” RFC-5751 messages • Evidence through demonstration 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) – 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 ETT and provide a name for each ETT connection. 2. The user sends the payload to the ETT using SOAP Protocols with XDR Validation with limited metadata to the ETT's SOAP endpoint. 3. The user sends the payload to the ETT using SOAP Protocols with XDR Validation with full metadata to the ETT'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 ETT. 2. Using the validation report, the tester verifies the payload using full XDS metadata was successfully received by the ETT.

(i)(B) – Receive using Direct + XDM

Criteria ¶	System Under Test	Test Lab Verification
(i)(B)	<ol style="list-style-type: none"> 1. Hosting Certificates: The user performs setup tasks to test hosting of certificates by entering the Health IT module's Direct address within DCDT. 2. Hosting Certificates: 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. 3. The user selects "2014 Direct" 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 sign 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. 	<ol style="list-style-type: none"> 1. Hosting Certificates: The tester verifies that the Health IT module's hosted certificates are discoverable as displayed on screen for the DCDT test cases executed. 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. 5. 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.

Criteria ¶	System Under Test	Test Lab Verification
(i)(B)	<p>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.</p> <p>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.</p> <p>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> <p>9. The Health IT module rejects health information sent from ETT that is not in accordance with the standard specified at §170.202(a)(2) ONC XDR and XDM for Direct Messaging Specification.</p> <p>10. 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. The evidence includes documentation of:</p> <ul style="list-style-type: none"> • The Health IT module receiving “Wrapped” RFC-5751 messages from 3 partner HISPs • The Health IT module generating and sending processed Message Disposition Notifications (MDNs) that are transmitted to each of the 3 partner HISPs generated upon successfully receiving a Direct message from the partner HISP. 	<p>6. 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> <p>7. 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>8. 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. 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>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.</p> <p>10. 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. The documentation includes:</p> <ul style="list-style-type: none"> • Indication that the Health IT module successfully received “Wrapped” RFC-5751 messages • Evidence of the Health IT module generating and transmitting processed Message Disposition Notifications (MDNs) to each of the 3 partner HISPs generated upon receiving the Direct message from the partner HISP.

(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 ETT for each message. 2. The user shall define and identify an Actor Simulator in the ETT terminology (as described in the ETT User Guide). 3. The user receives health information from the ETT using SOAP Protocols with XDR Validation with limited metadata. 4. The user receives health information from the ETT using SOAP Protocols with XDR Validation with full metadata. 5. The user receives health information from the ETT 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 ETT 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 ETT 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 ETT 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

Criteria ¶	System Under Test	Test Lab Verification
(i)(C)	<ol style="list-style-type: none"> 1. The user shall execute XDR Tests using the ETT for “System as Sender.” 2. Authentication: The user establishes a Mutual TLS session for the Health IT module to authenticate to the ETT (XDR Test 6). 3. Authentication: The user authenticates the Health IT module to the ETT using an incorrect Mutual TLS session (XDR Test 7). 4. Send: The user provides the Health IT module’s Direct “From” address to generate endpoints for Limited Metadata (XDR Test 1) and Full Metadata (XDR Test 2). 5. Message Tracking Using Processed MDNs: The user sends 3 messages to the ETT with unique message IDs for each XDR profile (XDR Test 19). 6. Message Tracking Using Processed MDNs: The user sends health information to multiple recipients including both valid (Endpoint 5) and invalid recipients (Endpoint 9) (XDR Test 20a, XDR Test 20b). 	<ol style="list-style-type: none"> 1. Using the ETT, the tester verifies all XDR test cases for “System as Sender” are successful and valid. 2. Using the ETT, the tester verifies the Health IT module establishes a mutual TLS session prior to transmitting any data and disconnects when the ETT provides an invalid certificate and incorrect Mutual TLS configuration. 3. Using the ETT, the tester verifies the Health IT module can send an XDR Message using limited metadata and full metadata using §170.202(d): ONC Implementation Guide for Direct Edge Protocols v1.1. 4. Using the ETT, the tester verifies the Health IT module successfully performs message tracking using processed MDNs.

