

# 2015 Edition Certification Companion Guide

## Direct Project, Edge Protocol, and XDR/XDM - 45 CFR 170.315(h)(2)

Links will be updated as available: [Final Rule Preamble](#) – [Test Procedure](#) – [Direct Certificate Discovery Test Tool](#) – [Edge Test Tool](#) – [Test Tool Supplemental Guide](#)

Version 1.0 – Last Updated 10/30/2015

New/Revised/Unchanged Compared to 2014 Edition	Gap Certification Eligible	Base EHR Definition	In Scope for Certified EHR Technology Definition	Associated EHR Incentive Program Objective(s)
Revised	No	Yes <sup>1</sup>	Yes	N/A

### Certification Requirements

**Privacy and Security:** This certification criterion was adopted at § 170.315(h)(2). As a result, an ONC-ACB must ensure that a product presented for certification to a § 170.315(h) “paragraph (h)” criterion includes the privacy and security criteria (adopted in § 170.315(d)) within the overall scope of the certificate issued to the product.

- The privacy and security criteria (adopted in § 170.315(d)) do not need to be explicitly tested with this specific paragraph (h) criterion unless it is the only criterion for which certification is requested.
- As a general rule, a product presented for certification only needs to be tested once to each applicable privacy and security criterion (adopted in § 170.315(d)) so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification. However, exceptions exist for § 170.315(e)(1) “VDT” and (e)(2) “secure messaging,” which are explicitly stated.

**Design and Performance and Other Requirements:** The following design and performance certification criteria (adopted in § 170.315(g)) must also be certified in order for the product to be certified.

- When a single quality management system (QMS) is used, the QMS only needs to be identified once. Otherwise, the QMS’ need to be identified for every capability to which it was applied.
- When a single accessibility-centered design standard is used, the standard only needs to be identified once. Otherwise, the accessibility-centered design standards need to be identified for every capability to which they were applied; or, alternatively the developer must state that no accessibility-centered design was used.

---

<sup>1</sup> In order to meet the Base EHR Definition, a provider would need to possess technology that has been certified to either this criterion at § 170.315(h)(2) or the “Direct Project” criterion at § 170.315(h)(1).

Privacy and Security (§ 170.315(d))	Design and Performance (§ 170.315(g)) and Other Requirements
<ul style="list-style-type: none"> <li>• If choosing Approach 1:               <ul style="list-style-type: none"> <li>○ <a href="#">Authentication, access control, and authorization (§ 170.315(d)(1))</a></li> <li>○ <a href="#">Auditable events and tamper-resistance (§ 170.315(d)(2))</a></li> <li>○ <a href="#">Audit reports (§ 170.315(d)(3))</a></li> </ul> </li> <li>• If choosing Approach 2:               <ul style="list-style-type: none"> <li>○ For each applicable P&amp;S certification criterion not certified for approach 1, the health IT developer may certify for the criterion using system documentation which provides a clear description of how the external services necessary to meet the P&amp;S criteria would be deployed and used.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">Quality management system (§ 170.315(g)(4))</a></li> <li>• <a href="#">Accessibility-centered design (§ 170.315(g)(5))</a></li> </ul>

**Regulation Text**

Direct Project, Edge Protocol, and XDR/XDM.

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

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

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

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

(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).

Criterion Subparagraph	Technical Explanations and Clarifications	Standard(s) Referenced
Applies to entire criterion	<p><b>Clarifications:</b></p> <ul style="list-style-type: none"> <li>• A training/demo video of the <a href="#">ETT Transport Testing Tool</a> used for the testing and certification of health IT is available: <ul style="list-style-type: none"> <li>○ 1. Follow this link to download a zipped file: <a href="http://cda-validation.nist.gov/ETTDemo.zip">http://cda-validation.nist.gov/ETTDemo.zip</a>.</li> <li>○ 2. Unzip the zipped folder.</li> <li>○ 3. Open the Recording 2 Folder and click on the item titled Index.</li> </ul> </li> </ul> <p>Please address any ETT-related questions through the NIST ETT Google Group: <a href="https://groups.google.com/forum/?hl=en#!forum/edge-test-tool">https://groups.google.com/forum/?hl=en#!forum/edge-test-tool</a></p> <ul style="list-style-type: none"> <li>• This certification criterion uses the Applicability Statement for Secure Health Transport, Version 1.2 standard. This new version of the specification includes updates that improve interoperability through the clarification of requirements that have been subject to varying interpretations, particularly requirements around message delivery notifications. This version also clarifies pertinent requirements in the standards underlying the Applicability Statement for Secure Health Transport. Refer to the standard for more details about the improvements it includes. [see also <a href="#">80 FR 62679</a>]</li> <li>• Testing for this criterion will require the processing of invalid test cases that frequently occur in real-world situations so that Security/Trust Agents (STAs) can demonstrate error handling abilities, including handling XDM packages and message disposition.</li> </ul>	N/A

