The Office of the National Coordinator for Health Information Technology

2015 Edition §170.315(d)(2) Auditable Events and Tamper-resistance

Testing Components: Health IT developer self-declaration to the testing outcomes

Test Procedure Version 1.3 – Last Updated 09/21/17

Please consult the Final Rule entitled: 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications for a detailed description of the certification criterion with which these testing steps are associated. We also encourage developers to consult the Certification Companion Guide in tandem with the test procedure as they provide clarifications that may be useful for product development and testing.

Note: The order in which the test steps are listed reflects the sequence of the certification criterion and does not necessarily prescribe the order in which the test should take place.

Required Tests

(d)(2) *Auditable events and tamper-resistance* –

(i) ***Record actions.*** Technology must be able to:

(A) Record actions related to electronic health information in accordance with the standard specified in § 170.210(e)(1);

(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 technology in accordance with the standard specified in § 170.210(e)(3) unless the technology prevents electronic health information from being locally stored on end-user devices (see paragraph (d)(7) of this section).

Cross Reference Criteria:

(d)(7) (ii) Technology is designed to prevent electronic health information from being locally stored on end-user devices after use of the technology on those devices stops.

Standard(s):

§170.210(e)(1):

(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) and changes to user privileges when health IT is in use.

(ii) The date and time must be recorded in accordance with the standard specified at § 170.210(g).

§170.210(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).

§170.210(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)

Criteria ¶	System Under Test	Test Lab Verification
(i)(A)	1. The user demonstrates that the Health IT Module records, at a minimum, each of the following actions, including Auditable Events, in accordance with the standard specified in § 170.210(e)(1)(i), sections 7.2 through 7.4, 7.6, and 7.7 of ASTM E2147-01, when supported, related to electronic health information: • Additions; • Deletions; • Changes, • Queries; • Print; • Copy; • Access to patient information, • Emergency access to patient information • Change to user privilege, • Change to audit log status, and • Change to encryption status. 2. For all permissible actions, the audit log function records the following data elements: • Date and time of event, synchronized according to NTPv3 or NTPv4 in accordance with the standard specified in § 170.210(g); • Patient identification; • User identification; • Type of action, including Auditable Events, as listed in 1, specifying inquiry, any changes made (if any), and for deletions a pointer to deleted information (see the Certification Companion Guide for (d)(2) for more detail as necessary), and • Identification of the Data that are Accessed.	1. The tester verifies that the Health IT Module records an audit log entry for each of the specified actions in accordance with the standard specified in § 170.210(e)(1), when supported. 2. The tester verifies that for all specified actions, an audit log entry related to each action taken has been correctly generated according to the standard specified in § 170.210(e)(1)(i), and that the date/time is recorded in accordance with the standard specified in § 170.210(g). 3. The tester verifies that the actions the health IT developer has indicated it does not support via documentation are not available in the Heath IT Module.

Criteria ¶	System Under Test	Test Lab Verification
(i)(A) continued	3. The health IT developer provides documentation that demonstrates the actions listed above that are not supported within the Module and therefore not subject to testing.	
(i)(B) (Conditional)	If the audit log can be disabled, the user demonstrates that the Health IT Module records when the audit log status changes from enabled to disabled (or vice versa), and logs the status change in accordance with the standard specified in §170.210(e)(2), by recording: • date and time, synchronized according to NTPv3 or NTPv4 in accordance with the standard specified in § 170.210(g); • user identification; and • which action(s) occurred.	Unless the developer attests that the audit log cannot be disabled by any user, the tester verifies that the system appropriately logs changes to the audit log status in accordance with the standard specified in § 170.210(e)(2).
(i)(C) (Conditional)	If electronic health information can be locally stored on end user devices, the Health IT Module records when the encryption status of electronic health information locally stored on end-user devices, by the technology, changes from enabled to disabled (or vice versa) and logs the status change in accordance with the standard specified in § 170.210(e)(3), by recording: • date and time, synchronized according to NTPv3 or NTPv4 in accordance with the standard specified in § 170.210(g); • user identification; and • which action(s) occurred.	Unless the developer attests that the technology prevents electronic health information from being locally stored on end-user devices, the tester verifies that the system appropriately logs changes to the encryption status in accordance with the standard specified in § 170.210(e)(3).

(ii) *Default setting.* 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) and (d)(2)(i)(C) of this section.
Standard(s): None

Criteria ¶	System Under Test	Test Lab Verification
(ii)	The health IT developer provides documentation outlining that by default, the Health IT Module performs the capabilities described in Criteria (i)(A), and where applicable, in Criteria (i)(B) and (i)(C).	The tester verifies that the documentation provided indicates that: • if the audit log can be disabled, the default setting for recording audit log status changes is enabled; • if the encryption status can be disabled, the default setting for recording encryption status changes is enabled; • if the audit log cannot be disabled, it is so indicated by the documentation; and • if the encryption status cannot be disabled, it is so indicated by the documentation.

(iii) *When disabling the audit log is permitted.* For each capability specified in paragraphs (d)(2)(i)(A) through (C) of this section that technology permits to be disabled, the ability to do so must be restricted to a limited set of users.
Standard(s): None

Criteria ¶	System Under Test	Test Lab Verification
(iii) Conditional	Where the Health IT Module permits disabling, the user demonstrates that the capability to do so is restricted to a limited set of users for each auditing function: • Record actions; • Record the audit log status; and • Record encryption status.	The tester verifies that each of the capabilities which permit the ability to enable and disable the recording of auditable events, is limited to an identified set of users: • Record actions; • Record the audit log status; and • Record encryption status.

(iv) *Audit log protection.* Actions and statuses recorded in accordance with paragraph (d)(2)(i) of this section must not be capable of being changed, overwritten, or deleted by the technology.
Standard(s): None

Criteria ¶	System Under Test	Test Lab Verification
(iv)	The health IT developer provides documentation outlining how the audit log protects the following from being changed, overwritten, or deleted by the Health IT Module: • Recording of actions related to electronic health information; • Recording of audit log status; and • Recording of encryption status.	The tester verifies that the Health IT Module audit log protects the outlined items from being changed, overwritten, or deleted from the audit log.

(v) *Detection.* Technology must be able to detect whether the audit log has been altered.
Standard(s): None

Criteria ¶	System Under Test	Test Lab Verification
(v)	The health IT developer provides documentation outlining how alterations to an audit log are detected.	The tester verifies that alterations to an audit log is successfully detected.

Document History

Version Number	Description of Change	Date
1.0	Final Test Procedure	January 08, 2016
1.1	(i)(A) step 2 updated types of actions.	May 08, 2016
1.2	(i)A) “changes to user privilege” was moved to be grouped with “change” to make clear that they can be separately recorded actions or that this more specific change can be labeled first as a “change” and then with more specificity as to the type of change.	May 26, 2017
1.3	As of September 21, 2017, Test Procedure has been moved to Attestation/Developer self-declaration only	September 21, 2017

Dependencies: For all related and required criteria, please refer to the Master Table of Related and Required Criteria.