Encrypt authentication credentials | HealthIT.gov

healthit.gov/test-method/encrypt-authentication-credentials

§170.315(d)(12) Encrypt authentication credentials

- Certification Companion Guide (CCG)
- Conformance Method

Updated on 03-11-2024

Regulation Text

Regulation Text

§ 170.315 (d)(12) *Encrypt authentication credentials*. Health IT developers must make one of the following attestations and may provide the specified accompanying information, where applicable:

1. Yes – the Health IT Module encrypts stored authentication credentials in accordance with standards adopted in § 170.210(a)(2).
2. No – the Health IT Module does not encrypt stored authentication credentials. When attesting "no," the health IT developer may explain why the Health IT Module does not support encrypting stored authentication credentials.

Standard(s) Referenced

Paragraph (d)(12)(i)

§ 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, October 8, 2014 (incorporated by reference in §170.299).

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)(12) *Encrypt authentication credentials*. Health IT developers must make one of the following attestations and may provide the specified accompanying information, where applicable:

1. Yes – the Health IT Module encrypts stored authentication credentials in accordance with standards adopted in § 170.210(a)(2).
2. No – the Health IT Module does not encrypt stored authentication credentials. When attesting "no," the health IT developer may explain why the Health IT Module does not support encrypting stored authentication credentials.

Standard(s) Referenced

Paragraph (d)(12)(i)

§ 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, October 8, 2014 (incorporated by reference in §170.299).

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

This Test Procedure illustrates the test steps required to certify a Health IT Module to this criterion. Please consult the most recent ONC Final Rule on the Certification Regulations page for a detailed description of the certification criterion with which these testing steps are associated. ONC also encourages developers to consult the Certification Companion Guide in tandem with the test procedure as it provides clarifications that may be useful for product development and testing.

Note: The test step order does not necessarily prescribe the order in which the tests should take place.

Testing components

Paragraph (d)(12)(i) - (Alternative)

System Under Test

The health IT developer attests, “Yes, the Health IT Module stores authentication credentials in accordance with standards adopted in § 170.210(a)(2).”

Test Lab Verification

The ONC-ACB verifies the health IT developer attests, “Yes, the Health IT Module encrypts stored authentication credentials in accordance with standards adopted in § 170.210(a)(2).”

System Under Test	ONC-ACB Verification
The health IT developer attests, “Yes, the Health IT Module stores authentication credentials in accordance with standards adopted in § 170.210(a)(2).”	The ONC-ACB verifies the health IT developer attests, “Yes, the Health IT Module encrypts stored authentication credentials in accordance with standards adopted in § 170.210(a)(2).”

Paragraph (d)(12)(ii) - (Alternative)

System Under Test

1. The health IT developer attests, “No, the Health IT Module does not encrypt stored authentication credentials.”
2. The health IT developer may submit an explanation why the Health IT Module does not encrypt stored authentication credentials.

Test Lab Verification

1. The ONC-ACB verifies the health IT developer attests “No, the Health IT Module does not encrypt stored authentication credentials.”
2. If the health IT developer provides an explanation, then the ONC-ACB verifies the health IT developer provides explanation why the Health IT Module does not encrypt stored authentication credentials.

System Under Test	ONC-ACB Verification

System Under Test	ONC-ACB Verification
1. The health IT developer attests, “No, the Health IT Module does not encrypt stored authentication credentials.”	1. The ONC-ACB verifies the health IT developer attests “No, the Health IT Module does not encrypt stored authentication credentials.”
2. The health IT developer may submit an explanation why the Health IT Module does not encrypt stored authentication credentials.	2. If the health IT developer provides an explanation, then the ONC-ACB verifies the health IT developer provides explanation why the Health IT Module does not encrypt stored authentication credentials.

Updated on 03-11-2024

Regulation Text

Regulation Text

§ 170.315 (d)(12) *Encrypt authentication credentials*. Health IT developers must make one of the following attestations and may provide the specified accompanying information, where applicable:

1. Yes – the Health IT Module encrypts stored authentication credentials in accordance with standards adopted in § 170.210(a)(2).
2. No – the Health IT Module does not encrypt stored authentication credentials. When attesting “no,” the health IT developer may explain why the Health IT Module does not support encrypting stored authentication credentials.

Standard(s) Referenced

Paragraph (d)(12)(i)

§ 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, October 8, 2014 (incorporated by reference in §170.299).

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)(12) *Encrypt authentication credentials*. Health IT developers must make one of the following attestations and may provide the specified accompanying information, where applicable:

1. Yes – the Health IT Module encrypts stored authentication credentials in accordance with standards adopted in § 170.210(a)(2).
2. No – the Health IT Module does not encrypt stored authentication credentials. When attesting "no," the health IT developer may explain why the Health IT Module does not support encrypting stored authentication credentials.

Standard(s) Referenced

Paragraph (d)(12)(i)

§ 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, October 8, 2014 (incorporated by reference in §170.299).

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: Encrypt authentication credentials

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:

- The criterion does not require certified health IT to have these capabilities or for health IT developers to implement these capabilities for a specific use case or any use case, just that they attest “yes” or “no” to whether the Health IT Module encrypts authentication credentials. The criterion places no requirements on health IT customers, such as healthcare providers, to implement these capabilities (if present in their products) in their health care settings.
- If a health IT developer attests “no” to support for encrypting stored authentication credentials, they may provide an explanation to the ONC Authorized Certification Body (ONC-ACB) that is either a hard copy or in an acceptable human readable electronic format. To be open and transparent to the public, developers should provide a hyperlink to any optional documentation to be published with the product on the ONC Certified Health IT Product List (CHPL).
- The referenced standard item “§ 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” has been updated to a new version dated October 12, 2021. It is recommended that health IT developers use the updated NIST-documented standard for encryption algorithms.
- Encrypting authentication credentials may include password encryption or cryptographic hashing, which is storing encrypted or cryptographically hashed passwords, respectively (85 FR 25700).

Clarifications:

- The criterion does not require certified health IT to have these capabilities or for health IT developers to implement these capabilities for a specific use case or any use case, just that they attest “yes” or “no” to whether the Health IT Module encrypts authentication credentials. The criterion places no requirements on health IT customers, such as healthcare providers, to implement these capabilities (if present in their products) in their health care settings.
- If a health IT developer attests “no” to support for encrypting stored authentication credentials, they may provide an explanation to the ONC Authorized Certification Body (ONC-ACB) that is either a hard copy or in an acceptable human readable electronic format. To be open and transparent to the public, developers should provide a hyperlink to any optional documentation to be published with the product on the ONC Certified Health IT Product List (CHPL).
- The referenced standard item “§ 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” has been updated to a new version dated October 12, 2021. It is recommended that health IT developers use the updated NIST-documented standard for encryption algorithms.
- Encrypting authentication credentials may include password encryption or cryptographic hashing, which is storing encrypted or cryptographically hashed passwords, respectively (85 FR 25700).

Paragraph (ii) Attesting "no"

Clarifications:

> If a health IT developer attests “no” for its Health IT Module(s) it can indicate why the Health IT Module(s) does not support encrypting stored authentication credentials. For example, the health IT developer could explain that its Health IT Module is not designed to store authentication credentials; therefore, there is no need for the Health IT Module to encrypt authentication credentials.

Clarifications:

> If a health IT developer attests “no” for its Health IT Module(s) it can indicate why the Health IT Module(s) does not support encrypting stored authentication credentials. For example, the health IT developer could explain that its Health IT Module is not designed to store authentication credentials; therefore, there is no need for the Health IT Module to encrypt authentication credentials.

Was this page helpful?

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

Content last reviewed on March 11, 2024