Test Procedure for §170.314(d)(1) Authentication, access control, and authorization

This document describes the test procedure for evaluating conformance of EHR technology 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 http://www.healthit.gov/certification (navigation: 2014 Edition Test Method). The test procedures may be updated to reflect on-going feedback received during the certification activities.

The Department of Health and Human Services (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 Health Information Technology (HIT) Certification Program[2], is carried out by National Voluntary Laboratory Accreditation Program (NVLAP)-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 CRITERIA

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)(1) Authentication, access control, and authorization.

(i) Verify against a unique identifier(s) (that is, username or number) that a person seeking access to electronic health information is the one claimed; and

[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.

(ii) Establish the type of access to electronic health information a user is permitted based on the unique identifier(s) provided in paragraph (d)(1)(i) of this section, and the actions the user is permitted to perform with the EHR technology.

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 (September 4, 2012), the 2014 Edition of 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.

2014 Edition Preamble Language

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 (September 4, 2012) where the authentication, access control, and authorization certification criterion is discussed:

- "We also expressed the HITSC's authentication recommendation as additional guidance for this certification criterion in that the capability to authenticate human users would consist of the assertion of an identity and presentation of at least one proof of that identity."
- "We stated that it is most appropriate for this certification criterion to focus on users that would be able to access electronic health information in EHR technology within an EP, EH, or CAH's organization and not to focus on external users that may make requests for access to health information contained in the EHR technology for the purpose of electronic health information exchange."
- "…we have purposefully left this certification criterion flexible to accommodate for different implementations, deployments, and organizational policy decisions."

2011 Edition Preamble Language

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 (July 29, 2010) where the authentication certification criterion is discussed:

- "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."

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 (September 4, 2012) where the authentication, access control, and authorization certification criterion is discussed:

- "…merg[ing] the "access control" certification criterion at § 170.302(o) and the "authentication" certification criterion at § 170.302(t) into one certification criterion for the 2014 Edition EHR certification criteria…would allow for more efficient testing and was consistent with EHR technology development."

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 procedure evaluates the capability for an EHR technology to assign a unique identifier (that is, username or number) for identifying user identity and to establish permitted access to electronic health information.

The Vendor supplies the test data for this test procedure.

This test procedure is organized into two sections:

- Authenticate Unique User—evaluates the capability of the EHR technology to establish the identification and authentication information associated with a unique user identifier
    - The Vendor identifies the EHR function(s) that allow a user to log in to and out of the EHR, create a unique user identifier (that is, username or number), and establish the identification and authentication information associated with a unique user identifier
    - The Tester uses the Vendor-identified EHR function(s) to create a new, unique user identifier (that is, username or number), establish authentication information, and verify that a unique user identifier was created

- The Tester logs in to the EHR using the newly created user identifier and associated authentication information and verifies that the access attempt was successful
- The Tester logs out of the EHR, and then attempts to create a new user account using the same unique user identifier established in previous steps
- The Tester verifies that the EHR technology prevents an existing user identifier from being used again to demonstrate that user identifiers are unique
- The Tester disables (that is, removes, deactivates) the new unique user identifier and verifies that the unique user identifier was disabled (that is, removed, deactivated)
- The Tester attempts to log in to the EHR using the deleted unique user identifier and verifies that the log in attempt failed

- Establish Permitted User Access—evaluates the capability of the EHR technology to establish permitted access to electronic health information and to permit authorized actions within the EHR technology
  - The Vendor identifies the EHR function(s) that allow a user to
    - Log in to and out of the EHR
    - Create a unique user identifier (that is username or number) and establish the associated authentication information
    - Assign permissions for users to access electronic health information
  - The Tester first attempts to log in to the EHR using incorrect credentials to verify that the EHR technology requires valid credentials in order for a user to access the system
  - The Tester uses the Vendor-identified EHR function(s) to create a new user account and assign a unique user identifier (that is username or number), establish identification and authentication information (that is password), and verify that a unique user identifier was created
  - The Tester grants access to perform authorized actions in the EHR to the newly created user account, then demonstrates that the new user account is able to perform authorized actions but does not have permission to perform unauthorized actions, thereby validating the access control mechanism of the EHR
  - The Tester logs out of the EHR and uses the Vendor-identified EHR function(s) to change the permissions assigned to the new user account in previous steps
  - The Tester verifies that the new user now has access to perform actions that were prohibited under previous permissions
  - The Tester logs in to the EHR using the same unique user identifier and performs a previously unauthorized action that is now authorized under the newly set permissions
  - The Tester verifies that the EHR technology allows the newly authorized action(s) to be performed

REFERENCED STANDARDS

None

NORMATIVE TEST PROCEDURES

Derived Test Requirements

DTR170.314(d)(1) – 1: Authenticate Unique User
DTR170.314(d)(1) – 2: Establish Permitted User Access

DTR170.314(d)(1) – 1: Authenticate Unique User

Required Vendor Information

VE170.314(d)(1) – 1.01: The Vendor shall identify the EHR function(s) that are available to log in to the EHR, create a unique user identifier (that is, username or number), and establish identification and authentication information (that is, password)

Required Test Procedures

TE170.314(d)(1) – 1.01: Using the Vendor-identified EHR function(s), the Tester shall create a new user account, with a unique user identifier (that is, username or number) and establish identification and authentication information

TE170.314(d)(1) – 1.02: The Tester shall log in to the EHR using the new unique user identifier and authentication information

