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

2015 Edition CCGs

Version 1.6 Updated on 10-27-2017

Revision History

Version #	Description of Change	Version Date
1.0	Initial Publication	10-22-2015
1.1	Clarification added around types of audit logs which should be captured with this criterion.	03-24-2016
1.2	Clarification added around recording actions in the audit log.	07-06-2016
1.3	Clarification added related to functionality not included in health IT. Clarification added in (d)(2)(i)(C) related to testing (d)(2) without (d)(7).	11-28-2016
1.4	Clarification added for “Query” actions.	01-27-2017
1.5	Clarifications added for the application of this criterion to relied upon software and HISPs. In addition, clarified the meaning of the term “user,” the requirements for recording changes to user privileges, the timing of logging changes is dependent on Health IT design or workflow, and	05-26-2017

	that either a single audit log or multiple audit logs may be used to meet the requirements of this criterion.	
1.6	Clarification added for the entire criterion related to testing of "portal" products.	10-27-2017

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)

Certification Companion Guide: Auditable events and tamper-resistance

This Certification Companion Guide (CCG) is an informative document designed to assist with health IT product development. The CCG is not a substitute for the 2015 Edition final regulation. It extracts key portions of the rule's preamble and includes subsequent clarifying interpretations. To access the full context of regulatory intent please consult the 2015 Edition final rule or other included regulatory reference. The CCG is for public use and should not be sold or redistributed.

Link to Final Rule Preamble

Edition Comparision	Gap Certification Eligible	Base EHR Definition
Revised	No	Not Included

Certification Requirements

Quality management system (§ 170.315(g)(4)) and accessibility-centered design (§ 170.315(g)(5)) must be certified as part of the overall scope of the certificate issued to the product.

- When a single quality management system (QMS) is used, the QMS only needs to be identified once. Otherwise, the QMS' need to be identified for every capability to which it was applied.
- When a single accessibility-centered design standard is used, the standard only needs to be identified once. Otherwise, the accessibility-centered design standards need to be identified for every capability to which they were applied; or, alternatively the developer must state that no accessibility-centered design was used.

Table for Design and Performance

- Quality management system (§ 170.315(g)(4))
- Accessibility-centered design (§ 170.315(g)(5))

Technical Explanations and Clarifications

Applies to entire criterion

Clarifications:

- The ONC Cures Act Final Rule included the requirement for Health IT Modules to support 7.1.3 Duration of Access in the ASTM E2147 – 18 standard. However, ONC determined this requirement will not be in scope for testing and certifying to 2015 Edition Cures Update certification and removed the 7.1.3 requirement in the subsequent IFC.
- The ONC Cures Act Final Rule included the requirement for Health IT Modules to support updates to audit logging and has incorporated by reference the standards, as amended effective June 30, 2020,

§ 170.299(1) ASTM E2147-18 Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems, approved May 1, 2018, IBR approved for §170.210(h).

- For purposes of certification, a Health IT Module should adhere to (RFC 5905) Network Time Protocol Version 4 for the synchronized clock requirement. The previous (RFC 1305) Network Time Protocol is obsolete and was replaced by the updated standard in the IFC..
- Actions and information must be captured in a manner that supports the forensic reconstruction of the sequence of changes to a patient's chart. [77 FR 54235]
- Any changes to a user's privileges must be captured to meet this criterion (e.g., user account creation, user switches roles and new privileges are assigned, revoking privileges, account disabling, etc.). [see also 77 FR 54235]
- If the health IT does not include a capability for which an ''action'' is listed, testing and certification can proceed for the audit log process without health IT showing that it can record actions related to a non-existent capability.
- Similarly, for example, a developer that is seeking to certify a Health IT Module to 170.315(h) will not necessarily have end-user device encryption features (see 170.315(d)(7)). As such, certification can proceed for the audit log process without the health IT Module demonstrating that it can record an encryption status as required by 170.315(d)(2)(i)(C).
- If third party software is relied upon to meet the criteria, one of the following approaches applies:
  - Approach 1 requires disclosure of the software that was relied upon to meet the criterion.
  - Approach 2 requires documentation of how the external services that are necessary to meet the requirements of criteria will be deployed and used.
- A user could be a health care professional or office staff; or a software program or service that would interact directly with the certified health IT. [see 80 FR 62611; 77 FR 54168] A "user" is not a patient for the purposes of this criterion. [see also 77 FR 54168]
- For HISP software that does not normally store patient data, certification to (d)(2) does not create the obligation to do so. Rather, certification to (d)(2) requires that a user is able to produce a forensic reconstruction of events in the case of a security incident. At a minimum, some type of message ID, date/time, sender, receiver, confirmation of receipt, and other values may be necessary. For example, it may be helpful to consider what types of data a user would need to track misrouted or dropped messages. Additionally, the HISP software being certified may contain error queues, support dashboards, and other tools where messages containing PHI are persisted. Audit records would have to be created when actions are performed on PHI through these tools, per (d)(2).
- For portal products seeking (e)(1) certification, testing the activity history log will involve much of the patient level audit recording, such as patient account login, view, download, and transmit actions. This criterion would not be applicable to the patient user. Rather, it applies to administrative functionality such as creating accounts, revoking privileges, and account disabling. It is not applicable to the activity history log for patient use of the (e)(1) functionality.
- Compliance date updated to December 31, 2022, per IFC.

