

Test Procedure for §170.302 (u) Encryption

This document describes the draft test procedure for evaluating conformance of complete EHRs or EHR modules to the certification criteria defined in 45 CFR Part 170 Subpart C of the Interim Final Rule (IFR) as published in the Federal Register on January 13, 2010. The document 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. These test procedures will be updated to reflect the certification criteria defined in the ONC Final Rule.

Note: This test procedure is scoped only to the criteria defined in 45 CFR Part 170 Subpart C of the Interim Final Rule (IFR) as published in the Federal Register on January 13, 2010. This test procedure will be updated to reflect updates to the criteria and standards as published in the ONC Final Rule. Questions about the criteria and standards should be directed to ONC.

CERTIFICATION CRITERIA

§170.302(u) Encryption:

- (1) General. Encrypt and decrypt electronic health information according to user defined preferences in accordance with the standard specified in 170.210(a)(1).
- (2) Exchange. Encrypt and decrypt electronic health information when exchanged in accordance with the standard specified in 170.210(a)(2).

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 Module¹ to encrypt and decrypt electronic health information to user defined preferences using a symmetric 128 bit fixed-block cipher algorithm capable of using 128, 192, or 256 bit encryption key. This test also evaluates the capability to encrypt and decrypt electronic health information when exchanged through an encrypted and integrity protected link. The Vendor supplies the test data for this test procedure.

This test procedure is organized into two sections:

- Encrypt electronic health information – evaluates the capability to transform electronic health information into an unreadable format using an algorithm
 - The Tester encrypts electronic health information according 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

¹ Department of Health and Human Services, 45 CFR Part 170 Proposed Establishment of Certification Programs for Health Information Technology, Proposed Rule, March 10, 2010.

- The tester validates that the electronic health information is readable

REFERENCED STANDARDS

§170.210(a)(1) and (2)	Regulatory Referenced Standard
(a) Encryption and decryption of electronic health information (1) <u>General</u> . A symmetric 128 bit fixed-block cipher algorithm capable of using 128, 192, or 256 bit encryption key (2) <u>Exchange</u> . An encrypted and integrity protected link must be implemented.	

NORMATIVE TEST PROCEDURES

Derived Test Requirements

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

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

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

Required Vendor Information

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

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

VE170.302.u – 1.03: The vendor shall identify the user-defined preferences available for this test

Required Test Procedure:

TE170.302.u – 1.01: Examine Vendor-provided EHR documentation to determine if the vendor-identified encryption function utilizes a symmetric 128 bit fixed-block cipher algorithm capable of using a 128, 192, or 256 bit encryption key

TE170.302.u – 1.02: Using the vendor-provided user-defined preferences and test data, the tester shall encrypt the test data using the encryption function

TE170.302.u – 1.03: The tester shall verify that the encrypted test data is unreadable

Inspection Test Guide:

IN170.302.u – 1.01: Tester shall verify that Vendor encryption function utilizes a symmetric 128 bit fixed-block cipher algorithm capable of using a 128, 192, or 256 bit encryption key

IN170.302.u – 1.02: Tester shall verify that the encrypted electronic health information is unreadable

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

Required Vendor Information

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

Required Test Procedure:

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

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

Inspection Test Guide:

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

EXAMPLE TEST DATA

Test data for this test procedure is supplied by the Vendor.

CONFORMANCE TEST TOOLS

None