TE170.314(d)(1) – 1.03: The Tester shall log out of the EHR

TE170.314(d)(1) – 1.04: The Tester shall attempt to create a new user account with the user identifier that was created in TE170.314(d)(1) – 1.01 and establish that the user identifier is unique

TE170.314(d)(1) – 1.05: The Tester shall disable (that is, remove or deactivate) the new user account and unique identifier established in TE170.314(d)(1) – 1.01

TE170.314(d)(1) – 1.06: The Tester shall attempt to access the EHR using the disabled unique user identifier

Inspection Test Guide

IN170.314(d)(1) – 1.01: The Tester shall verify that a unique user identifier was created

IN170.314(d)(1) – 1.02: The Tester shall verify that the attempts to log in to and out of the EHR were successful

IN170.314(d)(1) – 1.03: The Tester shall verify that the EHR technology prevents an existing user identifier from being re-used when creating a new user account

IN170.314(d)(1) – 1.04: The Tester shall verify that the unique user identifier was disabled successfully

IN170.314(d)(1) – 1.05: The Tester shall verify that the attempt to log in to the EHR after disabling the user account failed

DTR170.314(d)(1) – 2: Establish Permitted User Access

Required Vendor Information

VE170.314(d)(1) – 2.01: The Vendor shall identify the EHR function(s) that are available to log in to and log out of the EHR

VE170.314(d)(1) – 2.02: The Vendor shall identify the EHR function(s) to set up and disable a user account, including creating a unique user identifier (that is, username or number) and establishing the identification and authentication information associated with the unique user identifier

VE170.314(d)(1) – 2.03: The Vendor shall identify the EHR function(s) to assign permissions to a user account

Required Test Procedures

TE170.314(d)(1) – 2.01: Using the Vendor-identified EHR function(s), the Tester shall log in to the EHR using incorrect user credentials

TE170.314(d)(1) – 2.02: Using the Vendor-identified EHR function(s), the Tester shall create a new, unique user identifier (that is, username or number) and establish authentication information

TE170.314(d)(1) – 2.03: The Tester shall establish the type of access to EHR function(s) that the new user account is permitted to perform with the EHR technology, allowing access to some functions and preventing access to other functions

TE170.314(d)(1) – 2.04: The Tester shall log in to the EHR using the unique user identifier and authentication information

TE170.314(d)(1) – 2.05: The Tester shall perform an action authorized by the assigned permissions

TE170.314(d)(1) – 2.06: The Tester shall perform an action not authorized by the assigned permissions

TE170.314(d)(1) – 2.07: The Tester shall log out of the EHR

TE170.314(d)(1) – 2.08: Using the Vendor-identified EHR function(s), the Tester shall change the permissions assigned to the user account in TE170.314(d)(1) – 2.03 so that the user has access to all functions, including those that were previously prohibited

TE170.314(d)(1) – 2.09: The Tester shall log in to the EHR again using the user account modified in TE170.314(d)(1) – 2.08

TE170.314(d)(1) – 2.10: The Tester shall perform the action that was previously not authorized in TE170.314(d)(1) – 2.06 under the newly assigned permissions

Inspection Test Guide

IN170.314(d)(1) – 2.01: The Tester shall verify that the incorrect credentials did not grant user access to the EHR technology

IN170.314(d)(1) – 2.02: The Tester shall verify that a unique identifier was created

IN170.314(d)(1) – 2.03: The Tester shall verify that the authorized action in TE170.314(d)(1) – 2.05 was performed

IN170.314(d)(1) – 2.04: The Tester shall verify that the unauthorized action in TE170.314(d)(1) – 2.06 was not performed

IN170.314(d)(1) – 2.05: The Tester shall verify that the assigned permissions were changed to allow access to all previously prohibited functions

IN170.314(d)(1) – 2.06: The Tester shall verify that the previously unauthorized action in TE170.314(d)(1) – 2.06 is now authorized and was performed successfully

TEST DATA

Vendor supplied test data are provided with the test procedure to ensure that the applicable requirements identified in the criteria can be adequately evaluated for conformance, as well as to provide consistency in the testing process across multiple National Voluntary Laboratory Accreditation Program (NVLAP) - Accredited Testing Labs (ATLs). The provided test data focus on evaluating the basic capabilities of required EHR technology, rather than exercising the full breadth/depth of capability that installed EHR technology might be expected to support. The test data are formatted for readability of use within the testing process. The format is not prescribing a particular end-user view or rendering. No additional requirements should be drawn from the format.

Any test data provided shall focus on meeting the basic capabilities required of EHR technology relative to the certification criterion rather than exercising the full breadth/depth of capability that installed EHR technology might be expected to support.

The test procedures require that the Tester enter the applicable test data into the EHR technology being evaluated for conformance. The intent is that the Tester fully controls the process of entering the test data in order to ensure that the data are correctly entered as specified in the test procedure. If a situation arises where it is impractical for a Tester to directly enter the test data, the Tester, at the Tester's discretion, may instruct the Vendor to enter the test data, so long as the Tester remains in full control of the testing process, directly observes the test data being entered by the Vendor, and validates that the test data are entered correctly as specified in the test procedure.

For Vendor-supplied test data, the Tester shall address the following:

- Vendor-supplied test data shall ensure that the 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
1.0	Released for public comment	November 19, 2012
1.1	Delivered for National Coordinator Approval	December 3, 2012
1.2	Posted Approved Test Procedure	December 14, 2012