

Test Procedure for §170.314(d)(2) Auditable events and tamper-resistance

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 (September 4, 2012). The document¹ 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 Program², 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 (September 4, 2012). This certification criterion is included in the definition of a Base EHR.

§170.314(d)(2) Auditable events and tamper-resistance.

- (i) Record actions. EHR technology must be able to:
 - (A) Record actions related to electronic health information in accordance with the standard specified in §170.210(e)(1);

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.

(B) Record the audit log status (enabled or disabled) in accordance with the standard specified in §170.210(e)(2) unless it cannot be disabled by any user; and

(C) Record the encryption status (enabled or disabled) of electronic health information locally stored on end-user devices by EHR technology in accordance with the standard specified in §170.210(e)(3) unless the EHR technology prevents electronic health information from being locally stored on end-user devices (see §170.314(d)(7) of this section).

(ii) Default setting. EHR technology must be set by default to perform the capabilities specified in paragraph (d)(2)(i)(A) of this section and, where applicable, paragraphs (d)(2)(i)(B) or (d)(2)(i)(C), or both paragraphs (d)(2)(i)(B) and (C).

(iii) When disabling the audit log is permitted. For each capability specified in paragraphs (d)(2)(i)(A), (B), and (C) of this section that EHR technology permits to be disabled, the ability to do so must be restricted to a limited set of identified users.

(iv) Audit log protection. Actions and statuses recorded in accordance with paragraph (d)(2)(i) must not be capable of being changed, overwritten, or deleted by the EHR technology.

(v) Detection. EHR technology must be able to detect whether the audit log has been altered.

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 revised from the 2011 Edition. This certification criterion meets at least one of the three factors of revised certification criteria: (1) the certification criterion includes changes to capabilities that were specified in the previously adopted certification criterion, (2) the certification criterion has a new mandatory capability that was not included in the previously adopted certification criterion, or (3) the certification criterion was previously adopted as “optional” for a particular setting and is subsequently adopted as “mandatory” for that setting.

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 auditable events and tamper-resistance certification criterion is discussed:

- “...expansion included the specific capabilities that the audit log must be enabled by default (i.e., turned on), immutable (i.e., unable to be changed, overwritten, or deleted), and able to record not only which action(s) occurred, but more specifically the electronic health information to which the action applies.”
- “...the ability to enable and disable the recording of actions [should] be limited to an identified set of users (for example, system administrator).”
- “...a revised standard at § 170.210(e)...require[s] that: 1) when the audit log is enabled or disabled, the date and time (in accordance with the standard specified at § 170.210(g)

(synchronized clocks)), user identification, and the action(s) that occurred must be recorded; and 2) as applicable, when encryption for end-user devices managed by EHR technology is enabled or disabled, the date and time (in accordance with the standard specified at § 170.210(g) (synchronized clocks)), user identification, and the actions that occurred must be recorded.”

- “We acknowledge that 2014 Edition EHR technology will need to be setup and configured at each practice or hospital in which EHR technology with this capability is installed. This certification criterion is not meant to prohibit such configuration...what this certification criterion expresses...is that in order to for the EHR technology to be certified it must be set by default to record the actions and information specified in the standards referenced by the certification criterion. Thus...at the point of installation or upgrade EHR technology certified to this 2014 Edition EHR certification criterion...will be set by default for an EP, EH, or CAH...”
- “... [We] believe that it is appropriate for actions made to electronic health information and recorded in the audit log to be identified at a categorical (or type) level – this is also consistent with the guidance included in ASTM E2147-01(2009).”
- “...we acknowledge that there is only so much that is within the control of EHR technology and that nothing is ever 100% impenetrable. Thus, we have revised this specific capability within the certification criterion to state that the audit log must not be capable of being changed, overwritten, or deleted by the EHR technology.”

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 28, 2010) where audit log certification criterion is discussed:

- “While we believe that in most cases a user will be a health care professional performing an action using Certified EHR Technology, it is also possible that a device or another software process or program could perform any one of these actions. We do not intend to preclude EHR technology developers from including these and other types of specific features.”

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, 2010) where the auditable events certification criterion is discussed:

- “We proposed two revised certification criteria at § 170.314(d)(2) and (3) – one focused on the capability to record auditable events and another focused on the capability to create audit reports

- in place of the single 2011 Edition EHR certification criterion for audit logs adopted at § 170.302(r).”
- “We also proposed to move the specific capability “detection” from the integrity certification criterion (§ 170.302(s)(3)) to the proposed auditable events and tamper-resistance certification criterion.”
- “We made these proposals based on HITSC recommendations as well as stakeholder feedback that indicated splitting the 2011 Edition certification criterion into two separate certification criteria would permit a wider variety of EHR technologies to be certified as EHR Modules.”
- “Thus, the standards we express now refer to the appropriate sections of ASTM E2147-01(2009), rather than an enumerated list.”

