Test Procedure for §170.302 (v) Encryption when exchanging electronic health information

This document describes the test procedure for evaluating conformance of complete EHRs or EHR modules[1] to the certification criteria defined in 45 CFR Part 170 Subpart C of the Final Rule for Health Information Technology: Initial Set of standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology as published in the Federal Register on July 28,2010. The document[2] is organized by test procedure and derived test requirements with traceability to the normative certification criteria as described in the Overview document located at http://healthcare.nist.gov/docs/TestProcedureOverview_v1.pdf. The test procedures may be updated to reflect on-going feedback received during the certification activities.

The HHS/Office of the National Coordinator for Health Information Technology (ONC) has defined the standards, implementation guides and certification criteria used in this test procedure. Applicability and interpretation of the standards, implementation guides and certification criteria to EHR technology is determined by ONC. Test procedures to evaluate conformance of EHR technology to ONC's requirements are defined by NIST. Testing of EHR technology is carried out by ONC-Authorized Testing and Certification Bodies (ATCBs), not NIST, as set forth in the final rule establishing the Temporary Certification Program (*Establishment of the Temporary Certification Program for Health Information Technology, 45 CFR Part 170; June 24, 2010*.)

Questions about the applicability of the standards, implementation guides or criteria should be directed to ONC at ONC.Certification@hhs.gov. Questions about the test procedures should be directed to NIST at hit-tst-fdbk@nist.gov. Note that NIST will automatically forward to ONC any questions regarding the applicability of the standards, implementation guides or criteria. Questions about functions and activities of the ATCBs should be directed to ONC at ONC.Certification@hhs.gov .

CERTIFICATION CRITERIA

§170.302(v) Encryption when exchanging electronic health information. Encrypt and decrypt electronic health information when exchanged in accordance with the standard specified in §170.210(a)(2).

Per Section III.D of the preamble of the Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, Final Rule where the encryption when exchanging electronic health information certification criterion is discussed:

- "Certified EHR Technology must include the capability to encrypt and decrypt information regardless of the transmission method used. This certification criterion and related standard do

[1] Department of Health and Human Services, 45 CFR Part 170 Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, Final Rule, July 28, 2010.

[2] Disclaimer: Certain commercial products are identified in this document. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology.

not specify the circumstances under which encryption and decryption must be performed; they simply require the capability."

- "[…] we want to ensure that Certified HER Technology is capable of assisting eligible professionals and eligible hospitals to implement more secure technical solutions if they determine, based on their risk analysis, that technical safeguards such as encryption are reasonable and appropriate, or required."
- "[…] consistent with the way we have restructured the regulatory text for some standards (to better associate them with the adopted certification criterion that reference them), modified this standard to simply express that the standard is any encrypted and integrity protected link."

INFORMATIVE TEST DESCRIPTION

This section provides an informative description of how the test procedure is organized and conducted. It is not intended to provide normative statements of the certification requirements.

This test evaluates the capability for a Complete EHR or EHR Module to encrypt and decrypt electronic health information when exchanged using an encrypted and integrity protected link.

The Vendor supplies the test data for this test procedure.

This test procedure is organized into three sections:

- Encrypt electronic health information – evaluates the capability to transform electronic health information into an unreadable format using an algorithm
    - Using Vendor-identified functions, the Tester encrypts electronic health information using a symmetric algorithm
    - The Tester validates that the electronic health information is unreadable

- Decrypt electronic health information – evaluates the capability to transform electronic health information into a readable format
    - The tester decrypts the electronic health information using a decryption function
    - The tester validates that the electronic health information is readable

- Transmit electronic health information – evaluates the capability to transmit electronic health information over an encrypted and integrity protected link
    - Using Vendor-identified functions, the Tester transmits the electronic health information to a receiving system (either a Tester's receiving system or a vendor-identified system) using the Vendor-identified encrypted and integrity protected link. This may require configuration on the part of the Tester's receiving system

Referenced Standards

§170.210(a)(2)	Regulatory Referenced Standard
(a) Encryption and decryption of electronic health information (2) Exchange. An encrypted and integrity protected link must be implemented.	

Normative Test Procedures

Derived Test Requirements

DTR170.302.v – 1: Encrypt electronic health information

DTR170.302.v – 2: Decrypt electronic health information

DTR170.302.v – 3: Transmit electronic health information

DTR170.302.v – 1: Encrypt electronic health information

Required Vendor Information

VE170.302.v – 1.01: The vendor shall provide EHR documentation that specifies encryption and decryption capabilities and identifies algorithm and encryption key specifications used

VE170.302.v – 1.02: The vendor shall identify test data available for this test

VE170.302.v – 1:03: The vendor shall identify the technology used to transmit electronic health information over an encrypted and integrity protected link. Note: This test procedure does not require any particular technology or algorithms for use. Nor does this test procedure dictate when an encrypted and integrity protected link must be used and for specific types of data. The FR text referenced above indicates that the conditions under which the link is used is determined by the user

Required Test Procedure:

TE170.302.v – 1.01: Using the vendor-provided test data, the tester shall encrypt the test data using the encryption function

TE170.302.v – 1.02: The tester shall verify that the encrypted test data is unreadable

Inspection Test Guide:

IN170.302.v – 1.01: Tester shall verify that the encrypted electronic health information is unreadable Note: This test procedure does not require any particular technology or algorithms for use. Nor does this test procedure dictate when an encrypted and integrity protected link must be used and for specific types of data. The FR text referenced above indicates that the conditions under which the link is used is determined by the user.

DTR170.302.v – 2: Decrypt electronic health information

Required Vendor Information

- As defined in DTR170.302.v – 1, no additional information is required

Required Test Procedure:

TE170.302.v – 2.01: The tester shall decrypt the encrypted test data using the decryption function

TE170.302.v – 2.02: The tester shall verify that the decrypted data is readable

Inspection Test Guide:

IN170.302.v – 2.01: Tester shall verify that the decrypted electronic health information is readable

DTR170.302.v – 3: Transmit electronic health information

Required Vendor Information

- As defined in DTR170.302.v – 1, no additional information is required

Required Test Procedure:

TE170.302.v – 3.01: Using the EHR function(s) identified by the Vendor, the Tester shall transmit the electronic health information to an external receiving system using the Vendor-identified encrypted and integrity protected link. The receiving system may either be a Tester's receiving system that is configurable to use the transport technology of the EHR system or module, or a vendor-identified system capable of receiving from the EHR system or module

Inspection Test Guide:

IN170.302.v – 3.01: Tester shall verify that the electronic health information was received by the external receiving system, using the encrypted and integrity protected link and based on the transport technology and configuration necessary to communicate with the EHR system

Test Data

This Test Procedure requires the vendor to supply the test data. The Tester shall address the following:

- Vendor-supplied test data shall ensure that the functional and interoperable requirements identified in the criterion can be adequately evaluated for conformance
- Vendor-supplied test data shall strictly focus on meeting the basic capabilities required of an EHR relative to the certification criterion rather than exercising the full breadth/depth of capability that an installed EHR might be expected to support
- Tester shall record as part of the test documentation the specific Vendor-supplied test data that was utilized for testing

Conformance Test Tools

None

Document History

Version Number	Description of Change	Date Published
0.2	Original draft version	April 9, 2010
1.0	Updated to reflect Final Rule	July 21, 2010
1.0	Updated to remove “Pending” from header	August 13, 2010
1.1	Removed “draft” from introductory paragraph	September 24, 2010