

2015 Edition §170.315(d)(3) Audit Report(s)

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)(3) Audit report(s). Enable a user to create an audit report for a specific time period and to sort entries in the audit log according to each of the data specified in the standards in §170.210(e).

Standards:

170.210(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 at § 170.210(h) and changes to user privileges when EHR technology is in use.
- (ii) The date and time must be recorded in accordance with the standard specified at § 170.210(g).
- (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).
- (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\(Reapproved 2013\)](#), (incorporated by reference in § 170.299)

Criteria ¶	System Under Test	Test Lab Verification
(d)(3)	<p>Generate Audit Report</p> <ol style="list-style-type: none"> 1. A user generates at least one audit report for a specific time period. 2. The user generates one or more audit reports that include the Date and Time of Event synchronized according to NTPv3 or NTPv4 in accordance with the standard specified in § 170.210(g), and User Identification as well as some or all of the following content as applicable to the audit report(s) generated: <ul style="list-style-type: none"> • Patient Identification; • Type of Action, including Auditable Events specifying inquiry, any changes made (if any), and for deletions, a pointer to deleted information (see Certification Companion Guide for (d)(3) as necessary): <ul style="list-style-type: none"> ○ Additions, ○ Deletions, ○ Changes, ○ Queries, ○ Print, ○ Copy, ○ Access to patient information, ○ Emergency access to patient information, ○ Change to user privilege, ○ Change to audit log status, ○ Change to encryption status, and • Identification of the Data that are Accessed. 	<p>Generate Audit Report</p> <ol style="list-style-type: none"> 1. The tester verifies that the generated audit report(s) data are limited to the specified time period entered in/selected. 2. A) IF a single audit report is generated, the tester verifies that the audit report includes all of the information specified (in the SUT column) when EHR technology is in use. <p style="margin-left: 40px;">B) IF multiple audit reports are generated, the tester verifies that when all of the audit reports are considered together the total content they include represents all of the information specified (in the SUT column) when EHR technology is in use.</p> <p style="margin-left: 40px;">For either pathway 2A or 2B, the Date and Time of Event and User Identification data must always be included in each audit report.</p> <p>Synchronized Clocks</p> <ol style="list-style-type: none"> 1. The tester verifies that the date and time is recorded in the audit report in accordance with the standard specified at § 170.210(g) <p>Change in Audit Log Status (Conditional)</p> <p>If the Health IT Module permits changes to the audit log status:</p> <ol style="list-style-type: none"> 1. The tester verifies that the audit report includes 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: <ul style="list-style-type: none"> • Date and Time of Event; and • User Identification. 2. The tester verifies that the date and time is included in the audit report in accordance with the standard specified at § 170.210(g) when the audit log status is changed.

Criteria ¶	System Under Test	Test Lab Verification
<p>(d)(3), continued</p>	<p>Synchronized Clocks 1. The date and times recorded in the user generated audit report use synchronized clocks.</p> <p>Change in Audit Log Status (Conditional) If the Health IT Module permits changes to the audit log status: 1. The user generated audit report content includes required content when the audit log status is changed. 2. The date and times recorded in the user generated audit report use synchronized clocks when the audit log status is changed.</p> <p>Change in Encryption Status (Conditional) If the Health IT Module permits changes to the encryption status: 1. The user generated audit report content includes required content when the encryption status of electronic health information locally stored by EHR technology on end-user devices is changed. 2. The date and times recorded in the user generated audit report use synchronized clocks when the encryption status of electronic health information locally stored by EHR technology on end-user devices is changed.</p> <p>Sort Audit Log Entries A user can sort the audit report(s) information by the data elements included in the audit report, specified in the standard at §170.210(e).</p>	<p>Change in Encryption Status (Conditional) If the Health IT Module permits changes to the encryption status: 1. The tester verifies that the audit report includes 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 the Health IT Module on end-user devices is changed: <ul style="list-style-type: none"> • Date and Time of Event; and • User Identification. 2. The date and time each action occurs in accordance with the standard specified at § 170.210(g).</p> <p>Sort Audit Log Entries The tester verifies that for each audit report generated the required data included are sortable in ascending or descending order.</p>

Document History

Version Number	Description of Change	Date
1.0	Final Test Procedure	January 08, 2016
1.1	Updated Gap Eligibility	April 08, 2016
1.2	Step 2 for SUT and TLV were both clarified and changed to reflect that multiple audit reports can also be created to meet the criterion. The data references in the SUT column were also re-ordered to make the required data clearer.	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](#).