Criterion Subparagraph	Technical Explanations and Clarifications	Standard(s) Referenced
(i)	<ul style="list-style-type: none"> <li>• Technical outcome - The Health IT Module can electronically transmit (send and receive) health information to and from a third party using each of:               <ul style="list-style-type: none"> <li>• Applicability Statement for Secure Health Transport, Version 1.2 (the “Direct Project” specification);</li> <li>• The ONC XDR and XDM for Direct Messaging Specification, Version 1, including support for both limited and full XDS metadata profiles;</li> <li>• And both of the protocols in the ONC Implementation Guide for Direct Edge Protocols, Version 1.1.</li> </ul> </li> </ul> <p><b>Clarifications:</b></p> <ul style="list-style-type: none"> <li>• This criterion requires the three capabilities specified (Direct Project specification, Edge Protocol compliance, and XDR/XDM processing) because it must support interoperability and all potential certified exchange options. A provider could use an “independent” health information service provider (HISP) to meet the Base EHR definition. In such a case, the HISP would need to be certified to this criterion in order for the provider to use it to meet the Base EHR definition, which is part of the CEHRT definition under the EHR Incentive Programs. [see also <a href="#">80 FR 62681</a>]</li> <li>• Testing and certification will <u>not</u> focus on particular deployments or configurations, but rather on what will remain constant across those variances— technology's ability to correctly produce and receive SMTP + S/MIME messages formatted in accordance with the Applicability Statement for Secure Health Transport specification. We further clarify that we do not intend for testing and certification to focus on the particular email protocols that may be implemented to support the routing of these messages, such as Internet Message Access Protocol (IMAP), Post Office Protocol (POP) and other vendor-specific proprietary protocols. These capabilities and others such as mailbox management, storage, and forwarding of received messages that would be implementation or deployment specific would not be assessed as part of testing or as a condition of certification. [see also <a href="#">77 FR 54222</a>]</li> </ul>	<p>§ 170.202(a)(2) <a href="#">Applicability Statement for Secure Health Transport, Version 1.2, August 2015</a></p> <p>§ 170.202(b) <a href="#">ONC XDR and XDM for Direct Messaging Specification</a></p> <p>§ 170.202(d) <a href="#">ONC Implementation Guide for Direct Edge Protocols, Version 1.1, June 25, 2014</a></p>

*Continued on the next page*

Criterion Subparagraph	Technical Explanations and Clarifications	Standard(s) Referenced
(i), continued	<ul style="list-style-type: none"> <li>For developers implementing the ONC XDR/XDM for Direct Messaging Specification, when converting an SMTP message into XDR (with limited metadata), UUID URNs formatted as OIDs should be used for DocumentEntry.uniqueId, SubmissionSet.sourceId, and SubmissionSet.uniqueId We expect testing to this specification to reflect this clarification. <a href="#">[FAQ #31]</a></li> <li>For health IT to be certified to this criterion, it must be able to support both of the Edge Protocols methods referenced in the ONC Implementation Guide (IG) for Edge Protocols Version 1.1 (i.e., the “IHE XDR profile for Limited Metadata Document Sources” edge protocol or an SMTP-focused edge protocol (SMTP alone or SMTP in combination with either IMAP4 or POP3)). [see also <a href="#">80 FR 62680</a>]</li> <li>Even though the IG for Edge Protocols requires support for XDS limited metadata, XDR/XDM supports capability to transform messages using full metadata wherever appropriate. Therefore, we require that a Health IT Module must support both the XDS Metadata profiles (Limited and Full), as specified in the underlying IHE specifications, to ensure that the transformation between messages packaged using XDR/XDM are done with as much appropriate metadata as possible. [see also <a href="#">80 FR 62681</a>]</li> <li>For certification to this criterion, we have made it a requirement to send and receive messages in only “wrapped” format even though the specification (IG) allows use of “unwrapped” messages. This requirement will further improve interoperability among Security/Trust Agents (STAs) while having minor development impact on health IT developers. [see also <a href="#">80 FR 62679</a>]</li> </ul>	<p>§ 170.202(a)(2) <a href="#">Applicability Statement for Secure Health Transport, Version 1.2, August 2015</a></p> <p>§ 170.202(b) <a href="#">ONC XDR and XDM for Direct Messaging Specification</a></p> <p>§ 170.202(d) <a href="#">ONC Implementation Guide for Direct Edge Protocols, Version 1.1, June 25, 2014</a></p>
(ii)	<ul style="list-style-type: none"> <li>Technical outcome – The health IT can electronically transmit (send and receive) health information to a third party using Direct in accordance with the Implementation Guide (IG) for Delivery Notification in Direct, Version 1.0.</li> </ul> <p><b>Clarifications:</b></p> <ul style="list-style-type: none"> <li>The Implementation Guide for Delivery Notification in Direct, Version 1.0, June 29, 2012 functionality supports interoperability and exchange, particularly for both sending and receiving parties, guidance enabling health information service providers (HISPs) to provide a high level of assurance to senders that a message has arrived at its destination, a necessary component to interoperability. The IG also outlines the various exception flows that result in compromised message delivery and the mitigation actions that should be taken by STAs to provide success and failure notifications to the sending system. [see also <a href="#">80 FR 62729</a>]</li> </ul>	<p>§ 170.202(e)(1) <a href="#">Implementation Guide for Delivery Notification in Direct, Version 1.0, June 29, 2012</a></p>

**Note:** This Certification Companion Guide (CCG) is an informative document designed to assist with health IT product development. The CCG is not a substitute for the 2015 Edition final regulation. It extracts key portions of the rule’s preamble and includes subsequent clarifying interpretations. To access the full context of regulatory intent please consult the 2015 Edition final rule or other included regulatory reference. The CCG is for public use and should not be sold or redistributed.

**Version History**

Version #	Change(s) Summary	Date Made
1.0	Initial Publication	Oct 30, 2015