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 the EHR technology to:

- Be set by default to record actions related to electronic health information in an audit log, and record audit log status or encryption status
- Permit disabling of audit logs, audit log status, and encryption status to be restricted to a limited set of identified users (for example, system administrators)
- Record actions related to electronic health information in an audit log. Information to be recorded for each action includes the date and time of the event, patient identification, user identification, type of action, and identification of the patient data that was accessed
- Protect actions and statuses related to recording of electronic health information, audit log status, and encryption status from being changed, overwritten, or deleted by the EHR technology
- Detect when the audit log has been altered

The test also verifies that when the audit log function records the date and time of an action related to electronic health information, that the EHR utilizes a system clock that has been synchronized following (RFC₃ 1305) Network Time Protocol, or (RFC 5905) Network Time Protocol Version 4.

The Tester is encouraged to reuse the results of other related test procedures to gain efficiencies in the EHR technology test process.

The Vendor supplies the test data for this test procedure.

This test procedure uses the term “audit log” to refer to the “record [of] actions related to electronic health information”. For example, “disabling audit logs” is meant to convey the action of disabling recording of actions related to electronic health information.

The test procedure also uses the terms “audit log status” which indicates whether an audit log has been enabled or disabled.

This test procedure is organized into five sections:

- Record Default Setting—evaluates that the EHR technology has the capability to be set by default to record actions related to electronic health information and, where applicable, to record either audit log status or encryption status, or to record both audit log status and encryption status
 - The Vendor identifies the default configuration settings for recording actions related to electronic health information in an audit log
 - Where applicable, the Vendor identifies the default configuration settings of the audit log status (i.e. whether the audit log is enabled or disabled)
 - Where applicable, the Vendor identifies the default configuration settings of the encryption status (i.e. whether encryption is enabled or disabled) of electronic health information stored locally on end-user devices by EHR technology
 - The Tester examines the default configuration settings for recording actions related to electronic health information and verifies that the function can be performed by default
 - Where applicable, the Tester examines the configuration settings for recording the audit log status and verifies that the function can be performed by default
 - Where applicable, the Tester examines the configuration settings for recording the encryption status of electronic health information stored locally on end-user devices and verifies that the function can be performed by default
- Permit Audit Log, Audit Log Status, Encryption Status Disabling—evaluates the capability of the EHR technology, as applicable, to restrict disabling of audit logs, disabling of audit log status, and disabling of encryption status to a limited set of identified users (for example, system administrator)

Disabling of audit logs may include functions that activate or deactivate the audit service that generates and logs the audit events.

The test steps in the following sections of “Permit Audit Log Disabling” are separated into two sections to accommodate 1) EHR technology that directly allows users to perform the disabling functions described and 2) EHR technology that does not allow users to perform the disabling functions.

- Permit Disabling of Audit Logs:
As the EHR technology permits,
 - The Vendor identifies the EHR function(s) that
 - allow a user to disable audit logs
 - enable specification of a limited set of identified users (for example, system administrator) to disable audit logs
 - The Vendor sets up and identifies test user accounts which have and do not have permission to disable audit logs

- The Tester reviews the Vendor-identified EHR function(s) that allow audit logs to be disabled and establishes that the user has permission to change the audit logs
- Using the Vendor-provided identifier and authentication information, the Tester accesses the EHR as a user without permission to disable audit logs and verifies that the user is not permitted to disable audit logs
- Using the Vendor-provided identifier and authentication information, the Tester accesses the EHR as a user with permission to disable audit logs and verifies that the audit logs can be disabled
- The Tester verifies that the date, time, and user identification related to disabling the are recorded in the audit log entry
- The Tester re-enables the audit log
- If the EHR technology does not allow any users to perform the disabling functions described, the Vendor shall submit documentation indicating the inability to allow users to disable audit logs
- Permit Disabling of Audit Log Status
 - As the EHR technology permits,
 - The Vendor identifies the EHR function(s) that allow a user to disable the audit log status (enabled or disabled)
 - The Vendor identifies the EHR function(s) that enable specification of a limited set of identified users (for example, system administrator) to disable the audit log status
 - The Vendor identifies unique identifiers and authentication information that allow a user to access the EHR technology both with and without permissions to disable the audit log status
 - The Tester reviews the Vendor-identified EHR function(s) that allow the audit log status to be disabled and establishes that the identifier has permission to change the audit log status
 - Using the Vendor-provided identifier and authentication information, the Tester accesses the EHR as a user without permission to disable the audit log status and verifies that the ability to disable the function is not allowed
 - Using the Vendor-provided identifier and authentication information, the Tester accesses the EHR as a user with permission to disable the audit log status and verifies that the audit log status can be disabled
 - The Tester verifies that the date, time, and user identification related to disabling the audit log status are recorded in the audit log entry
 - The Tester re-enables the audit log status
 - If the EHR technology does not allow any users to perform the disabling functions described, the Vendor shall submit documentation indicating the inability to allow users to disable the audit log status
 - Permit Disabling of Encryption Status
 - As the EHR technology permits,
 - The Vendor identifies the EHR function(s) that allow a user to disable the encryption status

