Test Procedure for §170.314(d)(7) End-user device encryption

This document describes the 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 Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology, Final Rule. The document[1] is organized by test procedure and derived test requirements with traceability to the normative certification criteria as described in the Overview document located at [available when final]. 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. Testing of EHR technology in the Permanent Certification Program, henceforth referred to as the ONC HIT Certification Program[2], is carried out by National Voluntary Laboratory Accreditation Program-Accredited Testing Laboratories (ATLs) as set forth in the final rule establishing the Permanent Certification Program (*Establishment of the Permanent Certification Program for Health Information Technology, 45 CFR Part 170; February 7, 2011*.)

Questions or concerns regarding the ONC HIT Certification Program should be directed to ONC at ONC.Certification@hhs.gov.

CERTIFICATION CRITERIA

This Certification Criterion is from the Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology, Final Rule issued by the Department of Health and Human Services (HHS) on September 4, 2012.

§170.314(d)(7) End-user device encryption. Paragraph (d)(7)(i) or (ii) of this section must be met to satisfy this certification criterion.

(i) EHR technology that is designed to locally store electronic health information on end-user devices must encrypt the electronic health information stored on such devices after use of EHR technology on those devices stops.

(A) Electronic health information that is stored must be encrypted in accordance with the standard specified in § 170.210(a)(1).

[1] Disclaimer: Certain commercial products may be identified in this document. Such identification does not imply recommendation or endorsement by ONC.

[2] Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology, Final Rule

(B) Default setting. EHR technology must be set by default to perform this capability and, unless this configuration cannot be disabled by any user, the ability to change the configuration must be restricted to a limited set of identified users.

(ii) EHR technology is designed to prevent electronic health information from being locally stored on end-user devices after use of EHR technology on those devices stops.

Per Section III.A of the preamble of the Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology, Final Rule, the 2014 Edition of this Certification Criterion is classified as revised from the 2011 Edition. This Certification Criterion meets at least one of the three factors of revised certification criteria: (1) the certification criterion includes changes to capabilities that were specified in the previously adopted certification criterion, (2) the certification criterion has a new mandatory capability that was not included in the previously adopted certification criterion, or (3) the certification criterion was previously adopted as "optional" for a particular setting and is subsequently adopted as "mandatory" for that setting.

Per Section III.A of the preamble of the Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology, Final Rule where the end-user device encryption certification criterion is discussed:

- "…use of EHR technology is considered to be stopped when a user closes or exits the EHR technology application and would need to re-execute the EHR technology application to again engage in use."
- "…we clarify that testing and certification will focus on normal terminations."
- "…locally stored electronic health information is intended to mean the storage actions that EHR technology is programmed to take (i.e., creation of temp files, cookies, or other types of cache approaches) and not an individual or isolated user action to save or export a file to their personal electronic storage media."
- "We interpret "prevent" to include, for example, situations where EHR technology is designed to and would normally disallow electronic health information to be locally stored on end-user devices after use of EHR technology on those devices stops, but is run in a browser that does not respect "no-cache" headers."
- "We clarified that we intended for the term "stopped" to mean that the session had been terminated, including the termination of the network connection."
- "We…clarify that this certification criterion focuses on, and only applies with respect to, the storage capabilities that are designed for use with EHR technology developer provided or supported technologies for desktop, laptop, or mobile technologies (and similar variations of such technologies) (i.e., it is generally not intended to apply to personally owned end-user devices, unless an EHR technology developer supported technology is loaded/installed on such a device). The certification criterion does not apply with respect to capabilities that may be present in the underlying technology on which EHR technology may run, but is unable to control through the

EHR software, such as operating systems, swap files, and memory management technologies that are embedded and non-configurable by the EHR technology."

- "[We] acknowledge that despite an EHR technology developer's best effort to design EHR technology in such a way…that electronic health information never remains, we understand…that such absolutes cannot always be guaranteed (especially when an EHR technology developer is unable to modify the functionality a particular web browser or operating system employs)."
- "…an EHR technology developer would not have to demonstrate that its EHR technology can encrypt electronic health information locally stored on end-users devices if the EHR technology is designed to prevent electronic health information from being locally stored on end-user devices after use of EHR technology on those devices stops."
- "This certification criterion applies to EHR technology and does not supersede or affect the HIPAA Security Rule's requirements or associated flexibilities."

