

§170.315(d)(2) Auditable events and tamper-resistance

2015 Edition Test Procedure

Version 1.3 Updated on 09-21-2017

Revision History

Version #	Description of Change	Version Date
1.0	Final Test Procedure	01-08-2016
1.1	(d)(2)(i)(A) step 2 updated types of actions.	05-08-2016
1.2	(d)(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.	05-26-2017
1.3	As of September 21, 2017, Test Procedure has been moved to Attestation/Developer self-declaration only.	09-21-2017

Regulation Text

Regulation Text

§170.315 (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).

(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.

(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.

(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.

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

Standard(s) Referenced

Cross Reference Criteria

[§ 170.315\(d\)\(7\)\(ii\)](#) 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.

Paragraph (d)(2)(i)(A)

§ 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 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 5905](#)) Network Time Protocol Version 4, (incorporated by reference in § 170.299).

§ 170.210(h) *Audit log content.* [ASTM E2147-01 \(Reapproved 2013\) Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems](#)

Paragraph (d)(2)(i)(B)

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

§ 170.210(h) *Audit log content.* [ASTM E2147-01 \(Reapproved 2013\) Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems](#)

Paragraph (d)(2)(i)(C)

§ 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 5905](#)) Network Time Protocol Version 4, (incorporated by reference in § 170.299).

§ 170.210(h) *Audit log content*. [ASTM E2147-01 \(Reapproved 2013\) Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems](#)

Additional Resources

Not required, but recommended: § 170.210(c)(2) A hashing algorithm with a security strength equal to or greater than SHA-2 as specified by NIST in [FIPS Publication 180-4, Secure Hash Standard, 180-4 \(August 2015\)](#)


Testing components

Self-Declaration: As of September 21, 2017, the testing approach for this criterion is satisfied by self-declaration.

The archived version of the Test Procedure is attached below for reference.

System Under Test	Test Lab Verification
The health IT developer submits their self-declaration to the ONC-ATL.	The Tester verifies the self-declaration document contains all of the required data elements.

Archived Version:

 [§170.315\(d\)\(2\) Test Procedure](#)

Content last reviewed on November 5, 2020