- The Vendor identifies the EHR function(s) that enable specification of a limited set of identified users (for example, system administrators) to disable the encryption status
 - The Vendor identifies the EHR function(s) that are available to assign permission to disable the encryption status
 - The Vendor identifies unique identifiers and authentication information that allow a user to access the EHR technology both with and without permissions to disable the encryption status
 - The Tester reviews the Vendor-identified EHR function(s) that allow the encryption status to be disabled and establishes that the identifier has permission to change the encryption status
 - Using the Vendor-provided identifier and authentication information, the Tester accesses the EHR as a user without permission to disable the encryption status and verifies that the ability to disable the function is not allowed
 - Using the Vendor-provided identifier and authentication information, the Tester accesses the EHR as a user with permission to disable the encryption status and verifies that the encryption status can be disabled
 - The Tester verifies that the date, time, and user identification related to disabling the encryption status are recorded in the audit log entry
 - The Tester re-enables the encryption status
 - If the EHR technology does not allow any users to perform the disabling functions described, the Vendor shall submit documentation indicating the inability to allow users to disable the encryption status
- Record Actions—evaluates the capability of the EHR technology audit log function to record information related to an action that is made in respect to electronic health information while the EHR technology is in use
 - The Vendor identifies the EHR function(s) that are available for a user to perform actions (additions, deletions, changes, queries, print, and copy) related to electronic health information
 - For further clarification on actions, please see ASTM E2147-01 in the audit log content standard
 - If the EHR technology does not allow any users to perform one or more of the actions listed above, the Vendor submits documentation to demonstrate this
 - The Vendor identifies EHR function(s) that are available to record actions (these will be automatic functions used to create audit log entries) related to electronic health information
 - The Vendor provides an identifier and authentication information that allow a user to access the EHR technology
 - The Vendor identifies a patient with an existing record in the EHR to be used for this test and a set of electronic health test data for the patient
 - The Tester uses Vendor-identified EHR function(s) to perform the following actions, if permitted, and verifies that the actions were performed successfully:
 - Addition

- Deletion
- Change
- Query
- Print
- Copy
- For all permissible actions, the Tester verifies that an audit log entry related to each action taken has been generated correctly
- For all permissible actions, the Tester verifies that the EHR technology audit log function records data elements related to each action listed above, including:
 - Date and time of event
 - Patient identification
 - User identification
 - Type of action (additions, deletions, changes, queries, print, copy), specifying inquiry, any changes made (with pointer to original data state), and a delete specification (with a pointer to deleted information)
 - Identification of the patient data that is accessed
- If the EHR technology does not allow any users to perform one or more of the actions listed above, the Tester verifies this for each applicable action through examination of documentation submitted by the Vendor

While section 7.7 of the audit log content standard, “Identification of the Patient Data that is Accessed (optional)” is specified as optional in the context of the standard, it is a data element that is required to be recorded by the audit log function as part of certification criterion §170.314(d)(2).i.A, in accordance with §170.210(e)(1).

- Protect Audit Log—evaluates the capability of the EHR technology to protect audit logs from being changed, overwritten or deleted by the EHR technology; this includes recording of actions related to electronic health information, recording of audit log status, and recording of encryption status
 - The Vendor submits documentation to identify how the EHR technology protects the following from being changed, overwritten, or deleted by the EHR technology: 1) recording of actions related to electronic health information, 2) recording of audit log status, and 3) recording of encryption status
 - The Tester verifies that the method(s) presented by the Vendor demonstrate that the EHR technology protects actions related to electronic health information and audit log and encryption statuses from being changed, overwritten or deleted by the EHR technology
- Detect Audit Log Alteration—evaluates the capability of the EHR technology to detect whether the audit log has been altered
 - The Vendor submits documentation to identify how the EHR technology detects alterations to the audit log
 - The Tester verifies that the method(s) identified by the Vendor sufficiently demonstrate that the EHR technology is capable of detecting audit log alteration

REFERENCED STANDARDS

§170.210 Standards for health information technology to protect electronic health information created, maintained, and exchanged.

