The Office of the National Coordinator for
Health Information Technology

2015 Edition §170.315(d)(10) Auditing actions on health information

Testing Components:

Test Procedure Version 1.0 – Last Updated 1/08/16

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)(10) Auditing actions on health information - optional, depending on the Health IT Module's configuration.

(i) By default, be set to record actions related to electronic health information in accordance with the standard specified in §170.210(e)(1).

Standards:

§ 170.210(e)(1): (e) Record actions related to electronic health information, audit log status, and encryption of end-user devices. (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 in § 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(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 2013), (incorporated by reference in § 170.299).

Criteria ¶	System Under Test	Test Lab Verification
(i)	1. Documentation is provided by the health IT developer demonstrating that by default, the Health IT Module records actions related to electronic health information in accordance with the standard specified in § 170.210(e)(1). 2. The user demonstrates that the Health IT Module records, at a minimum, each of the following actions 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: a. Additions; b. Deletions; c. Changes; d. Queries; e. Print; f. Copy; g. Changes to user privileges; and h. Access to patient information, including emergency access events. 3. For all permissible actions, specified in step 2, the audit log function records at a minimum 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 (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); and • Identification of the patient data that are accessed.	1. The tester reviews the documentation to verify that the default setting for audit log is enabled, 2. 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. 3. The tester verifies using visual inspection 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 verifies through visual inspection **of time clock synchronization with a time server** that the date/time is recorded in accordance with the standard specified in § 170.210(g). 4. The tester verifies that the health IT developer has submitted documentation indicating each action that is not supported by the Heath IT Module.

(ii) If technology permits auditing 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
(ii) (Conditional)	1. Where the technology 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. 2. Negative test: The unauthorized user is not able to disable the Health IT Module's auditing.	1. 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. 2. Negative test: The tester verifies that the user that does not have access to disable auditing cannot disable auditing.

(iii) Actions recorded related to electronic health information must not be capable of being changed, overwritten, or deleted by the technology.
Standard(s): None

Criteria ¶	System Under Test	Test Lab Verification
(iii)	The health IT developer supplies documentation describing the actions recorded that relate to electronic health information not being changed, overwritten, or deleted.	The tester verifies that the documentation outlines how the audit log cannot be changed, overwritten, or deleted.

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

Criteria ¶	System Under Test	Test Lab Verification
(iv)	The health IT developer supplies documentation describing how alterations to the audit log are detected.	The tester verifies that the documentation outlines how an alteration of an audit log is successfully detected.

Document History

Version Number	Description of Change	Date
1.0	Final Test Procedure	January 08, 2016

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