Test Procedure for §170.302 (s) Integrity

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

This Certification Criterion is from the Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology Final Rule issued by the Department of Health and Human Services (HHS) on July 28, 2010.

§170.302(s) Integrity
(1) Create a message digest in accordance with the standard specified in 170.210(c).
(2) Verify in accordance with the standard specified in 170.210(c) upon receipt of electronically exchanged health information that such information has not been altered.
(3) Detection. Detect the alteration of audit logs.

[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.

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 integrity certification criterion is discussed:

- "We clarify that we expect Certified EHR Technology to be capable of creating a message digest and when in receipt of a message digest, to use the message digest to verify that the contents of the message have not been altered."
- "[…] we clarify that Certified EHR Technology must include the capability to check the integrity of health information that has been received through electronic exchange. However, similar to our approach to many adopted certification criteria, we do not specify the instance in which the capability needs to be executed."

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 generate a message digest using the standard specified and to verify, upon receipt of electronic health information that the information has not been altered using a secure hashing algorithm (SHA-1 or higher). For the purposes of this test procedure, audit logs (170.302.s-3) are considered a type of information for which a message digest can be generated. The Vendor supplies test data for this test.

This test procedure consists of three sections:

- Generate hash values – evaluates the capability to generate a hash value
  - The Tester generates two hash values for comparison using Vendor-supplied test data
  - The Tester modifies the Vendor-supplied test data set and generates a hash value for the modified data set

- Compare hash values – evaluates the capability to compare hash values to ensure the electronic health information has not been altered in transit
  - The Tester compares the generated hash values
  - The Tester determines if the hash values are the same or different depending on the data sets

- Generate, Exchange, and Verify– evaluates the capability to generate a hash of health information in accordance with the standard specified in 170.210(c), electronically exchange the health information and the generated message digest to a receiving system, and verify that the electronically exchanged health information has not been altered.
  - Using Vendor-identified functions, the Tester generates a message digest of the health information.

- Using Vendor-identified functions, the Tester electronically exchanges the health information and the generated message digest to a receiving system (either a Tester's receiving system or a vendor-identified system) using the Vendor-identified transport technology of the EHR. This may require configuration on the part of the Tester's receiving system.
- The Tester verifies that the electronically exchanged health information and generated message digest is the same.

REFERENCED STANDARDS

§170.210(c)	Regulatory Referenced Standard
Verification that electronic health information has not been altered in transit. Standard. A hashing algorithm with a security strength equal to or greater than SHA-1 (Secure Hash Algorithm (SHA-1) as specified by the National Institute of Standards and Technology (NIST) in FIPS PUB 180-3 (October, 2008) must be used to verify that electronic health information has not been altered	

NORMATIVE TEST PROCEDURES

Derived Test Requirements

DTR170.302.s – 1: Generate hash values
DTR170.302.s – 2: Compare hash values
DTR170.302.s – 3: Generate, exchange, and verify hash values

DTR170.302.s – 1: Generate hash values

Required Vendor Information

VE170.302.s – 1.01: The Vendor shall provide EHR documentation identifying the secure hash algorithm (e.g., security strength equal to or greater than SHA-1) used to provide the hash value

VE170.302.s – 1.02: The Vendor shall identify the EHR function(s) that are available to generate and read hash values

VE170.302.s – 1.03: The Vendor shall identify test data available for this test

Required Test Procedure:

TE170.302.s – 1.01: The Tester shall examine Vendor-provided EHR documentation to determine if the vendor-identified secure hashing algorithm used to provide the hash value is equal to or greater in strength than SHA-1

TE170.302.s – 1.02: Using the Vendor-identified EHR function(s), the Tester shall generate two hash values for the Vendor-supplied test data
Using the Vendor-supplied test data set, the Tester shall modify the test data

TE170.302.s – 1.03: Using the Vendor identified EHR function (s), the Tester shall generate a hash value for the modified test data set

TE170.302.s – 1.04: The Tester shall output and store the hash value for comparison

Inspection Test Guide

IN170.302.s – 1.01: Tester shall verify that the Vendor-identified secure hashing algorithm used to provide the hash value is SHA-1 or higher

IN170.302.s – 1.02: Tester shall verify that two hash values have been generated from the Vendor-supplied test data and that one hash value has been generated from the modified Vendor-supplied test data

DTR170.302.s – 2: Compare hash values

Required Vendor Information

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

Required Test Procedure:

TE170.302.s – 2.01: The Tester shall compare the hash values generated in the Generate hash values test using the Vendor-supplied test data

TE170.302.s – 2.02: The Tester shall compare one hash value generated in the Generate hash value test using the Vendor-supplied test data and the hash value generated using the modified Vendor-supplied test data

Inspection Test Guide

IN170.302.s – 2.01: Tester shall verify that the hash values are the same for the Vendor-supplied test data

IN170.302.s – 2.02: Tester shall verify that the hash values are different for the modified Vendor-supplied test data

DTR170.302.s – 3: Generate, exchange, and verify hash values

Required Vendor Information

- Information as defined in DTR170.302.s.1 – 1 and the following additional information is required

VE170.302.s – 3.01: The Vendor shall identify the transport technology available to electronically exchange test data.

VE170.302.s – 3.02: The Vendor shall identify a receiving system to receive electronically exchanges test data.

Required Test Procedure:

TE170.302.s – 3.01: The Tester shall generate a message digest of Vendor-provided test data.

TE170.302.s – 3.02: The Tester shall electronically exchange the Vendor-provided test data and the generated message digest from TE 170.302.s-3.01 to a receiving system (either

a Tester's receiving system or a vendor-identified system) using the Vendor-identified transport technology of the EHR. This may require configuration on the part of the Tester's receiving system.

TE170.302.s – 3.03: The Tester shall generate a message digest on the receiving system of the electronically exchanged Vendor-provided test data.

TE170.302.s – 3.04: The Tester shall compare the electronically exchanged message digest and the message digest generated on the receiving system.

Inspection Test Guide

IN170.302.s – 3.01: Tester shall verify that the electronically exchanged message digest and the message digest generated on the receiving system are the same for the Vendor-provided test data

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
0.3	Original draft version	April 9, 2010
1.0	Updated to reflect Final Rule	July 21, 2010
1.0	Updates include: • removed “Pending” from header • updated typographical error	August 13, 2010
1.1	Updates include: • removed “draft” from introductory paragraph • Added new DTR – Generate, exchange, and verify hash values	September 24, 2010