Test Procedure for §170.314(e)(3) Secure messaging – ambulatory setting only

This document describes the test procedure for evaluating conformance of EHR technology 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 http://www.healthit.gov/certification (navigation: 2014 Edition Test Method). The test procedures may be updated to reflect on-going feedback received during the certification activities.

The Department of Health and Human Services (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 Health Information Technology (HIT) Certification Program[2], is carried out by National Voluntary Laboratory Accreditation Program (NVLAP)-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(e)(3) Ambulatory setting only – secure messaging. Enable a user to electronically send messages to, and receive messages from, a patient in a manner that ensures:

(i) Both the patient (or authorized representative) and EHR technology user are authenticated; and

(ii) The message content is encrypted and integrity-protected in accordance with the standard for encryption and hashing algorithms specified at § 170.210(f).

[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 for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology, Final Rule.

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 (September 4, 2012), the 2014 Edition of this certification criterion is classified as new. This certification criterion meets at least one of the two factors of new certification criteria: (1) the certification criterion only specifies capabilities that have never been included in previously adopted certification criteria; or (2) the certification criterion was previously adopted as mandatory" for a particular setting and subsequently adopted as "mandatory" or "optional" for a different setting.

2014 EDITION PREAMBLE LANGUAGE

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 (September 4, 2012) where the secure messaging certification criterion is discussed:

- "We share commenters' sentiment that this certification criterion needs to permit/accommodate a range of possible innovative options. To that end, we intentionally proposed this certification criterion to only specify the particular baseline security and functional capabilities we believed were necessary to require for certification. So long as the method included with EHR technology presented for certification can meet these baseline requirements it would be able to meet this certification criterion. Thus, secure email, a secure portal, even some type of mobile application could all be examples for secure messaging methods that could potentially meet this certification criterion. Along those lines, we decline to specify or restrict certification in this case to a particular transport standard because, again, we intend to permit a wide range of different secure messaging solutions, that will likely use different approaches and transport standards."
- "As noted in the standard proposed just the encryption and hashing algorithms are in scope. Random number generator standards would not necessarily be within scope."
- "One commenter recommended that we investigate evolving secure e-mail and other supporting technologies to protect and verify transactions that include personally identifiable health information. They noted that current Direct Project guidance requires the use of organizational PKI certificates for which the FBCA does not include a profile in its certificate policy. They stated that certificates cited in the Direct project documentation also suggest that the encryption, digital signature and non-repudiation bits all be turned on and that this requirement is an unacceptable practice under the terms of RFC 3647. They concluded by recommending that federally approved NIST LOA 3, 2-factor credentials for patients to authenticate to secure e-mail and or/or portals should be used to fulfill this requirement…At this point, we decline to include such a specific requirement as part of this certification criterion. As the industry gains more experience with different secure messaging approaches, we will consider whether additional specificity such as this is necessary."
- "Certification does not address the relevance of the information that is part of a secure

message. Please see CMS's discussion related to secure messaging in the Stage 2 final rule…"

INFORMATIVE TEST DESCRIPTIONS

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 an EHR technology to enable sending and receiving of messages to and from patients (and their authorized representatives) in an ambulatory setting in a manner that provides for security based on authentication of users/patients/patient representatives and use of encryption in accordance with any encryption and hashing 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 140-2i.

The EHR technology may support separate email inboxes for the patient and authorized patient representative or the same email inbox for both.

The Vendor supplies the test data for this test procedure.

This test procedure is organized into two sections:

- Send – evaluates the capability for using the EHR technology to send messages to a patient and an authorized patient representative based on authentication of users/patients/patient representatives and use of encryption in accordance with any encryption and hashing 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
  - The Vendor tells the Tester which authentication method(s) and which encryption and hashing 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) the Vendor is using for this test
  - Using Vendor-identified EHR function(s), the Tester logs on to the EHR technology as an authenticated Vendor-identified user and sends Vendor-supplied message(s) to Vendor-identified test patient
  - Using Vendor-identified EHR function(s), the Tester logs on to the EHR technology as an authenticated Vendor-identified test patient and views the sent message(s)
  - Tester verifies that the message(s) is/are sent in conformance with the named encryption and hashing algorithm standards, and that the text received in the message(s) is/are complete and accurate
  - Using Vendor-identified EHR function(s), the Tester logs on to the EHR technology as an authenticated Vendor-identified user and sends Vendor-supplied message(s) to Vendor-identified authorized patient representative