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

Criteria ¶	System Under Test	Test Lab Verification
(i)(C)	<ol style="list-style-type: none"> 1. The user shall execute SMTP Tests using the ETT for “System as Sender.” 2. 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). 3. Start TLS Session: The user initiates a TLS session for the Health IT module with the ETT using address 15 (SMTP Test 15 – not supported at this time). 4. 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). 5. Authentication to SMTP Server: The user authenticates the Health IT module to the ETT using DIGEST-MD5 SASL using email address wellformed1@edge.nist.gov (SMTP Test 19 – not supported at this time). 6. Send: The user sends a document to the ETT using the email address wellformed1@edge.nist.gov (SMTP Tests 1-8). 7. Message Tracking Using Processed MDNs: The user sends 3 messages to the ETT with unique message IDs for each message to wellformed14@edge.nist.gov (MU Tracking Step 17). 8. Message Tracking Using Processed MDNs: The user sends health information in a single SMTP message to processedonly5@edge.nist.gov and noaddressfailure@edge.nist.gov (MU Tracking Step 18). 	<ol style="list-style-type: none"> 1. Using the ETT, the tester verifies all SMTP test cases for “System as Sender” are successful and valid. 2. Using the ETT, the tester verifies the Health IT module initiates a TLS session and can authenticate using PLAIN SASL and DIGEST-MD5 SASL authentication. 3. Using the ETT, the tester verifies the Health IT module can send an SMTP Message using §170.202(d): ONC Implementation Guide for Direct Edge Protocols v1.1. 4. Using the ETT, the tester verifies the Health IT module successfully performs message tracking using processed MDNs.

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

Criteria ¶	System Under Test	Test Lab Verification
(i)(C)	<ol style="list-style-type: none"> 1. The user shall execute XDR Tests using the ETT for “System as Receiver.” 2. Authentication: The user establishes authentication from the ETT to the Health IT module using Mutual TLS correctly (XDR Test 8). 3. Authentication: The user establishes authentication from the ETT to the Health IT module using bad certificates (incorrect Mutual TLS configuration (XDR Test 9). 4. Receive: The Health IT module receives a properly formatted XDR message with limited metadata from the ETT (XDR Test 3). 5. Receive: The Health IT module receives a properly formatted XDR message with full metadata from the ETT (XDR Test 5). 6. Incorrect XDR Message Receive: The Health IT module returns errors when the following incorrect messages are received from the ETT (XDR Test 4): <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. 	<ol style="list-style-type: none"> 1. Using the ETT, the tester verifies all XDR test cases for “System as Receiver” are successful and valid. 2. Using the ETT, the tester verifies the Health IT module is capable of accepting a validating a Mutual TLS session when authenticating to the ETT. 3. Using visual inspection of the logs, the tester verifies the Health IT module does not accept connections due to incorrect Mutual TLS configuration and an invalid certificate published by the ETT. 4. Using visual inspection of the logs, the tester verifies the Health IT module is capable of receiving and processing a valid XDR message with limited metadata. 5. Using visual inspection of the logs, the tester verifies the Health IT module is capable of receiving and processing a valid XDR message with full metadata. 6. Using visual inspection of the logs, the tester verifies the Health IT module does not accept invalid messages sent from the ETT.

