

# 2015 Edition Certification Companion Guide

## Auditable events and tamper-resistance - 45 CFR 170.315(d)(2)

Links will be updated as available: [Final Rule Preamble](#) – [Test Procedure](#) – [Test Data](#)

Version 1.3 – Last Updated 11/28/2016

New/Revised/Unchanged Compared to 2014 Edition	Gap Certification Eligible	Base EHR Definition	Certified EHR Technology Definition	Associated EHR Incentive Program Objective(s)
Revised	No	No	Not Included	N/A

### 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.

### Regulation Text

#### 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.

Criterion Subparagraph	Technical Explanations and Clarifications	Standard(s) Referenced
Applies to entire criterion	<p><b>Clarification:</b></p> <ul style="list-style-type: none"> <li>• Actions and information must be captured in a manner that supports the forensic reconstruction of the sequence of changes to a patient’s chart. [ <a href="#">77 FR 54235</a> ]</li> <li>• 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 <a href="#">77 FR 54235</a> ]</li> <li>• 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.</li> <li>• 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).</li> </ul>	
(i)(A)	<ul style="list-style-type: none"> <li>• 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.</li> </ul> <p><b>Clarifications:</b></p> <ul style="list-style-type: none"> <li>• Only those sections specified from section 7 of ASTM E2147-01 are the minimum required for certification. [see also <a href="#">77 FR 54234</a> ]</li> <li>• 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 <a href="#">77 FR 54234</a> ]</li> <li>• “Copy” can encompass a variety of actions, including extracting data from the health IT.</li> </ul>	<p>§ 170.210(e)(1)</p> <p>(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.</p> <p>(ii) The date and time must be recorded in accordance with the standard specified at § 170.210(g).</p> <p>§ 170.210(h) <a href="#">ASTM E2147-01 (Reapproved 2013) Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems</a></p> <p>§ 170.210(g) The date and time recorded utilize a system clock that has been synchronized following (<a href="#">RFC 1305</a>) Network Time Protocol, or (<a href="#">RFC 5905</a>) Network Time Protocol Version 4.</p>

Criterion Subparagraph	Technical Explanations and Clarifications	Standard(s) Referenced
(i)(A), continued	<ul style="list-style-type: none"> <li>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.</li> <li>Demonstration of the ability to use NIST time servers is required for certification, however vendors are not required to use NIST servers post certification.</li> <li>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.</li> <li>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.</li> </ul>	
(i)(B)	<ul style="list-style-type: none"> <li>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.</li> </ul> <p><b>Clarifications:</b></p> <ul style="list-style-type: none"> <li>This provision only applies when the technology allows the audit log to be disabled.</li> <li>Only those sections specified from section 7 of ASTM E2147-01 are the minimum required for certification. [see also <a href="#">77 FR 54234</a>]</li> </ul>	<p>§ 170.210(e)(2)</p> <p>(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.</p> <p>(ii) The date and time each action occurs in accordance with the standard specified at § 170.210(g).</p>

Criterion Subparagraph	Technical Explanations and Clarifications	Standard(s) Referenced
(i)(B), continued	See above.	<p>§ 170.210(h) <a href="#">ASTM E2147-01 (Reapproved 2013) Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems</a></p> <p>§ 170.210(g) The date and time recorded utilize a system clock that has been synchronized following (<a href="#">RFC 1305</a>) Network Time Protocol, or (<a href="#">RFC 5905</a>) Network Time Protocol Version 4.</p>
(i)(C)	<ul style="list-style-type: none"> <li>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.</li> </ul> <p><b>Clarifications:</b></p> <ul style="list-style-type: none"> <li>Only those sections specified from section 7 of ASTM E2147-01 are the minimum required for certification. [see also <a href="#">77 FR 54234</a>]</li> <li>This provision does <u>not</u> apply when the technology prevents electronic health information from being locally stored on end-user devices.</li> <li>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.</li> </ul>	<p>§ 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).</p> <p>§ 170.210(h) <a href="#">ASTM E2147-01 (Reapproved 2013) Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems</a></p> <p>§ 170.210(g) The date and time recorded utilize a system clock that has been synchronized following (<a href="#">RFC 1305</a>) Network Time Protocol, or (<a href="#">RFC 5905</a>) Network Time Protocol Version 4.</p>

Criterion Subparagraph	Technical Explanations and Clarifications	Standard(s) Referenced
(ii)	<ul style="list-style-type: none"> <li>Technical outcome – The Health IT is set by default to record actions related to electronic health information (per provision (i)(A)), (where applicable) record the audit log status (per provision (i)(B)), and (where applicable) record the encryption status of locally stored electronic health information on end-user devices (per provision (i)(C)).</li> </ul> <p><b>Clarifications:</b></p> <ul style="list-style-type: none"> <li>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 <a href="#">77 FR 54233</a>]</li> <li>The default setting requirement is only applicable for recording the audit log status if the technology permits the audit log be disabled.</li> <li>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 <a href="#">77 FR 54233</a>]</li> <li>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 <a href="#">§170.315(d)(7)</a> End-user device encryption certification criterion.</li> </ul>	N/A
(iii)	<ul style="list-style-type: none"> <li>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.</li> </ul> <p><b>Clarifications:</b></p> <ul style="list-style-type: none"> <li>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 <a href="#">77 FR 54233</a>]</li> </ul>	N/A

Criterion Subparagraph	Technical Explanations and Clarifications	Standard(s) Referenced
(iv)	<ul style="list-style-type: none"> <li>Technical outcome – The health IT will not allow actions and status recorded related to electronic health information per provision (i)(A), (B), and (C) to be changed, overwritten, or deleted by the technology.</li> </ul> <p><b>Clarifications:</b></p> <ul style="list-style-type: none"> <li>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 <a href="#">77 FR 54235</a>]</li> </ul>	N/A
(v)	<ul style="list-style-type: none"> <li>Technical outcome – The health IT must be able to detect whether the audit log has been altered.</li> </ul> <p><b>Clarifications:</b></p> <ul style="list-style-type: none"> <li>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 <a href="#">77 FR 54235</a>]</li> <li>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 <a href="#">77 FR 54235</a>]</li> </ul>	Not required, but recommended: <a href="#">FIPS PUB 180-4, Secure Hash Standard, 180-4 (August 2015)</a>

**Note:** 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.

### Version History

Version #	Change(s) Summary	Date Made
1.0	Initial Publication	Oct 22, 2015
1.1	Clarification added around types of audit logs which should be captured with this criterion	Mar 24, 2016
1.2	Clarification added around recording actions in the audit log	Jul 06, 2016
1.3	Clarification added related to functionality not included in health IT. Clarification added in (i)(C) related to testing (d)(2) without (d)(7).	Nov 28, 2016