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

Technical outcome – The health IT records actions pertaining to electronic health information in accordance with sections 7.2 through 7.4, 7.6, and 7.7 of the ASTM E2147-01 standard when health it is in use; changes to user privileges when health IT is in use; and records the date and time in accordance with either RFC 1305 or RFC 5905.

Clarifications:

- Only those sections specified from section 7 of ASTM E2147-01 are the minimum required for certification. [see also 77 FR 54234]
- Regarding the granularity of the information we expect to be recorded, this should be consistent with the guidance in Section 7.7 of ASTM E2147-01, which states the "granularity should be specific enough to clearly determine if data designated by federal or state law as requiring special confidentiality protection has been accessed." And, more to the point, Section 7.7 goes on to state

that “[s]pecific category of data content, such as demographics, pharmacy data, test results, and transcribed notes type, should be identified.” For example, the ability of the audit log to record that the user accessed a patient’s medication list would be sufficient for certification, and the audit log would not need to also record the specific medication. [see also 77 FR 54234]

- “Copy” can encompass a variety of actions, including extracting data from the health IT.
- For "Query" actions, some of the fields listed in ASTM E2147-01 may not apply, such as patient ID. To enable a forensic reconstruction of the query, the health IT should capture information about the query, such as the search the user performed, so that a security professional could identify nefarious user behavior. For example, a user performing multiple searches looking for famous individuals who may be patients in the system.
- The certification criterion requires actions initiated by the user from within the health IT interface to be tracked in the audit log. The copy and paste functions of Microsoft Windows originate outside of the health IT environment and are thus outside the scope of certification. Copy actions originating from within the health IT interface (e.g., exporting or downloading a copy of electronic health information from the health IT) are required to be tracked in the audit log.
- Demonstration of the ability to use NIST time servers is required for certification, however vendors are not required to use NIST servers post certification.
- A "pointer to original data state" is a means of identifying original information that has been changed by a user. Similarly, a "pointer to deleted information" is a means of identifying information prior to deletion. A description of a change or deletion is acceptable as long as the type of action is specified and both the original and modified data states are able to be identified. For example, an audit log could include a link to an original document and provide a description of the modified state. Conversely, it could include a description of the original data state and provide a link to the modified document. The certification criterion is not prescriptive of how the requirement should be achieved. Demonstrating the ability to view the original document prior to a change or deletion is an acceptable method of meeting the certification requirement, however it is not required during testing.
- Information related to the required actions (additions, deletions, changes, queries, print, and copy) must be recorded in the audit log, however the certification criterion is not prescriptive to the method by which this is achieved and does not place limitations on the format in which this information is presented in the audit log. Namely, the audit log should record actions in a way that assists the user in reconstructing events that occurred effecting health information. For example, a "change" action may be listed in the audit log as an "edit" event if that is the labeling the user is accustomed to using in the health IT Module for those kinds of actions.
- “Changes to user privilege” are considered a type of “change.” Health IT may separately record this auditable event or may reflect an approach that records user privilege changes as a subtype or reason (description) for the change.
- If the audit log reflects the privilege modification to each individual user account that was part of the group, the privilege modification may be applied as a group change.
- The elements "Patient identification" and "Identification of the patient data that are accessed" are not applicable when capturing a "user privilege change" action.
- The exact point in time when an action is logged may depend on the architecture/design of the Health IT Module or the workflow.
- For the purposes of certification, a Health IT Module may create a single audit log file with all of the specified auditable data or it may use multiple audit log files. However, if this latter approach is used, when all of the audit log files are considered together the total content they include must represent all of the required auditable data (which would be equivalent to the single audit log file approach).