Regulatory Referenced Standard

The Secretary adopts the following standards to protect electronic health information created, maintained, and exchanged:

(e)(1) Record actions related to electronic health information, audit log status, and encryption of end-user devices. (i) The audit log must record the information specified in sections 7.2 through 7.4, 7.6, and 7.7 of the standard specified at §170.210(h) when EHR technology is in use. (ii) The date and time must be recorded in accordance with the standard specified at §170.210(g).

(e)(2) (i) The audit log must record the information specified in sections 7.2 and 7.4 of the standard specified at §170.210(h) when the audit log status is changed. (ii) The date and time each action occurs in accordance with the standard specified at §170.210(g).

(e)(3) The audit log must record the information specified in sections 7.2 and 7.4 of the standard specified at §170.210(h) when the encryption status of electronic health information locally stored by EHR technology on end-user devices is changed. The date and time each action occurs in accordance with the standard specified at §170.210(g).

170.210(g) Synchronized clocks. The date and time recorded utilize a system clock that has been synchronized following (RFC 1305) Network Time Protocol, (incorporated by reference in §170.299) or (RFC 5905) Network Time Protocol Version 4, (incorporated by reference in §170.299).

170.210(h) Audit log content. ASTM E2147-01 (Reapproved 2009), (incorporated by reference in §170.299)

NORMATIVE TEST PROCEDURES

Network Time Protocol (NTP) Test

The test steps below must be performed by the Vendor and the results validated by the Tester prior to beginning the test steps in the Derived Test Requirements. These tests evaluate an EHR technology's ability to meet the standard adopted at 45 CFR 170.210(g), which requires that the date and time

recorded by the EHR technology “utilize a system clock that has been synchronized following (RFC 1305) Network Time Protocol Version 3 or (RFC 5905) Network Time Protocol Version 4”.

NTP170.314(d)(2) – 1.01: The Vendor shall identify the protocol used to synchronize the system clock on which the EHR technology will base its time

NTP170.314(d)(2) – 1.02: The Vendor shall choose a time server from the list below, used by the NIST Internet Time Service (ITS), and shall add it to their NTP software configuration, and synchronize the system clock that will be used by the EHR technology as the basis for its time

Note: All users should ensure that their software NEVER queries a server more frequently than once every 4 seconds. Systems that exceed this rate will be refused service. In extreme cases, systems that exceed this limit may be considered as attempting a denial-of-service attack.

Name	IP Address	Location
nist1-ny.ustiming.org	64.90.182.55	New York City, NY
nist1-nj.ustiming.org	96.47.67.105	Bridgewater, NJ
nist1-pa.ustiming.org	206.246.122.250	Hatfield, PA
time-a.nist.gov	129.6.15.28	NIST, Gaithersburg, Maryland
time-b.nist.gov	129.6.15.29	NIST, Gaithersburg, Maryland
nist1.aol-va.symmetricom.com	64.236.96.53	Reston, Virginia
nist1.columbiacountyga.gov	216.119.63.113	Columbia County, Georgia
nist1-atl.ustiming.org	64.250.177.145	Atlanta, Georgia
nist1-chi.ustiming.org	216.171.120.36	Chicago, Illinois
nist-chicago (No DNS)	38.106.177.10	Chicago, Illinois
nist.time.nosc.us	96.226.123.117	Carrollton, Texas
nist.expertsmi.com	50.77.217.185	Monroe, Michigan
nist.netservicesgroup.com	64.113.32.5	Southfield, Michigan
nisttime.carsoncity.k12.mi.us	66.219.116.140	Carson City, Michigan
nist1-lnk.binary.net	216.229.0.179	Lincoln, Nebraska
www.nist.gov	24.56.178.140	WWV, Fort Collins, Colorado
time-a.timefreq.bldrdoc.gov	132.163.4.101	NIST, Boulder, Colorado

time-b.timefreq.blrdoc.gov	132.163.4.102	NIST, Boulder, Colorado
time-c.timefreq.blrdoc.gov	132.163.4.103	NIST, Boulder, Colorado
time.nist.gov	global address for all servers	Multiple locations
utcnist.colorado.edu	128.138.140.44	University of Colorado, Boulder
utcnist2.colorado.edu	128.138.141.172	University of Colorado, Boulder
ntp-nist.lidsbc.edu	198.60.73.8	LDSBC, Salt Lake City, Utah
nist1-lv.ustiming.org	64.250.229.100	Las Vegas, Nevada
time-nw.nist.gov	131.107.13.100	Microsoft, Redmond, Washington
nist-time-server.eoni.com	216.228.192.69	La Grande, Oregon
nist1.aol-ca.symmetricom.com	207.200.81.113	Mountain View, California
nist1.symmetricom.com	69.25.96.13	San Jose, California
nist1-sj.ustiming.org	216.171.124.36	San Jose, California
nist1-la.ustiming.org	64.147.116.229	Los Angeles, California

