

## Test Procedure for §170.314(d)(5) Automatic log-off

This document describes the test procedure for evaluating conformance of electronic health record (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<sup>1</sup> 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<sup>2</sup>, 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](mailto: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)(5) Automatic log-off. Prevent a user from gaining further access to an electronic session after a predetermined time of inactivity.

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

---

<sup>1</sup> Disclaimer: Certain commercial products may be identified in this document. Such identification does not imply recommendation or endorsement by ONC.

<sup>2</sup> 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.

to the Permanent Certification Program for Health Information Technology, Final Rule, 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 automatic log-off certification criterion is discussed:

- "...EHR technology developers should interpret this certification criterion to require... that after a period of inactivity the EHR technology must make a user's session inaccessible and subsequently require the user to re-authenticate using the same credentials used to begin the session."
- "Additionally, we clarify that this certification criterion is not meant to result in the termination of network connections, especially network connections that are not in use by the EHR technology, but by other applications."

## 2011 EDITION PREAMBLE LANGUAGE

None referenced

## 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 automatic log-off certification criterion is discussed:

- "To make the capability expressed by this certification criterion clearer to EHR technology developers, we have replaced "Terminate" with "Prevent a user from gaining further access to..." Although this may be longer phrasing toward the same meaning, we believe it less ambiguous than "terminate," is more plain language, and that it is also consistent with the language used for the "session lock" security control specified in NIST 800-53 rev3."

## 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 EHR technology to prevent a user from gaining further access to an electronic session after a predetermined time of inactivity.

The Vendor supplies the test data for this test procedure.

This test procedure consists of one section:

- Prevent a user from gaining further access to an electronic session – evaluates the capability to prevent a user from gaining further access to an electronic session after a predetermined time of inactivity
  - The Tester establishes an electronic session
  - The Tester verifies that a user is prevented from gaining further access to an electronic session after a predetermined time of inactivity

## REFERENCED STANDARDS

None

## NORMATIVE TEST PROCEDURES

### Derived Test Requirements

DTR170.314(d)(5) – 1: Prevent a User from Gaining Further Access to an Electronic Session

### **DTR170.314(d)(5) – 1: Prevent a User from Gaining Further Access to an Electronic Session**

#### Required Vendor Information

VE170.314(d)(5) – 1.01: The Vendor shall identify the EHR function(s) that are available to prevent a user from gaining further access to an electronic session after a predetermined time of inactivity

VE170.314(d)(5) – 1.02: The Vendor shall provide all test data necessary to perform the test procedure, including a valid log-in account that can be used to establish an electronic session

#### Required Test Procedure

TE170.314(d)(5) – 1.01: Using the Vendor-identified EHR function(s) and test data, the Tester shall establish an electronic session

TE170.314(d)(5) – 1.02: Using the Inspection Test Guide (below), the Tester shall verify that a user is prevented from gaining further access to an electronic session after the predetermined time of inactivity

#### Inspection Test Guide

IN170.314(d)(5) – 1.01: Tester shall verify that a user is prevented from gaining further access to an electronic session after a predetermined time of inactivity

## TEST DATA

The Vendor shall supply the test data for this test procedure.

Vendor-supplied test data 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
1.0	Released for public comment	September 7, 2012
1.1	Delivered for National Coordinator Approval	December 4, 2012
1.2	Posted Approved Test Procedure	December 14, 2012