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

Technical outcome – The health IT records the audit log status in accordance with sections 7.2 and 7.4 of the ASTM E2147-01 standard when the audit log status is changed and records the date and time each action occurs in accordance with either RFC 1305 or RFC 5905.

Clarifications:

- This provision only applies when the technology allows the audit log to be disabled.
- Only those sections specified from section 7 of ASTM E2147-01 are the minimum required for certification. [see also 77 FR 54234]

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

Technical outcome – The health IT records the information specified in sections 7.2 and 7.4, of the ASTM E2147-01 standard when the encryption status of locally stored electronic health information on end-user devices is changed and records the date and time each action occurs in accordance with either RFC 1305 or RFC 5905.

Clarifications:

- Only those sections specified from section 7 of ASTM E2147-01 are the minimum required for certification. [see also 77 FR 54234]
- This provision does not apply when the technology prevents electronic health information from being locally stored on end-user devices.
- Paragraph 170.315(d)(2)(i)(C) is NOT applicable for the privacy and security testing and certification of a Health IT Module required by § 170.550(h)(3)(iii), (v), (vii), and (viii). This specific requirement was intended to be exempted. It would only apply if § 170.315(d)(7) was also required for privacy and security testing and certification, which it is not under the aforementioned paragraphs.

Paragraph (d)(2)(ii)

Technical outcome – The health IT is set by default to record actions related to electronic health information (per provision (d)(2)(i)(A)), (where applicable) record the audit log status (per provision (d)(2)(i)(B)), and (where applicable) record the encryption status of locally stored electronic health information on end-user devices (per provision (d)(2)(i)(C)).

Clarifications:

- To meet this provision for certification, the health IT must be set by default to record the actions and information specified. This is to ensure that at the point of installation or upgrade, the health IT will be set by default for a provider to record the actions and information specified. [see also 77 FR 54233]
- The default setting requirement is only applicable for recording the audit log status if the technology permits the audit log be disabled.
  - The default setting requirement is only applicable for recording the encryption status of electronic health information when the information is locally stored on end-user devices. [see also 77 FR 54233]
- The developer must demonstrate that the audit log is capable of recording the details (date, time, and user identification at a minimum) related to enabling and disabling of the encryption status. However, if the health IT is designed in such a way that no users are able to enable or disable the encryption status, the vendor is permitted to submit supporting documentation to demonstrate this. Requirements related to the specific process of encrypting electronic health information locally stored on end- user devices by health IT are outside the scope of this certification criterion, but are addressed in the § 170.315(d)(7) End-user device encryption certification criterion.

Paragraph (d)(2)(iii)

Technical outcome – The health IT will restrict the ability for auditing to be disabled to a limited set of users if the technology permits auditing to be disabled.

Clarifications:

- Health IT does not have to interpret the meaning of "limited." To meet this provision, health IT would need to include a capability that allows only a limited set of users to have the privileges necessary to change when auditing is enabled or disabled. Generally, we would expect any general health IT user could perform such actions. [see also 77 FR 54233]

Paragraph (d)(2)(iv)

Technical outcome – The health IT will not allow actions and status recorded related to electronic health information per provision (d)(2)(i)(A), (B), and (C) to be changed, overwritten, or deleted by the technology.

Clarifications:

- This provision would not prohibit an organization from making a policy decision to delete or purge audit logs after a legal retention period. Rather it focuses only on the prohibition of health IT to delete an audit log as a condition of certification. [see also 77 FR 54235]

Paragraph (d)(2)(v)

Technical outcome – The health IT must be able to detect whether the audit log has been altered.

Clarifications:

- This provision requires health IT to be able to determine whether activity outside of its control has in some way altered the audit log (e.g., that the operating system was exploited to modify the health IT's database). [see also 77 FR 54235]
- We encourage the use hashing algorithms with strength equal or greater than SHA-2 as specified in FIPS 180-4 (Secure Hash Standard) to determine whether the audit log has been altered. [see also 77 FR 54235]

Content last reviewed on November 5, 2020