NTP170.314(d)(2) – 1.03: After configuring NTP, the Vendor shall wait the amount of time necessary to ensure synchronization occurs

NTP170.314(d)(2) – 1.04: Using the NTP logs, the Vendor and Tester shall verify that the system time is accurate within five seconds of the NIST time sever chosen in NTP170.314(d)(2) – 1.01. The NIST time servers follow NTPv3 (RFC 1305), thus, the Tester shall consider an accurate synchronization to a NIST time server as evidence of compliance to RFC 1305 or RFC 5905 and does not need to evaluate the polling value/interval.

NTP170.314(d)(2) – 1.05: The Vendor shall construct or use an existing display in the EHR system that shows the time from the system clock and the EHR time for comparison (these times should be synchronized to within five seconds). Five seconds was chosen to allow testers to visually verify that there is limited to no time discrepancy between the EHR technology and the synchronized system clock used (in cases where the EHR technology does not implement its own NTP client).

NTP170.314(d)(2) – 1.06: The Tester shall verify, via the NTP logs, that the system time is synchronized to the NIST time server to within five seconds; and then the Tester shall verify, via the EHR display, that the EHR time is synchronized to the system time to within five seconds

The test procedure assumes the operating system synchronizes to the NTP server and the EHR then synchronizes to the operating system; however, the EHR could synchronize directly to the NTP server. The EHR technology may use either method to demonstrate that the synchronization has occurred. Use of internal NTP servers are allowed, but the EHR technology must demonstrate that the internal servers are synced to a NIST timeserver for accuracy.

Derived Test Requirements

- DTR170.314(d)(2) – 1: Default Setting
- DTR170.314(d)(2) – 2: Permit Audit Log, Audit Log Status, Encryption Status Disabling
- DTR170.314(d)(2) – 3: Record Actions
- DTR170.314(d)(2) – 4: Audit Log Protection
- DTR170.314(d)(2) – 5: Detection of Audit Log Alteration

DTR170.314(d)(2) – 1: Default Setting

Required Vendor Information

- VE170.314(d)(2) – 1.01: The Vendor shall identify the default configuration settings for recording actions related to electronic health information
- VE170.314(d)(2) – 1.02: Where applicable, the Vendor shall identify the default configuration settings for recording the audit log status (enabled or disabled)
- VE170.314(d)(2) – 1.03: Where applicable, the Vendor shall identify the default configuration settings for recording the encryption status (enabled or disabled) of electronic health information stored locally on end-user devices by EHR technology
- VE170.314(d)(2) – 1.04: The Vendor shall identify a patient with an existing record in the EHR to be used for this test and a set of electronic health test data for the patient

Required Test Procedures

- TE170.314(d)(2) – 1.01: The Tester shall determine that the EHR technology has a default audit log setting to record actions related to electronic health information
- TE170.314(d)(2) – 1.02: Where applicable, the Tester shall determine that the EHR technology has a default audit log setting to record the audit log status (enabled or disabled)
- TE170.314(d)(2) – 1.03: Where applicable, the Tester shall determine that the EHR technology has a default audit log setting to record the encryption status (enabled or disabled) of electronic health information locally stored on end-user devices by EHR technology

Inspection Test Guide

- IN170.314(d)(2) – 1.01: Where applicable, the Tester shall verify that the default setting for audit logs is enabled
- IN170.314(d)(2) – 1.02: Where applicable, the Tester shall verify that the default setting for recording audit log status is enabled

IN170.314(d)(2) – 1.03: Where applicable, the Tester shall verify that the default audit log setting for recording the encryption status (enabled or disabled) of electronic health information locally stored on end-user devices by EHR technology is enabled

DTR170.314(d)(2) – 2: Permit Audit Log, Audit Log Status and Encryption Status Disabling

Required Vendor Information

- VE170.314(d)(2) – 2.01: The Vendor shall identify the EHR function(s) that are available for a user to disable 1) audit logs, 2) the audit log status, or 3) the encryption status. If the EHR technology does not allow users to perform disabling functions, refer to VE170.314(d)(2) – 2.05
- VE170.314(d)(2) – 2.02: The Vendor shall identify the EHR function(s) that enable specification of a limited set of identified users to disable: 1) the audit log, 2) the audit log status, or 3) the encryption status
- VE170.314(d)(2) – 2.03: The Vendor shall provide a user account and associated authentication information for a user authorized to disable: 1) audit logs, 2) the audit log status, or 3) the encryption status
- VE170.314(d)(2) – 2.04: The Vendor shall provide a user account and associated authentication information for users who are not authorized to disable 1) audit logs, 2) the audit log status, or 3) the encryption status
- VE170.314(d)(2) – 2.05: If the EHR technology does not allow any users to perform the disabling functions described, the Vendor shall submit documentation indicating the inability to allow users to disable 1) audit logs, 2) the audit log status, or 3) the encryption status

