End-user device encryption | HealthIT.gov

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

- Certification Companion Guide (CCG)
- Conformance Method

Updated on 03-11-2024

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.

1. 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.
    1. Electronic health information that is stored must be encrypted in accordance with the standard specified in § 170.210(a)(2).
    2. *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.
2. 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 Dependencies

Design and performance: 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.

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

Revision History

Version #	Description of Change	Version Date
1.0	Initial publication	03-11-2024

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.

1. 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.
   1. Electronic health information that is stored must be encrypted in accordance with the standard specified in § 170.210(a)(2).
   2. *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.
2. 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 Dependencies
Design and performance: 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.

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

Revision History

Version #	Description of Change	Version Date
1.0	Initial publication	03-11-2024

Testing components

Attestation: As of September 21, 2017, the testing approach for this criterion is satisfied by attestation.

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

System Under Test	ONC-ACB Verification
The health IT developer will attest directly to the ONC-ACB to conformance with the § 170.315(d)(7) *End-user device encryption* requirements.	The ONC-ACB verifies the health IT developer attests conformance to the § 170.315(d)(7) *End-user device encryption* requirements.

Archived Version:
§170.315(d)(7) Test Procedure
Updated on 03-11-2024

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.

1. 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.
    1. Electronic health information that is stored must be encrypted in accordance with the standard specified in § 170.210(a)(2).
    2. *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.
2. 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 Dependencies

Design and performance: 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.

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

Revision History

Version #	Description of Change	Version Date
1.0	Initial publication	03-11-2024

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.

1. 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.
    1. Electronic health information that is stored must be encrypted in accordance with the standard specified in § 170.210(a)(2).
    2. *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.
2. 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 Dependencies

Design and performance: 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.

- Quality management system (§ 170.315(g)(4)): 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.

- Accessibility-centered design (§ 170.315(g)(5)): 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.

Revision History

Version #	Description of Change	Version Date
1.0	Initial publication	03-11-2024

Certification Companion Guide: End-user device encryption

This Certification Companion Guide (CCG) is an informative document designed to assist with health IT product certification. The CCG is not a substitute for the requirements outlined in regulation and related ONC final rules. It extracts key portions of ONC final rules' preambles and includes subsequent clarifying interpretations. To access the full context of regulatory intent please consult the Certification Regulations page for links to all ONC final rules or consult other regulatory references as noted. The CCG is for public use and should not be sold or redistributed.

The below table outlines whether this criterion has additional Maintenance of Certification dependencies, update requirements and/or eligibility for standards updates via SVAP. Review the Certification Dependencies and Required Update Deadline drop-downs above if this table indicates "yes" for any field.

Base EHR Definition	Real World Testing	Insights Condition	SVAP	Requires Updates
Not Included	No	No	No	No

Certification Requirements

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 (e.g., 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. 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 around encryption as a possible risk management strategy to address storage of electronic protected health information. HHS has also issued guidance 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]

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 (e.g., 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. 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 around encryption as a possible risk management strategy to address storage of electronic protected health information. HHS has also issued guidance 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]

Paragraph (d)(7)(i)(A) End-user device encryption

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:

> ONC encourages developers to use encryption algorithms, such as Advanced Encryption Standard (AES), that are included in Annex A of FIPS 140-2. [see also 77 FR 54239]

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:

> ONC encourages developers to use encryption algorithms, such as Advanced Encryption Standard (AES), that are included in Annex A of FIPS 140-2. [see also 77 FR 54239]

Paragraph (d)(7)(i)(B) Default setting

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]

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) Local storage

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, ONC understands that such absolutes cannot always be guaranteed (especially when a 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-user 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]
- ONC interprets “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 (e.g., 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.

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, ONC understands that such absolutes cannot always be guaranteed (especially when a 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-user 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]
- ONC interprets “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 (e.g., 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.

Was this page helpful?

Form Approved OMB# 0990-0379 Exp. Date 9/30/2025

Content last reviewed on March 11, 2024