Test Procedure for §170.302 (t) Authentication

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(t) Authentication: Verify that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information.

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 authentication certification criterion is discussed:

[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.

- "We have considered the concerns issued by commenters and agree that the burden associated with cross enterprise authentication is unnecessarily high and cross-network authentication should not be a condition of certification at the present time."
- "We do not believe that it is appropriate to specify, as a condition of certification, the types of factors that users could utilize to authenticate themselves."

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 verify that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information. This test procedure excludes identity proofing and verification across networks.

The Vendor supplies test data for this test.

This test procedure consists of one section:

- <u>Verify authorization</u>– evaluates the capability to verify that a person or entity seeking access to electronic health information is the one claimed and is authorized
  - The Tester creates a new user account and assigns permissions
  - The Tester performs an action authorized by the assigned permissions and verifies that the authorized activity was performed
  - The Tester performs an action that is not authorized by the assigned permissions and verifies that the action was not performed
  - The Tester deletes (e.g., deactivates or disables) the user account
  - The Tester attempts to login to the account and verifies that the login attempt failed

Referenced Standards

None

Normative Test Procedures

Derived Test Requirements

DTR170.302.t – 1: Verify authorization

DTR170.302.t – 1: Verify authorization

<u>Required Vendor Information</u>

VE170.302.t – 1.01: The Vendor shall identify the EHR function(s) that are available to login and logout of the EHR, create a new account, establish the identification and

authentication information associated with the new account, assign permissions to the new user account, and delete the account

Required Test Procedure:

TE170.302.t – 1.01: Using the Vendor-identified EHR function(s), the Tester shall create a new user account and assign permissions to this new account

TE170.302.t – 1.02: Using the new user account, the Tester shall login to the EHR using the new account

TE170.302.t – 1.03: The Tester shall perform an action authorized by the assigned permissions.

TE170.302.t – 1.04: The Tester shall verify that the authorized action was performed

TE170.302.t – 1.05: The Tester shall perform an action not authorized by the assigned permissions

TE170.302.t – 1.06: The Tester shall verify that the unauthorized action was not performed

TE170.302.t – 1.07: The Tester shall log out of the EHR

TE170.302.t – 1.08: The Tester shall delete (e.g., deactivate or disable) the new account

TE170.302.t – 1.09: The Tester shall attempt to login to the EHR using the deleted account

TE170.302.t – 1.10: The Tester shall verify that the login attempt failed

TE170.302.t – 1.11: Using the NIST-supplied Inspection Test Guide, the Tester shall verify that:

- an account has been created
- can sign-in to the account
- can authorize the assigned permissions
- can delete (e.g., deactivate or disable) the account
- the log-in attempt has failed

Inspection Test Guide

IN170.302.t – 1.01: Tester shall verify that an account has been created, can sign-in to the account, and authorize the assigned permissions

IN170.302.t – 1.02: Tester shall verify that an account has been deleted (e.g., deactivated or disabled) and that the log-in attempt failed

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
0.2	Original draft version	April 9, 2010
0.3	Updated typographical error in derived test requirement on page 3	May 11, 2010
1.0	Updated to reflect Final Rule	July 21, 2010
1.0	Updates include: • removed “Pending” from header • updated to correct typographical errors • clarified the concept of user account deletion	August 13, 2010
1.1	Removed “draft” from introductory paragraph	September 24, 2010