§170.315(d)(7) End-user device encryption

2015 Edition CCGs

Version 1.1 Updated on 03-24-2016

Revision History

Version #	Description of Change	Version Date
1.0	Initial Publication	10-22-2015
1.1	Clarification added regarding attestation or documentation used to meet electronic health information not being stored on end-user devices after technology stops.	03-24-2016

Regulation Text

Regulation Text

§170.315 (d)(7) *End-user device encryption*—

The requirements specified in one of the following paragraphs (that is, paragraphs (d)(7)(i) and (d)(7)(ii) of this section) must be met to satisfy this certification criterion.

(i) Technology that is designed to locally store electronic health information on end-user devices must encrypt the electronic health information stored on such devices after use of the technology on those devices stops.

(A) Electronic health information that is stored must be encrypted in accordance with the standard specified in §170.210(a)(2).

(B) *Default setting.* Technology must be set by default to perform this capability and, unless this configuration cannot be disabled by any user, the ability to change the configuration must be restricted to a limited set of identified users.

(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.

Standard(s) Referenced

Paragraph (d)(7)(i)(A)

§ 170.210(a)(2) *General.* Any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, October 8, 2014

Certification Companion Guide: End-user device encryption

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	In Scope for CEHRT Definition
Unchanged	Yes	Not Included	No

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:

- To meet the criterion, only one paragraph (d)(7)(i) or (ii) needs to be met. Both do not need to be demonstrated.
- Use of technology is considered to be stopped when a user closes or exits the technology application and a user would need to re-execute the technology application to again engage in use. Testing and certification will focus on normal terminations. [see also 77 FR 54237]
- Locally stored electronic health information is intended to mean the storage actions that technology is programmed to take (i.e., creation of temp files, cookies, or other types of cache approaches) and not an individual or isolated user action to save or export a file to their personal electronic storage media. [see also 77 FR 54238]
- This criterion focuses on, and only applies with respect to, the storage capabilities that are designed for use with developer provided or supported technologies for desktop, laptop, or mobile technologies. [see also 77 FR 54238]
- The functionality included in this certification criterion does not focus on server-side or data center hosted technology. [see also 77 FR 54238] Rather, this criterion focuses on data locally stored on end-user devices after the use of the technology is stopped. [see also 77 FR 54238]
- Information that has been sent to a print queue or downloaded by the user (e.g., download a PDF report) is no longer considered managed by the technology. [see also 77 FR 54238]
- This certification criterion does not supersede or affect the HIPAA Security Rule's requirements or associated flexibilities. HHS has issued guidance[1] around encryption as a possible risk management strategy to address storage of electronic protected health information. HHS has also issued guidance[2] on how to render unsecured protected health information unusable, unreadable, or indecipherable to unauthorized individuals. We recommend developers refer to this guidance in developing their products. [see also 77 FR 54239]

---

1 https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf?language=es

2 https://www.federalregister.gov/documents/2012/09/04/2012-20982/health-information-technology-standards-implementation-specifications-and-certification-criteria-for#footnote-32

Paragraph (d)(7)(i)(A)

Technical outcome – Technology designed to locally store electronic health information on end-user devices must encrypt such information after use of technology on those devices stops in accordance with any encryption algorithm in Annex A of FIPS 140-2.

Clarifications:

- We encourage developers to use encryption algorithms, such as AES, that are included in Annex A of FIPS 140-2. [see also 77 FR 54239]

Paragraph (d)(7)(i)(B)

Technical outcome – The technology must be set by default to perform the capability in provision (d)(7)(i)(A) and the ability to change the configuration must be restricted to a limited set of identified users unless

the configuration cannot be disabled by any user.

Clarifications:

- If the developer designs technology that requires or utilizes locally stored electronic health information, it is the developer's responsibility to ensure that such information is set to be encrypted by default in order to meet this criterion. This could be accomplished through different technical mechanisms including techniques to "sandbox" and limit the extent to which data can be accessed and used to only be within a secure session. [see also 77 FR 54238]

Paragraph (d)(7)(ii)

Technical outcome – The technology prevents electronic health information from being locally stored on end-user devices after the technology on those devices stops.

Clarifications:

- The language for this portion of criterion acknowledges that despite a health IT developer's best effort to design health IT in such a way that electronic health information never remains, we understand that such absolutes cannot always be guaranteed (especially when an health IT developer is unable to modify the functionality a particular web browser or operating system employs). [see also 77 FR 54238]
- A health IT developer would not have to demonstrate that its technology can encrypt electronic health information locally stored on end-users devices if the EHR technology is designed to prevent electronic health information from being locally stored on end-user devices after use of health IT on those devices stops. [see also 77 FR 54238]
- We interpret "prevent" to include, for example, situations where health IT is designed to and would normally disallow electronic health information to be locally stored on end-user devices after use of health IT on those devices stops, but is run in a browser that does not respect "no-cache" headers. In this circumstance, and if shown under normal circumstances (i.e., running in a browser that does respect "no-cache" headers), the EHR technology could meet paragraph (d)(7)(ii) of this certification criterion. [see also 77 FR 54238]
- Health IT developer attestation or documentation could be used to meet the requirements of this criterion.

Content last reviewed on September 24, 2018