Required Test Procedures

Disable Audit Logs

- If the EHR technology allows a user to disable audit logs, the Tester shall perform the test steps below:
 - TE170.314(d)(2) – 2.01: The Tester shall access the EHR using a Vendor-provided account that does not authorize disabling audit logs
 - TE170.314(d)(2) – 2.02: The Tester shall attempt to disable audit logs and verify inability to disable audit logs
 - TE170.314(d)(2) – 2.03: The Tester shall access the EHR using a Vendor-provided account that authorizes disabling audit logs (for example, system administrator)
 - TE170.314(d)(2) – 2.04: The Tester shall attempt to disable audit logs and verify ability to successfully disable audit logs
 - TE170.314(d)(2) – 2.05: The Tester shall re-enable the audit log

- If the EHR technology does not allow any users to disable audit logs, the Tester shall perform the test steps below:

TE170.314(d)(2) – 2.06: The Tester shall examine the Vendor-provided documentation to determine that the EHR technology does not allow users to disable audit logs

Disable Audit Log Status

- If the EHR technology allows a user to disable the audit log status, the Tester shall perform the test steps below:

TE170.314(d)(2) – 2.07: The Tester shall access the EHR using a Vendor-provided account that does not authorize disabling of the audit log status

TE170.314(d)(2) – 2.08: The Tester shall attempt to disable recording of the audit log status and verify the inability to disable audit log status

TE170.314(d)(2) – 2.09: The Tester shall access the EHR using a Vendor-provided account that authorizes disabling of the audit log status (for example, system administrator)

TE170.314(d)(2) – 2.10: The Tester shall attempt to disable the audit log status and verify ability to successfully disable audit log status

TE170.314(d)(2) – 2.11: The Tester shall re-enable the audit log status

- If the EHR technology does not allow any users to disable audit log status, the Tester shall perform the test step below:

TE170.314(d)(2) – 2.12: The Tester shall examine the Vendor-provided documentation to determine that the EHR technology does not allow users to disable audit log status

Disable Encryption Status

- If the EHR technology allows a user to disable the encryption status, the Tester shall perform the test steps below:

TE170.314(d)(2) – 2.13: The Tester shall access the EHR using a Vendor-provided account that does not authorize disabling of the encryption status

TE170.314(d)(2) – 2.14: The Tester shall attempt to disable recording of the encryption status and verify the inability to disable encryption status

TE170.314(d)(2) – 2.15: The Tester shall access the EHR using a Vendor-provided account that authorizes disabling of the encryption status (for example, system administrator)

TE170.314(d)(2) – 2.16: The Tester shall attempt to disable the encryption status and verify ability to successfully disable encryption status

TE170.314(d)(2) – 2.17: The Tester shall re-enable the encryption status

- If the EHR technology does not allow any users to disable encryption status, the Tester shall perform the test step below:

TE170.314(d)(2) – 2.18: The Tester shall examine the Vendor-provided documentation to determine that the EHR technology does not allow users to disable encryption status

Inspection Test Guide (Disabling Audit Logs, Audit Log Status, Encryption Status)

- If the EHR technology allows a user to disable the audit log, the audit log status or encryption status, the Tester shall verify the following:
 - IN170.314(d)(2) – 2.01: The Tester shall verify that the date, time (utilizing a system clock that has been synchronized following the (RFC 1305) Network Time Protocol, or (RFC 5905) Network Time Protocol Version 4), and user identification related to the actions of disabling audit logs, disabling audit log status and disabling encryption status are recorded in the audit log entry
 - IN170.314(d)(2) – 2.02: As the EHR technology permits, the Tester shall verify whether audit logs, audit log status and encryption status can or cannot be disabled
 - IN170.314(d)(2) – 2.03: The Tester shall verify that the log in attempt was successful to attempt to disable audit logs, audit log status and encryption status
 - IN170.314(d)(2) – 2.04: The Tester shall verify that the EHR technology does not permit an unauthorized user to enable or disable audit logs, audit log status and encryption status
 - IN170.314(d)(2) – 2.05: The Tester shall verify that the EHR technology allows a user with permission to enable or disable audit logs, audit log status and encryption status
 - IN170.314(d)(2) – 2.06: The Tester shall verify that the changes made to enable/disable audit logs, audit log status and encryption status changes are recorded in the audit log
 - IN170.314(d)(2) – 2.07: The Tester shall verify that the audit log records the identification of the user that made the audit log, audit log status and encryption status changes
 - IN170.314(d)(2) – 2.08: The Tester shall verify that the audit log records the date and time (utilizing a system clock that has been synchronized following the (RFC 1305) Network Time Protocol, or (RFC 5905) Network Time Protocol Version 4) the audit log, audit log status and encryption status changes occur
- If the EHR technology does not allow a user to disable the audit log, the audit log status or encryption status, the Tester shall verify the following:
 - IN170.314(d)(2) – 2.09: The Tester shall verify that the Vendor-identified documentation and function(s) sufficiently explain that the EHR technology does not allow users to disable 1) audit logs, 2) the audit log status, or 3) the encryption status