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

Criteria ¶	System Under Test	Test Lab Verification
(i)(C)	<ol style="list-style-type: none"> 1. The user shall execute SMTP Tests using the ETT for “System as Receiver.” 2. 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). 3. Start TLS Session: The user initiates a TLS session for the Health IT module with the ETT sent from badcommands4@edge.nist.gov to welformed1@edge.nist.gov (SMTP Test 17). 4. Authentication: The user authenticates the ETT with the Health IT module using PLAIN SASL as an SMTP server from wellformed3@edge.nist.gov to welformed1@edge.nist.gov (SMTP Test 20). 5. Authentication: The user authenticates the ETT using DIGEST-MD5 SASL as an SMTP server from wellformed3@edge.nist.gov to welformed1@edge.nist.gov (SMTP Test 21 – cannot be tested at this time). 6. 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 welformed1@edge.nist.gov (SMTP Test 22). 7. Authentication: The Health IT module receives an authentication from the ETT using an Invalid DIGEST-MD5 as an SMTP server from wellformed3@edge.nist.gov to welformed1@edge.nist.gov (SMTP Test 23 – cannot be tested at this time). 8. Receive: 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). 	<ol style="list-style-type: none"> 1. Using the ETT, the tester verifies all SMTP test cases for “System as Receiver” are successful and valid. 2. Using the ETT, the tester verifies a secure session was established with the Health IT module based upon TLS initiation using correct syntax. 3. Using the ETT, the tester verifies the Health IT module does not accept the TLS session based upon incorrect syntax used. 4. 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. 5. Using the ETT, the tester verifies a secure session was established with the Health IT module based with successful DIGEST-MD5 authentication. 6. Using the ETT, the tester verifies the Health IT module does not accept the authentication request due to an invalid PLAIN SASL username and password. 7. Using the ETT, the tester verifies the Health IT module does not accept the authentication request due to a DIGEST-MD5 value. 8. 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. 9. 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: <ul style="list-style-type: none"> • Invalid DATA command; • Invalid SMTP commands; or • Invalid size limits of SMTP commands.

Criteria ¶	System Under Test	Test Lab Verification
	<p>9. Receive: 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> <p>10. Receive: 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>11. Receive: 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>12. Receive: 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>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>

(i)(C) – Receive Using Edge Protocol for IMAP (Optional)

Criteria ¶	System Under Test	Test Lab Verification
(i)(C)	<ol style="list-style-type: none"> 1. The user shall execute IMAP Tests using the ETT for “System as Receiver.” 2. Authentication: The user initiates an IMAP session with STARTTLS and PLAIN SSL authentication with the ETT. 3. The user demonstrates the Health IT module can use either the uppercase, lowercase, or mixed case mailbox names or access data. 4. The user demonstrates the Health IT module’s capability to deal with exceptions for different commands, including bad commands from the ETT. 5. The Health IT module is able to receive status and size updates from the IMAP4 server. 	<ol style="list-style-type: none"> 1. Using the ETT, the tester verifies all IMAP test cases for “System as Receiver” are successful and valid.

(i)(C) – Receive Using Edge Protocol for POP3 (Optional)

Criteria ¶	System Under Test	Test Lab Verification
(i)(C)	<ol style="list-style-type: none"> 1. The user shall execute POP3 Tests using the ETT for “System as Receiver.” 2. Authentication: The user initiates a POP session with STARTTLS and PLAIN SSL authentication with the ETT. 3. The user demonstrates the Health IT module’s capability to deal with exceptions for different commands, including bad commands from the ETT. 	<ol style="list-style-type: none"> 1. Using the ETT, the tester verifies all POP3 test cases for “System as Receiver” are successful and valid.

