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

2015 Edition CCGs

Version 1.0 Updated on 10-26-2015

Revision History

Version #	Description of Change	Version Date
1.0	Initial Publication	10-26-2015

Regulation Text

Regulation Text

§170.315 (d)(10) *Auditing actions on health information*—

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

(ii) If technology permits auditing to be disabled, the ability to do so must be restricted to a limited set of users.

(iii) Actions recorded related to electronic health information must not be capable of being changed, overwritten, or deleted by the technology.

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

Standard(s) Referenced

Paragraph (d)(10)(i)

§ 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 1305) Network Time Protocol or (RFC 5905) Network Time Protocol Version 4

§ 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: Auditing actions on health information

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
New	No	Not Included

Certification Requirements

This certification criterion at § 170.315(d)(10) may be required as part of the 2015 Edition privacy and security approach for the certification criteria at § 170.315(g)(7), (g)(8), and (g)(9). A developer may choose to demonstrate either § 170.315(d)(2) or § 170.315(d)(10) as part of the 2015 Edition privacy & security approach for § 170.315(g)(7), (g)(8), and (g)(9). If the developer chooses to demonstrate § 170.315(d)(10) for § 170.315(g)(7), (g)(8), and/or (g)(9), this criterion at § 170.315(d)(10) only needs to be demonstrated once as part of the overall scope of the certificate sought.

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:

- This criterion is an "abridged" version of § 170.315(d)(2) "auditable events and tamper resistance" as some of the capabilities included in § 170.315(d)(2) would likely not apply to a Health IT Module certified only to the applicable programming interface ("API") criteria, such as recording the audit log status or encryption status of electronic health information locally stored on end-user devices by the technology. A developer may choose to certify either § 170.315(d)(2) or this criterion at § 170.315(d)(10) to meet the requirements of 2015 Edition privacy and security approach. [see also 80 FR 62677]

Paragraph (d)(10)(i)

Technical outcome – The health IT, by default, is set to track 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, and records the date and time in accordance with either RFC 1305 or RFC 5905.

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 in § 170.210(e)(1). [see also 77 FR 54233]
- Only those sections specified from section 7 (i.e., 7.2 through 7.4, 7.6, and 7.7) 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]
- We intend that the actions and information can be captured in a manner that supports the forensic reconstruction of the sequence of changes to a patient's chart. [see also 77 FR 54235]
- "Copy" can encompass a variety of actions, including extracting data from the health IT.
- 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.
- 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. Developers may design systems to place content in the audit log as long as the audit logs can be used to identify the information before and after change. 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.

Paragraph (d)(10)(ii)

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)(10)(iii)

Technical outcome – The health IT will not allow actions recorded related to electronic health information 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)(10)(iv)

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]
- Hashing is one method to detect whether an audit log has been altered. We encourage the use of hashing algorithms 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 June 22, 2020