DTR170.314(d)(2) – 3: Record Actions

Required Vendor Information

- VE170.314(d)(2) – 3.01: The Vendor shall identify the EHR function(s) that are available for a user to perform actions (additions, deletions, changes, queries, print, and copy) related to electronic health information

- If the EHR technology does not allow any users to perform one or more of the actions above, the Vendor must submit documentation identifying that no users may perform the action(s)

VE170.314(d)(2) – 3.02: The Vendor shall identify the EHR function(s) that are available to record actions related to electronic health information. (These will be automatic functions used to create audit log entries.)

VE170.314(d)(2) – 3.03: The Vendor shall identify a patient with an existing record in the EHR to be used for this test and a set of electronic health test data for the patient

VE170.314(d)(2) – 3.04: The Vendor shall identify the EHR function(s) that are available to enable a user to verify that an audit log that has data elements including:

- Date and time of event
- Patient identification
- User identification
- Type of action (additions, deletions, changes, queries, print, copy), specifying inquiry, any changes made (with pointer to original data state) and a delete specification (with a pointer to deleted information)
- Identification of the patient data that is accessed

Required Test Procedures

If the EHR technology does not allow any users to perform one or more of the actions (additions, deletions, changes, queries, print, or copy) required to be performed during the following test steps, refer to IN170.314(d)(2) – 3.04.

TE170.314(d)(2) – 3.01: Using the EHR function(s) and test data identified by the Vendor, the Tester shall make an addition to electronic health information in the patient record provided by the Vendor

TE170.314(d)(2) – 3.02: Using the EHR function(s) and test data identified by the Vendor, the Tester shall make a deletion to electronic health information in the patient record provided by the Vendor

TE170.314(d)(2) – 3.03: Using the EHR function(s) and test data identified by the Vendor, the Tester shall make a change to electronic health information in the patient record provided by the Vendor

TE170.314(d)(2) – 3.04: Using the EHR function(s) and test data identified by the Vendor, the Tester shall make a query about electronic health information in the patient record provided by the Vendor

TE170.314(d)(2) – 3.05: Using the EHR function(s) and test data identified by the Vendor, the Tester shall print electronic health information in the patient record provided by the Vendor

TE170.314(d)(2) – 3.06: Using the EHR function(s) and test data identified by the Vendor, the Tester shall copy electronic health information in the patient record provided by the Vendor

Inspection Test Guide

IN170.314(d)(2) – 3.01: For each action performed in TE170.314(d)(2) – 3.01 through TE170.314(d)(2) – 3.06, the Tester shall verify that the action was recorded in the audit log

IN170.314(d)(2) – 3.02: If the EHR technology permits users to perform addition, change, query, print, or copy actions, the Tester shall verify that the following data elements were recorded by the audit log for each action performed in TE170.314(d)(2) – 3.01 and TE170.314(d)(2) – 3.03 through 3.06

- Date and time (utilizing a system clock that has been synchronized following the (RFC 1305) Network Time Protocol, or (RFC 5905) Network Time Protocol Version 4)
- Patient identification
- User identification
- The action(s) taken, specifying inquiry and any changes made (with pointer to original data state)

IN170.314(d)(2) – 3.03: If the EHR technology permits users to delete electronic health information in TE170.314(d)(2) – 3.02, the Tester shall verify that the following data elements were recorded by the audit log

- Date and time (utilizing a system clock that has been synchronized following the (RFC 1305) Network Time Protocol, or (RFC 5905) Network Time Protocol Version 4)
- Patient identification
- User identification
- The action(s) taken, including a delete specification (with a pointer to deleted information)