- Using Vendor-identified EHR function(s), the Tester logs on to the EHR technology as an authenticated Vendor-identified authorized patient representative and views the sent message(s)
- Tester verifies that the message(s) is/are sent in conformance with the named encryption and hashing algorithm standards, and that the text received in the message(s) is/are complete and accurate

- Receive – evaluates the capability for using the EHR technology to receive messages from a patient and an authorized patient representative based on authentication of users/patients/patient representatives and use of encryption in accordance with any encryption and hashing 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
  - The Vendor tells the Tester which authentication method(s) and which encryption and hashing 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) the Vendor is using for this test
  - Using Vendor-identified EHR function(s), the Tester logs on to the EHR technology as a Vendor-identified authenticated test patient and sends Vendor-supplied message(s) to the Vendor-identified user
  - Using Vendor-identified EHR function(s), the Tester logs on to the EHR technology as the authenticated Vendor-identified user and views the sent message(s)
  - Tester verifies that the message(s) is/are received in conformance with the named encryption and hashing algorithm standards, and that the text received in the message(s) is/are complete and accurate
  - Using Vendor-identified EHR function(s), the Tester logs on to the EHR technology as a Vendor-identified authenticated authorized patient representative and sends Vendor-supplied message(s) to the Vendor-identified user
  - Using Vendor-identified EHR function(s), the Tester logs on to the EHR technology as the authenticated Vendor-identified user and views the sent message(s)
  - Tester verifies that the message(s) is/are received in conformance with the named encryption and hashing algorithm standards, and that the text received in the message(s) is/are complete and accurate

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:	

(f) Encryption and hashing of electronic health information. Any encryption and hashing algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the FIPS Publication 140-2 (incorporated by reference in § 170.299).

NORMATIVE TEST PROCEDURES

Derived Test Requirements

DTR170.314(e)(3) – 1: Send Messages to a Patient and to an Authorized Patient Representative

DTR170.314(e)(3) – 2: Receive Messages from a Patient and from an Authorized Patient Representative

DTR170.314(e)(3) – 1: Send Messages to a Patient and to an Authorized Patient Representative

Required Vendor Information

VE170.314(e)(3) – 1.01: The Vendor shall identify the provider-type user to be used for this test

VE170.314(e)(3) – 1.02: The Vendor shall identify the patient to be used for this test

VE170.314(e)(3) – 1.03: The Vendor shall identify the authorized patient representative to be used for this test

VE170.314(e)(3) – 1.04: The Vendor shall identify the EHR function(s) that are available to send messages to a patient and an authorized patient representative

VE170.314(e)(3) – 1.05: The Vendor shall identify the EHR function(s) that are available to receive and display messages from a patient and an authorized patient representative

VE170.314(e)(3) – 1.06: The Vendor shall identify test data to be used for this test

VE170.314(e)(3) – 1.07: The Vendor shall identify the authentication methods and the encryption and hashing algorithm from Annex A of FIPS 140-2 to be used for this test

Required Test Procedure

TE170.314(e)(3) – 1.01: Using the Vendor-identified EHR technology function(s) and test data, the Vendor-identified patient authentication method, and the Vendor-identified encryption and hashing algorithm, the Tester shall send at least one message to the Vendor-identified test patient from the Vendor-identified provider-type user

TE170.314(e)(3) – 1.02: Using the Inspection Test Guide, the Tester shall verify that the message(s) is/are sent according to the named protocols and standards, and that the text in the message(s) is/are complete and accurate

TE170.314(e)(3) – 1.03: Using the Vendor-identified EHR technology function(s) and test data, the Vendor-identified authorized patient representative authentication method, and the Vendor-identified encryption and hashing algorithm, the Tester shall send at least one message to the Vendor-identified authorized patient representative from the Vendor-identified provider-type user

TE170.314(e)(3) – 1.04: Using the Inspection Test Guide, the Tester shall verify that the message(s) is/are sent according to the named protocols and standards, and that the text in the message(s) is/are complete and accurate

