Test Procedure for §170.314(d)(8) Integrity

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 CRITERION

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. This Certification Criterion is included in the definition of a Base EHR.

§170.314(d)(8) Integrity.

(i) Create a message digest in accordance with the standard specified in § 170.210(c).

(ii) 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.

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

[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

this Certification Criterion is classified as unchanged with refinements from the 2011 Edition. This Certification Criterion meets the three factors of unchanged certification criteria: (1) the certification criterion includes only the same capabilities that were specified in previously adopted certification criteria, (2) the certification criterion's capabilities apply to the same setting as they did in previously adopted certification criteria, and (3) the certification criterion remains designated as "mandatory," or it is re-designated as "optional," for the same setting for which it was previously adopted certification criterion. Accordingly, Section III.D of the Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, Final Rule published in the Federal Register on July 28, 2010 also applies to the 2014 Edition of this Certification Criterion.

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 integrity certification criterion is discussed:

- "We agree with commenters that EHR technology developers should migrate towards the use of SHA-2 because of its increased security strength, but only where possible and voluntarily. The SHA-1 standard included in this certification criterion serves as a floor and permits EHR technology to be certified if it includes hashing algorithms with security strengths equal to or greater than SHA-1."
- "…we seek to call readers' attention that NIST has superseded FIPS 180-3 with FIPS 180-4. The changed in FIPS 180-4 are limited in scope and do not affect the approach we expressed in the standard we adopted for this certification [sic]. Therefore, in order to keep the regulation current with this recent publication we have modified the regulation test to refer to FIPS 180-4 instead of FIPS 180-3."

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."

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 integrity certification criterion is discussed:

- "We also proposed to remove the capability to detect changes to an audit log because we proposed to add that capability to the proposed certification criterion for "auditable events and tamper resistance" at § 170.314(d)(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 Module to create 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).

The Vendor supplies test data for this test procedure.

This test procedure consists of three sections:

- Create hash values – evaluates the capability to create a hash value
  - The Tester creates two hash values for comparison using Vendor-supplied test data
  - The Tester changes the Vendor-supplied test data set and creates a hash value for the changed 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 created hash values
  - The Tester determines if the hash values are the same or different depending on the data sets

- Create, Exchange, and Verify– evaluates the capability to create a hash of health information in accordance with the standard specified in 170.210(c), electronically exchange the health information and the created message digest to a receiving system, and verify that the electronically exchanged health information has not been altered.
  - Using Vendor-identified functions, the Tester creates a message digest of the health information.
  - Using Vendor-identified functions, the Tester electronically exchanges the health information and the created 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 created 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 180-4 (March, 2012) must be used to verify that electronic health information has not been altered	

NORMATIVE TEST PROCEDURES

Derived Test Requirements

DTR170.314.d.8 – 1: Create hash values
DTR170.314.d.8 – 2: Compare hash values
DTR170.314.d.8 – 3: Create, exchange, and verify hash values

DTR170.314.d.8 – 1: Create hash values

Required Vendor Information

VE170.314.d.8 – 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
VE170.314.d.8 – 1.02: The Vendor shall identify the EHR function(s) that are available to create and read hash values
VE170.314.d.8 – 1.03: The Vendor shall identify test data available for this test

Required Test Procedure:

TE170.314.d.8 – 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
TE170.314.d.8 – 1.02: Using the Vendor-identified EHR function(s), the Tester shall create two hash values for the Vendor-supplied test data
Using the Vendor-supplied test data set, the Tester shall change the test data
TE170.314.d.8 – 1.03: Using the Vendor identified EHR function(s), the Tester shall create a hash value for the changed test data set
TE170.314.d.8 – 1.04: The Tester shall output and store the hash value for comparison

Inspection Test Guide

IN170.314.d.8 – 1.01: Tester shall verify that the Vendor-identified secure hashing algorithm used to provide the hash value is SHA-1 or higher

IN170.314.d.8 – 1.02: Tester shall verify that two hash values have been created from the Vendor-supplied test data and that one hash value has been created from the changed Vendor-supplied test data

DTR170.314.d.8 – 2: Compare hash values

Required Vendor Information

- As defined in DTR170.314.d.8 – 1, no additional information is required

Required Test Procedure:

TE170.314.d.8 – 2.01: The Tester shall compare the hash values created in the Create hash values test using the Vendor-supplied test data

TE170.314.d.8 – 2.02: The Tester shall compare one hash value created in the Create hash value test using the Vendor-supplied test data and the hash value created using the changed Vendor-supplied test data

Inspection Test Guide

IN170.314.d.8 – 2.01: Tester shall verify that the hash values are the same for the Vendor-supplied test data

IN170.314.d.8 – 2.02: Tester shall verify that the hash values are different for the changed Vendor-supplied test data

DTR170.314.d.8 – 3: Create, exchange, and verify hash values

Required Vendor Information

- Information as defined in DTR170.314.d.8 – 1 and the following additional information is required

VE170.314.d.8 – 3.01: The Vendor shall identify the transport technology available to electronically exchange test data.

VE170.314.d.8 – 3.02: The Vendor shall identify a receiving system to receive electronically exchanges test data.

Required Test Procedure:

TE170.314.d.8 – 3.01: The Tester shall create a message digest of Vendor-provided test data.

TE170.314.d.8 – 3.02: The Tester shall electronically exchange the Vendor-provided test data and the created message digest from TE 170.314.d.8 – 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.

TE170.314.d.8 – 3.03: The Tester shall create a message digest on the receiving system of the electronically exchanged Vendor-provided test data.

TE170.314.d.8 – 3.04: The Tester shall compare the electronically exchanged message digest and the message digest created on the receiving system.

Inspection Test Guide

IN170.314.d.8 – 3.01: Tester shall verify that the electronically exchanged message digest and the message digest created on the receiving system are the same for the Vendor-provided test data

CONFORMANCE TEST TOOLS

None

Document History

Version Number	Description	Date
1.0	Released for public comment	September 7, 2012