Test Procedure for §170.302 (o) Access Control

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(o) Access Control: Assign a unique name and/or number for identifying and tracking user identity and establish controls that permit only authorized users to access electronic health information.

[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.

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 assign a unique name and/or number for identifying and tracking user identity and establish controls that permit only authorized users to access electronic health information.

The Vendor supplies the test data for this test procedure.

This test procedure consists of one section:

- Assign unique name/number – evaluates the capability to assign a unique name and/or number to track user identity and establish controls for authorized users to access electronic health information in the EHR.
    - Tester shall create a unique name/number
    - Tester shall perform authorized actions based on user permissions and verify that authorized actions were performed
    - Tester shall perform unauthorized actions and verify that the unauthorized actions were not performed

REFERENCED STANDARDS

None

NORMATIVE TEST PROCEDURES

Derived Test Requirements
DTR170.302.o – 1: Assign unique name/number

DTR170.302.o – 1: Assign unique name/number
Required Vendor Information
VE170.302.o – 1.01: The Vendor shall identify the EHR function(s) that are available to assign a new user name/number, ensure that the name/number is unique, and assign permissions to the name/number for accessing electronic health information.
VE170.302.o – 1.02: The Vendor shall identify test data necessary for this test, including a listing of existing user names/numbers.

Required Test Procedure:
TE170.302.o – 1.01: The Tester shall identify an existing user name/number

TE170.302.o – 1.02:	Using the Vendor-identified EHR function(s), the Tester shall select an existing user name/number and shall attempt to create a duplicate user name/number
TE170.302.o – 1.03:	The Tester shall verify that the duplicate user name/number is not created
TE170.302.o – 1.04:	Using the Vendor-identified EHR function(s), the Tester shall create a unique user name/number and assign permissions to this new account to access electronic health information
TE170.302.o – 1.05:	The Tester shall verify that the unique user name/number is created
TE170.302.o – 1.06:	The Tester shall perform an action authorized by the assigned permissions
TE170.302.o – 1.07:	The Tester shall verify that the authorized action was performed
TE170.302.o – 1.08:	The Tester shall perform an action not authorized by the assigned permissions
TE170.302.o – 1.09:	The Tester shall verify that the unauthorized action was not performed

Inspection Test Guide

IN170.302.o – 1.01:	Tester shall verify that a unique user name/number has been created
IN170.302.o – 1.02:	Tester shall verify that authorized actions were performed
IN170.302.o – 1.03:	Test shall verify that unauthorized actions were no performed

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
1.0	Updated to reflect Final Rule	July 21, 2010
1.0	Updated to remove “Pending” from header	August 13, 2010
1.1	Removed “draft” from introductory paragraph	September 24, 2010