IN170.314(d)(2) – 3.04: If the EHR technology does not permit any users to perform one or more of the actions required to be recorded in the audit log (additions, deletions, changes, queries, print, or copy), the Tester shall verify that documentation submitted by the Vendor sufficiently demonstrates that no users are permitted to perform the action(s) in the EHR technology

DTR170.314(d)(2) – 4: Protect Audit Log

Required Vendor Information

VE170.314(d)(2) – 4.01: The Vendor shall submit documentation that identifies the method(s) by which the EHR technology protects 1) recording of actions related to electronic health information, 2) recording of audit log status, and 3) recording of encryption status) from being changed, overwritten, or deleted by the EHR technology

Required Test Procedures

TE170.314(d)(2) – 4.01: The Tester shall examine the Vendor-identified documentation to determine if audit logs are protected from being changed, overwritten, or deleted by the EHR technology

Inspection Test Guide

IN170.314(d)(2) – 4.01: The Tester shall verify that the method(s) presented by the Vendor sufficiently demonstrate that audit logs are protected from being changed, overwritten or deleted by the EHR technology

DTR170.314(d)(2) – 5: Detection of Audit Log Alteration

Required Vendor Information

VE170.314(d)(2) – 5.01: The Vendor shall submit documentation that identifies the method(s) by which the EHR technology detects whether the audit log has been altered

Required Test Procedures

TE170.314(d)(2) – 5.01: The Tester shall examine the Vendor-identified documentation to determine if the EHR technology is capable of detecting whether the audit log has been altered

Inspection Test Guide

IN170.314(d)(2) – 5.01: The Tester shall determine whether the method (s) specified in the Vendor documentation sufficiently demonstrate that the EHR technology is capable of detecting when the audit log has been altered

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	Post-public comment draft	November 19, 2012
1.1	Delivered for National Coordinator Approval	December 3, 2012
1.2	Posted Approved Test Procedure	December 14, 2012
1.3	<p>In the Informative Test Description, “Record Actions” section</p> <ul style="list-style-type: none"> Added “specifying inquiry, any changes made (with pointer to original data state) and a delete specification (with a pointer to deleted information)” to maintain consistency with ASTM E2147-01 requirements <p>In the Normative Test Procedure, DTR170.314(d)(2) – 3: Record Actions In Required Vendor Information</p> <ul style="list-style-type: none"> Added “specifying inquiry, any changes made (with pointer to original data state) and a delete specification (with a pointer to deleted information)” to fourth bullet point in VE170.314(d)(2) – 3.04 to maintain consistency with ASTM E2147-01 requirements <p>In Inspection Test Guide</p> <ul style="list-style-type: none"> Added “specifying inquiry and any changes made (with pointer to original data state)” to fourth bullet point in IN170.314(d)(2) – 3.02 to maintain consistency with ASTM E2147-01 requirements Added “including a delete specification (with a pointer to deleted information)” to fourth bullet point in IN170.314(d)(2) – 3.03 to maintain consistency with ASTM E2147-01 requirements 	May 6, 2013
1.4	<p>Updated Approved Test Procedure</p> <p>Updates:</p> <ul style="list-style-type: none"> Updated the NTP protocol to allow for synching to occur within 5 seconds 	July 11, 2013
1.5	<p>In the Informative Test Description, “Record Actions” section</p> <ul style="list-style-type: none"> Modified language to allow Vendor self-attestation for EHR technology that does not allow any users to perform one or more of the actions required to be recorded in the audit log <p>In the Normative Test Procedure, DTR170.314(d)(2) – 3: Record Actions In Required Vendor Information</p> <ul style="list-style-type: none"> Updated sub-bullet in VE170.314(d)(2) – 3.01 to expand applicability of Vendor self-attestation for impermissible actions from only the delete action to all actions <p>In Required Test Procedures</p> <ul style="list-style-type: none"> Added an exception statement to the beginning of the section that refers readers to relevant the Inspection test step if the EHR technology does not allow any users to perform one or more of the actions required to be recorded in the audit log Removed sub-bullet from TE170.314(d)(2) – 3.02 stating, “If the EHR technology does not allow any users to make deletions related to electronic health information, refer to IN170.314(2) – 3.04” due to addition of revised exception statement, above 	March 19, 2014

Version Number	Description of Change	Date Published
	<p>In Inspection Test Guide</p> <ul style="list-style-type: none">• Updated statement in IN170.314(d)(2) – 3.02 to clearly identify applicable actions (i.e., additions, deletions, changes, queries, print, and copy)• Updated statement in IN170.314(d)(2) – 3.04 to expand inspection of Vendor-submitted documentation from only deletions to all actions	
1.6	<p>Updated Approved Test Procedure</p> <ul style="list-style-type: none">• Modified steps for NTP protocol	December 24, 2014