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 general encryption 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."
- "If an eligible professional or eligible hospital determines that encryption is an appropriate and necessary safeguard, we believe that Certified EHR Technology should provide the capability to implement encryption. Overall, 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."
- "We require that Certified EHR Technology must be capable of encrypting electronic health information. We do not specify the policies surrounding the use of encryption by an eligible professional or eligible hospital nor do we specify that it should only apply to devices. Rather we intend for Certified EHR Technology to be technologically capable of encryption, thereby allowing, if desired or required, an eligible professional or eligible hospital who adopts Certified EHR Technology to use this capability."

CHANGES FROM 2011 TO 2014 EDITION

Per Section III.A of the preamble of the Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology, Final Rule where the end-user device encryption certification criterion is discussed:

- "…we proposed to revise the "general encryption" certification criterion adopted at § 170.302(u) as part of the 2011 Edition EHR certification criteria in favor of a certification criterion focused on the capability of EHR technology to encrypt and decrypt electronic health information managed by EHR technology on end-user devices if such electronic health information would remain stored on the devices after use of EHR technology on that device has stopped. We proposed this revised approach because we thought it would be more practical, effective, and easier to implement than the otherwise general encryption requirement adopted at § 170.302(u). Further, we agreed with the HITSC that we should focus more attention on promoting EHR technology to be designed to secure electronic health information on end-user devices (which are often a contributing factor to a breach of protected health information[3])."
- "We did not include "decrypt" in the proposed certification criterion because we determined it was best to focus certification on the most critical capability, the act of encryption after use of the EHR technology on the end-user device has stopped."

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 procedure evaluates the capability for a Complete EHR or EHR Module to prevent electronic health information from being locally stored on end-user devices, or to encrypt by default electronic health information stored locally on end-user devices after use of the EHR technology on those devices stops.

This test evaluates the capability for a Complete EHR or EHR Module to encrypt electronic health information in accordance with any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2[i].

The Vendor supplies the test data for this test procedure.

This test procedure is organized into two sections:

- Encrypt – evaluates the capability to encrypt by default electronic health information stored locally on end-user devices after normal use of the EHR technology on those devices stops
    - Determine that electronic health information locally stored on an end-user device is encrypted after normal use of the EHR technology on an end-user device stops
    - Determine that the EHR encrypts electronic health information stored on end-user devices in conformance with the encryption algorithm(s) in Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2

[3] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachrept.pdf

- Determine that the encryption of electronic health information on an end-user device is the EHR technology default setting and the setting cannot be disabled by any user
  OR
  If the encryption of electronic health information on an end-user device is a setting that can be disabled, determine that the ability to change the encryption configuration is restricted to a limited set of users

OR

- Prevent – evaluates the capability to prevent electronic health information from being locally stored on end-user devices after normal use of the EHR technology on those devices stops

REFERENCED STANDARDS

§ 170.210 Standards for health information technology to protect electronic health information created, maintained, and exchanged.	Regulatory Referenced Standard
The Secretary adopts the following standards to protect electronic health information created, maintained, and exchanged:	
(a) Encryption and decryption of electronic health information (1) General. Any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2 (incorporated by reference in §170.299).	§170.299 (i) National Institute of Standards and Technology, http://csrc.nist.gov/groups/STM/cmvp/standards.html (1) Annex A: Approved Security Functions for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, Draft, January 27, 2010, IBR approved for §170.210.

NORMATIVE TEST PROCEDURES

The Vendor will identify to the Tester if the EHR technology will satisfy the certification criterion through Derived Test Requirements 1 – 3 to demonstrate encryption of electronic health information locally stored on an end-user device, or if the EHR technology will satisfy the certification criterion through Derived Test Requirement 4 to demonstrate prevention of local storage of electronic health information on an end-user device.