(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

Criteria ¶	System Under Test	Test Lab Verification
(ii)	<ol style="list-style-type: none"> 1. The user enters the Health IT module's profile information into the Edge Testing Tool (ETT) with the HISP as Sender. 2. Execute ETT Test Cases for HISP as Sender. 	<ol style="list-style-type: none"> 1. (Successful Flow 1): The tester verifies the Health IT module sends both a successful handoff message and success notification to the ETT (as Sending Edge) if no security and trust processing is necessary. 2. (Successful Flow 2): The tester verifies the Health IT module returns a successful handoff status to the ETT (as Sending Edge) upon receipt of the message. 3. (Successful Flow 2): The tester verifies a processed MDN is received by the Health IT module and is decrypted with trust verified. 4. (Successful Flow 2): The tester verifies a dispatched MDN is received by the Health IT module and is decrypted with trust verified. 5. (Successful Flow 2): The tester verifies the Health IT module sends a success notification to the Sending Edge Client. 6. Negative Test (Delivery Failure Flow 1): The tester verifies the Health IT module returns an Error Condition to the Sending Edge Client when it cannot encrypt and/or sign the message or does not trust a recipient due to trust validation issues. This can be due to: <ol style="list-style-type: none"> a. Sending Edge Client is not authenticated or authorized; b. Message is invalid; or c. For internal Health IT module communication, a failure may indicate a message delivery failure if the Health IT module implements synchronous delivery. 7. Negative Test (Delivery Failure Flow 2): The tester verifies the Health IT module returns a successful handoff status message to the ETT (as Sending Edge Client) followed by a Failure Notification to the Sending Edge Client when the security and trust process fails. This can be due to: <ol style="list-style-type: none"> a. Trust relationship not established with the ETT (as Receiving HISP); b. Sending Edge Client's certificate and/or private key could not be resolved; c. Sending Edge Client's certificate is expired or revoked; d. The ETT (as Receiving HISP)'s certificate could not be resolved; e. The ETT (as Receiving HISP)'s certificate is expired or revoked; or f. The ETT (as Receiving HISP)'s certificate does not meet Health IT module's certificate policies. 8. Negative Test (Delivery Failure Flow 3): The tester verifies the Health IT module returns a Failure Notification to the Sending Edge Client when the ETT (as Receiving HISP) returns an SMTP error. This can be due to:

Criteria ¶	System Under Test	Test Lab Verification
(ii)		<ul style="list-style-type: none"> a. The Health IT module has been blacklisted by the ETT (as Receiving HISP) SMTP server; b. Message exceeds size limit; c. Invalid SMTP header format (invalid address format); or d. Invalid message format. <p>9. Negative Test (Delivery Failure Flow 4): The tester verifies the Health IT module returns a successful handoff status message followed by a Failure Notification to the Sending Edge Client when the wait time between successfully sending the message to the ETT (as Receiving HISP) and the wait time for the Health IT module to receive a processed MDN from the ETT (as Receiving HISP) has been exceeded.</p> <p>10. Negative Test (Delivery Failure Flow 5): The tester verifies the Health IT module returns a successful handoff status message followed by a Failure Notification to the ETT (as Sending Edge Client) when the Health IT module cannot deliver a message to its destination when no security and trust processing is necessary. This can be due to:</p> <ul style="list-style-type: none"> a. Delivery components are malfunctioning or unavailable; b. The final destination does not exist (invalid address); or c. The final destination is full (mail box over quota). <p>11. Negative Test (Delivery Failure Flow 6): The tester verifies the Health IT module returns a successful handoff message; receives, decrypts, and verifies trust of a processed MDN message received from the ETT (as Receiving HISP); and then generates a Failure Notification to the Sending Edge Client. The Health IT module receives, decrypts, and verifies trust of a MDN failed message from the ETT (as Receiving HISP).</p> <p>12. Negative Test (Notification Failure Flow 1): The tester verifies the Health IT module sends the ETT (as Sending Edge) a successful handoff status message upon message receipt; successfully encrypts and signs the message for sending to the ETT (as Receiving HISP); receives, decrypts, and verifies trust of a processed MDN from the ETT (as Receiving HISP); and generates and sends a Failure Notification to the ETT (as Sending Edge) when the wait time for receiving a dispatched MDN message from the ETT (as Receiving HISP) has been exceeded.</p> <p>13. Negative Test (Notification Failure Flow 2): The tester verifies the Health IT module sends the ETT (as Sending Edge) a successful handoff status message. The tester verifies a Failure Notification is sent by the Health IT module to the ETT (as Sending Edge) when the wait time for receiving a processed MDN from the ETT (as Receiving HISP) has been exceeded. The tester verifies that if a subsequent dispatched MDN message is received by the Health IT module from the ETT (as Receiving HISP) indicating the message has reached its final destination, no success message is sent to the ETT (as Sending Edge).</p>