Inspection Test Guide

IN170.314(e)(3) – 1.01: Using the Vendor-identified EHR technology function(s) and test data, the Vendor-identified authentication method, the Vendor-identified encryption and hashing algorithm, and the NIST-identified encryption and hashing algorithms listed as an approved security function in Annex A of the FIPS Publication 140-2, the Tester shall verify that secure messages were sent, and that the text sent in the message(s) is/are complete and accurate

DTR170.314(e)(3) – 2: Receive Messages from a Patient and from an Authorized Patient Representative Required Vendor Information

Required Vendor Information

- As defined in DTR170.314(e)(3) – 1, no additional information is required

Required Test Procedures

TE170.314(e)(3) – 2.01: Using the Vendor-identified EHR technology function(s) and test data, the Vendor- identified patient authentication method, and the Vendor-identified encryption and hashing algorithm, the Tester shall send at least one message from the Vendor- identified patient to the Vendor-identified provider-type user

TE170.314(e)(3) – 2.02: Using the Inspection Test Guide, the Tester shall verify that the message(s) is/are received according to the named protocols and standards, and that the text in the message(s) is/are complete and accurate

TE170.314(e)(3) – 2.03: Using the Vendor-identified EHR technology function(s) and test data, the Vendor- identified authorized patient representative authentication method, and the Vendor-identified encryption and hashing algorithm, the Tester shall send at least one message from the Vendor-identified authorized patient representative to the Vendor-identified provider-type user

TE170.314(e)(3) – 2.04: Using the Inspection Test Guide, the Tester shall verify that the message(s) is/are received according to the named protocols and standards, and that the text in the message(s) is/are complete and accurate

Inspection Test Guide

IN170.314(e)(3) – 2.01: Using the Vendor-identified EHR technology function(s) and test data, the Vendor- identified authentication method, the Vendor-identified encryption and hashing, and the NIST-identified encryption and hashing algorithms listed as an approved security function in Annex A of the FIPS Publication 140-2, the Tester shall verify that secure messages were received, and that the text sent in the message(s) is/are complete and accurate

TEST DATA

The Vendor shall supply the test data for this test procedure.

Vendor supplied test data are provided with the test procedure to ensure that the applicable requirements identified in the criteria can be adequately evaluated for conformance, as well as to provide consistency in the testing process across multiple National Voluntary Laboratory Accreditation Program (NVLAP) - Accredited Testing Labs (ATLs). The provided test data focus on evaluating the basic capabilities of required EHR technology, rather than exercising the full breadth/depth of capability that installed EHR technology might be expected to support. The test data are formatted for readability of use within the testing process. The format is not prescribing a particular end-user view or rendering. No additional requirements should be drawn from the format.

Any test data provided shall focus on meeting the basic capabilities required of EHR technology relative to the certification criterion rather than exercising the full breadth/depth of capability that installed EHR technology might be expected to support.

The test procedures require that the Tester enter the applicable test data into the EHR technology being evaluated for conformance. The intent is that the Tester fully controls the process of entering the test data in order to ensure that the data are correctly entered as specified in the test procedure. If a situation arises where it is impractical for a Tester to directly enter the test data, the Tester, at the Tester's discretion, may instruct the Vendor to enter the test data, so long as the Tester remains in full control of the testing process, directly observes the test data being entered by the Vendor, and validates that the test data are entered correctly as specified in the test procedure.

For Vendor-supplied test data, the Tester shall address the following:

- Vendor-supplied test data shall ensure that the 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
1.0	Released for public comment	November 19, 2012
1.1	Delivered for National Coordinator Approval	December 3, 2012
1.2	Posted Approved Test Procedure	December 14, 2012
1.3	Updated to correct formatting errors: 1) The following Required Test Procedure and Inspection Test Guide steps have been updated to correct a numbering error: DTR170.314(e)(3) – 2 Receive Messages from a Patient and from an Authorized Patient Representative • TE170.314(e)(3) – 1.01 updated to TE170.314(e)(3) – 2.01 • TE170.314(e)(3) – 1.02 updated to TE170.314(e)(3) – 2.02 • TE170.314(e)(3) – 1.03 updated to TE170.314(e)(3) – 2.03 • TE170.314(e)(3) – 1.04 updated to TE170.314(e)(3) – 2.04 • IN170.314(e)(3) – 1.01 updated to IN170.314(e)(3) – 2.01 2) Page numbers added to document	January 16, 2013

[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.