Derived Test Requirements

DTR170.314.d.7—1: Determine Encryption Algorithm Used

DTR170.314.d.7—2: Determine Default Setting and Configuration Capability

DTR170.314.d.7—3: Encrypt Data on End User Device after Use is Stopped

DTR170.314.d.7—4: Prevent Local Storage on End-User Device after Use is Stopped

DTR170.314.d.7–1: Determine Encryption Algorithm Used

Required Vendor Information

VE170.314.d.7 – 1.01: The Vendor shall provide EHR documentation that specifies encryption capabilities for electronic health information stored on an end-user device and identifies encryption algorithm used.

Required Test Procedures

TE170.314.d.7 – 1.01: The Tester shall examine Vendor-provided EHR documentation to determine if the Vendor-identified encryption function utilizes an encryption algorithm specified by Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2 to locally store electronic health information from the EHR technology on end-user devices.

Inspection Test Guide

IN170.314.d.7 – 1.01: The Tester shall verify that the Vendor-identified encryption function utilizes an encryption algorithm specified by Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2 to store electronic health information from the EHR technology on an end-user device.

DTR170.314.d.7–2: Determine Default Setting and Configuration Capability

Required Vendor Information

VE170.314.d.7 – 2.01: The Vendor shall identify the EHR function(s) that are available to enable access to electronic health information from an end-user device.

VE170.314.d.7 – 2.02: The Vendor shall identify the EHR function(s) that specify default configuration settings for encryption of electronic health information stored on an end-user device.

VE170.314.d.7 – 2.03: If electronic health information encryption can be disabled, the Vendor shall identify the EHR function(s) that enable specification of a limited set of identified users with the ability to change configuration settings for encryption of health information stored on an end-user device.

VE170.314.d.7 – 2.04: If electronic health information encryption can be disabled, the Vendor shall identify the EHR function(s) that are available to assign permissions to a user account for managing encryption configuration settings.

Required Test Procedures

TE170.314.d.7 – 2.01: The Tester shall examine the EHR technology setting that specifies default configuration for the encryption of electronic health information on end-user devices.

TE170.314.d.7 – 2.02: The Tester shall determine that the configuration setting is enabled by default and the setting cannot be disabled by any user
OR

The Tester shall determine that the configuration setting can be disabled and change of the encryption configuration is restricted to a limited set of users.

Inspection Test Guide

IN170.314.d.7 – 2.01: The Tester shall verify that the configuration setting is enabled by default and cannot be disabled by any user
OR
The Tester shall verify that the configuration setting can be disabled and change of the encryption configuration is restricted to a limited set of users.

DTR170.314.d.7–3: Encrypt Data on End User Device after Use is Stopped

Required Vendor Information

VE170.314.d.7 – 3.01: The Vendor shall identify the EHR function(s) that are available to store electronic health information from the EHR technology on an end-user device.

VE170.314.d.7 – 3.02: The Vendor shall identify the end-user devices and storage capabilities elected for use and management by the EHR technology developer.

Required Test Procedures

TE170.314.d.7 – 3.01: The Tester shall initiate, from an end-user device, an EHR technology session that is designed to store electronic health information on the end-user device.

TE170.314.d.7 – 3.02: The Tester shall stop the EHR technology session using the end-user device in TE170.314.d.7 – 3.01.

TE170.314.d.7 – 3.03: The Tester shall examine the end-user device in TE170.314.d.7 – 3.02 to verify that the electronic health information from the EHR stored locally on the end-user device after the EHR technology session stops is encrypted in accordance with Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2.

Inspection Test Guide

IN170.314.d.7 – 3.01: The Tester shall verify that the electronic health information stored locally on the end-user device in TE170.314.d.7 – 3.03 after the EHR technology session stops is encrypted in accordance with Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2.

DTR170.314.d.7–4: Prevent Local Storage on End-User Device after Use is Stopped

Required Vendor Information

VE170.314.d.7 – 4.01: The Vendor shall identify the EHR function(s) that are available to enable access to electronic health information from an end-user device.

