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

The purpose of this document is to record known technical corrections to v1.1 of the Encryption when Exchanging Electronic Health Information test procedure. Errata for other test procedures are located in separate documents. Each erratum entry includes the following information:

- Entry number
- The date the errata was added to the document
- The test procedure version and date published
- The test procedure section
- A description of the correction
- The text prior to the revision and the revised text

1. Technical Correction to Certification Criteria

Date: December 3, 2010
TP Version: Version 1.1, September 24, 2010
TP Section: Certification Criteria Section, page 2
Description: Fixed typo in informative description of certification criteria.

Text Prior to Revision:
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 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."

Revised Text:
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 not specify the circumstances under which encryption and decryption must be performed; they simply require the capability."
- "[…] we want to ensure that Certified **EHR** 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."

2. Technical Correction to Informative Test Description

Date: December 3, 2010
TP Version: Version 1.1, September 24, 2010
TP Section: Informative Test Description, page 2
Description: Updated informative test description to reflect intent of criteria.

Text Prior to Revision:
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

Revised Text:
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 exchange electronic health information using an encrypted and integrity protected link.

The Vendor supplies the test data for this test procedure.

This test procedure is organized into one section:

- Exchange 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

3. Technical Correction to Derived Test Requirements

Date: December 3, 2010
TP Version: Version 1.1, September 24, 2010
TP Section: Normative Test Procedure, Derived Test Requirements, page 3
Description: Removed two of the derived test requirements per the update to the informative test description.

Text Prior to Revision:
DTR170.302.v – 1: Encrypt electronic health information
DTR170.302.v – 2: Decrypt electronic health information
DTR170.302.v – 3: Transmit electronic health information

Revised Text:
DTR170.302.v – 1: Exchange electronic health information

4. Technical Correction to DTR170.302.v – 1: Encrypt electronic health information

Date: December 3, 2010
TP Version: Version 1.1, September 24, 2010
TP Section: Normative Test Procedure, Derived Test Requirements, DTR170.302.v – 1, page 3
Description: Removed encrypt and updated to reflect changes in derived test requirements. Moved the required test procedure and inspection test guide from DTR170.302.v – 3 to DTR170.302.v – 1.

Text Prior to Revision:

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.

Revised Text:

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

Required Vendor Information

VE170.302.v – 1.01: The vendor shall identify test data available for this test

VE170.302.v – 1:02: The vendor shall identify the function(s) used to exchange 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 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 – 1.01: 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

5. Technical Correction to DTR170.302.v – 2: Decrypt electronic health information

Date: December 3, 2010
TP Version: Version 1.1, September 24, 2010
TP Section: Normative Test Procedure, Derived Test Requirements, DTR170.302.v – 1, page 3
Description: Removed DTR170.302.v – 2: Decrypt electronic health information from the test procedure.

Text Prior to Revision:

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

Revised Text:
None; All the text has been removed from the test procedure.

6. Technical Correction to DTR170.302.v – 3: Transmit electronic health information

Date: December 3, 2010
TP Version: Version 1.1, September 24, 2010
TP Section: Normative Test Procedure, Derived Test Requirements, DTR170.302.v – 1, page 3
Description: Removed DTR170.302.v – 3: Transmit electronic health information from the test procedure.

Text Prior to Revision:

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

Revised Text:
None; all of the text has been removed from the test procedure.