

Document Change History

| Version Number | Description of Change | Date Published |
|----------------|---|----------------|
| 0.3 | Updated typographical error in derived test requirement on page 3 | May 11, 2010 |

Test Procedure for §170.302 (t) Authentication

This document describes the draft 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 Interim Final Rule (IFR) as published in the Federal Register on January 13, 2010. The document 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. These test procedures will be updated to reflect the certification criteria defined in the ONC Final Rule.

Note: This test procedure is scoped only to the criteria defined in 45 CFR Part 170 Subpart C of the Interim Final Rule (IFR) as published in the Federal Register on January 13, 2010. This test procedure will be updated to reflect updates to the criteria and standards as published in the ONC Final Rule. Questions about the criteria and standards should be directed to ONC.

CERTIFICATION CRITERIA

§170.302(t) Authentication:

- (1) Local. Verify that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information.
- (2) Cross network. Verify that a person or entity seeking access to electronic health information across a network is the one claimed and is authorized to access such information in accordance with the standard specified in 170.210(d).

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 Module¹ 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:

- Verify authorization– 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

¹ Department of Health and Human Services, 45 CFR Part 170 Proposed Establishment of Certification Programs for Health Information Technology, Proposed Rule, March 10, 2010.

- The Tester deletes the user account
- The Tester attempts to login to the account and verifies that the login attempt failed

REFERENCED STANDARDS

| §170.210(d) | Regulatory Referenced Standard |
|--|--------------------------------|
| <u>Cross-enterprise authentication.</u> A cross-enterprise secure transaction that contains sufficient identity information such that the receiver can make access control decisions and produce detailed and accurate security audit trails must be used. | |

NORMATIVE TEST PROCEDURES

Derived Test Requirements

DTR170.302.t – 1: Verify authorization

DTR170.302.t – 1: Verify authorization

Required Vendor Information

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:

- VE170.302.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.
- VE170.302.t – 1.02: Using the new user account, the Tester shall login to the EHR using the new account.
- VE170.302.t – 1.03: The Tester shall perform an action authorized by the assigned permissions.
- VE170.302.t – 1.04: The Tester shall verify that the authorized action was performed.
- VE170.302.t – 1.05: The Tester shall perform an action not authorized by the assigned permissions.
- VE170.302.t – 1.06: The Tester shall verify that the unauthorized action was not performed.
- VE170.302.t – 1.07: The Tester shall log out of the EHR.
- VE170.302.t – 1.08: The Tester shall delete the new account.
- VE170.302.t – 1.09: The Tester shall attempt to login to the EHR using the deleted account
- VE170.302.t – 1.010: The Tester shall verify that the login attempt 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 and that the log-in attempt failed

TEST DATA

Test data for this test procedure is supplied by the Vendor.

CONFORMANCE TEST TOOLS

None