VE170.314.d.7 – 4.02: The Vendor shall identify the EHR function(s) that are available to demonstrate that it does not enable electronic health information to remain on end-user devices after use of EHR technology on those devices has stopped.

Required Test Procedure

TE170.314.d.7 – 4.01: The Tester shall initiate, from an end-user device, an EHR technology session that is designed to store electronic health information on the end-user device.

TE170.314.d.7 – 4.02: The Tester shall stop the EHR technology session using the end-user device in TE170.314.d.7 – 4.01.

TE170.314.d.7 – 4.03: The Tester shall examine the end-user device in TE170.314.d.7 – 4.02 to verify that no electronic health information is locally stored on the end-user device.

Inspection Test Guide

IN170.314.d.7 – 4.01: The Tester shall verify that no electronic health information from the EHR technology session is locally stored on the end-user device in TE170.314.d.7 – 4.03.

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	Date Published
1.0	Released to for public comment	September 28, 2012

[i] **ANNEX A: APPROVED SECURITY FUNCTIONS**

Annex A provides a list of the Approved security functions applicable to FIPS PUB 140-2. The categories include transitions, symmetric key, asymmetric key, message authentication and hashing. An excerpt is provided below.

Transitions

National Institute of Standards and Technology, *Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, Special Publication 800-131A, January 2011. Sections relevant to this Annex: 1, 2, 3, 9 and 10.

Symmetric Key (AES, TDEA and EES)

1. **Advanced Encryption Standard (AES)**

National Institute of Standards and Technology, *Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication 197, November 26, 2001.

National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation, Methods and Techniques*, Special Publication 800-38A, December 2001.

National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode*, Addendum to Special Publication 800-38A, October 2010.

National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*, Special Publication 800-38C, May 2004.

National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*, Special Publication 800-38D, November 2007.

National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices*, Special Publication 800-38E, January 2010.

2. **Triple-DES Encryption Algorithm (TDEA)**

National Institute of Standards and Technology, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, Special Publication 800-67, May 2004.

National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation, Methods and Techniques*, Special Publication 800-38A, December 2001. Appendix E references Modes of Triple-DES.

American Bankers Association, *Triple Data Encryption Algorithm Modes of Operation,* ANSI X9.52-1998. Copies of X9.52-1998 may be obtained from X9, a standards committee for the financial services industry.

3. **Escrowed Encryption Standard (EES)**

National Institute of Standards and Technology, *Escrowed Encryption Standard (EES)*, Federal Information Processing Standards Publication 185, February 9, 1984.

Asymmetric Key (DSS – DSA, RSA and ECDSA)

1. **Digital Signature Standard (DSS)**
    a. National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-3, June, 2009. (DSA2, RSA2 and ECDSA2)
    b. National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-2, January, 2000 with Change Notice 1. (DSA, RSA and ECDSA)
    c. RSA Laboratories, *PKCS#1 v2.1: RSA Cryptography Standard*, June 14, 2002. Only the versions of the algorithms RSASSA-PKCS1-v1_5 and RSASSA-PSS contained within this document shall be used.

Secure Hash Standard (SHS)

1. **Secure Hash Standard (SHS) (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256)**

    National Institute of Standards and Technology, *Secure Hash Standard*, Federal Information Processing Standards Publication 180-4, March, 2012.

Random Number Generators (RNG and DRBG)

1. **Annex C: *Approved Random Number Generators*** National Institute of Standards and Technology, *Annex C: Approved Random Number Generators for FIPS 140-2, Security Requirements for Cryptographic Modules*.

Message Authentication (Triple-DES, AES and SHS)

1. **Triple-DES**
   National Institute of Standards and Technology, *Computer Data Authentication*, Federal Information Processing Standards Publication 113, 30 May 1985.
2. **AES**
   National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, Special Publication 800-38B, May 2005.
   National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*, Special Publication 800-38C, May 2004.
   National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*, Special Publication 800-38D, November 2007.

3. **SHS**

National Institute of Standards and Technology, *The Keyed-Hash Message Authentication Code (HMAC)*, Federal Information Processing Standards Publication 198-1, July, 2008.