Criteria ¶	System Under Test	Test Lab Verification
(ii)		<p>14. Negative Test (Notification Failure Flow 3): The tester verifies the Health IT module sends the ETT (as Sending Edge) a successful handoff status message and receives a dispatched MDN message from the ETT (as Receiving HISP) before receiving a processed MDN message from the ETT (as Receiving HISP). The wait time for receipt of a processed MDN has not been exceeded. The tester verifies the Health IT module sends a success notification of delivery of the message to the ETT (as Sending Edge).</p> <p>15. Negative Test (Notification Failure Flow 4): The Tester verifies the Health IT module sends the ETT (as Sending Edge) a successful handoff status message. The tester verifies a Failure Notification is sent by the Health IT module to the ETT (as Sending Edge) when the wait time for receiving a processed MDN from the ETT (as Receiving HISP) has been exceeded. The tester verifies that if a subsequent failed MDN message is received by the Health IT module from the ETT (as Receiving HISP), no further messages are sent to the ETT (as Sending Edge).</p> <p>16. Negative Test (Notification Failure Flow 5): The tester verifies that the Health IT module sends the ETT (as Sending Edge) a successful handoff status message, followed by a Failure Notification if the Health IT module receives a MDN failed message from the ETT (as Receiving HISP) prior to the wait time for receiving a processed MDN from the ETT (as Receiving HISP) message has been exceeded.</p>

(ii) – Receive

Criteria ¶	System Under Test	Test Lab Verification
(ii)	<ol style="list-style-type: none"> 1. Enter the Health IT module's profile information into the ETT with HISP as Receiver. 2. Enter the Health IT module's profile information into the ETT with HISP as Receiver. 	<ol style="list-style-type: none"> 1. (Successful Flow 2): The tester verifies the Health IT module can successfully receive a message from the ETT (as Sending HISP). 2. (Successful Flow 2): The tester verifies the Health IT module generates, encrypts, and signs a processed MDN message to the ETT (as Sending HISP) upon successfully receiving, decrypting, and validating trust. 3. (Successful Flow 2): The tester verifies the Health IT module generates, encrypts, and signs a dispatched MDN message to the ETT (as Sending HISP) upon receiving a success notification of delivery of the message from the ETT (as Receiving Edge Client). 4. Negative Test (Delivery Failure Flow 3): The tester verifies the Health IT module sends an SMTP error code to the ETT (as Sending HISP) when rejecting a message due to: <ul style="list-style-type: none"> • ETT (as Sending HISP) has been blacklisted by the Health IT module's SMTP server; • Message exceeds size limit; • Invalid SMTP header format (invalid address format); or • Invalid message format. 5. Negative Test (Delivery Failure Flow 4): The tester verifies the Health IT module successfully receives the message, but does <u>not</u> send a processed MDN to the ETT (as Sending HISP), because it does not pass security and trust validation due to: <ul style="list-style-type: none"> • Trust relationship not established with ETT (as Sending HISP); • ETT (as Sending HISP)'s certificate could not be resolved; • ETT (as Sending HISP)'s certificate is expired or revoked; • ETT (as Sending HISP)'s certificate does not meet Health IT module's certificate policies; or • Message is not encrypted or signed. 6. Negative Test (Delivery Failure Flow 6): The tester verifies the Health IT module successfully receives the message; generates, encrypts, and signs a processed MDN; but then is unable to deliver the message to its destination. The tester verifies the Health IT module generates, encrypts, and signs a failed MDN message to the ETT (as Sending HISP).

Document History Dependencies

Version Number	Description of Change	Date
1.0	Released for Comment - NPRM	March 31, 2015
1.1	Released for Comment - FR	October 30, 2015
1.2	Updated and Released for Comment	December 4, 2015

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