Multi-factor authentication | HealthIT.gov

§170.315(d)(13) Multi-factor authentication

- Certification Companion Guide (CCG)
- Conformance Method

Updated on 03-11-2024

Regulation Text

Regulation Text

§ 170.315 (d)(13) *Multi-factor authentication*.

Health IT developers must make one of the following attestations and, as applicable, provide the specified accompanying information:

1. Yes – the Health IT Module supports the authentication, through multiple elements, of the user's identity with the use of industry-recognized standards. When attesting "yes," the health IT developer must describe the use cases supported.
2. No – the Health IT Module does not support authentication, through multiple elements, of the user's identity with the use of industry-recognized standards. When attesting "no," the health IT developer may explain why the Health IT Module does not support authentication, through multiple elements, of the user's identity with the use of industry recognized standards.

Standard(s) Referenced

None

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)(13) *Multi-factor authentication*.

Health IT developers must make one of the following attestations and, as applicable, provide the specified accompanying information:

1. Yes – the Health IT Module supports the authentication, through multiple elements, of the user's identity with the use of industry-recognized standards. When attesting "yes," the health IT developer must describe the use cases supported.
2. No – the Health IT Module does not support authentication, through multiple elements, of the user's identity with the use of industry-recognized standards. When attesting "no," the health IT developer may explain why the Health IT Module does not support authentication, through multiple elements, of the user's identity with the use of industry recognized standards.

Standard(s) Referenced

None

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)(13)(i) – Attesting "yes" (Alternative)

System Under Test

1. The health IT developer attests, “Yes, the Health IT Module supports authentication, through multiple elements, of the user’s identity with the use of industry-recognized standards,” and;

2. The health IT developer submits a description of the supported use cases.

Test Lab Verification

1. The ONC-ACB verifies the health IT developer attests, ”Yes, the Health IT Module supports the authentication, through multiple elements, of the user’s identity with the use of industry-recognized standards.”
2. The ONC-ACB verifies the health IT developer provided a description of the supported use cases.

System Under Test	**ONC-ACB Verification**
1. The health IT developer attests, “Yes, the Health IT Module supports authentication, through multiple elements, of the user’s identity with the use of industry-recognized standards,” and; 2. The health IT developer submits a description of the supported use cases.	1. The ONC-ACB verifies the health IT developer attests, ”Yes, the Health IT Module supports the authentication, through multiple elements, of the user’s identity with the use of industry-recognized standards.” 2. The ONC-ACB verifies the health IT developer provided a description of the supported use cases.

Paragraph (d)(13)(ii) - Attesting "no" (Alternative)

System Under Test

1. The health IT developer attests, “No, the Health IT Module does not support authentication, through multiple elements, of the user’s identity with the use of industry-recognized standards.”
2. The health IT developer may submit an explanation why the Health IT Module does not support authentication, through multiple elements, of the user’s identity with the use of industry-recognized standards.

Test Lab Verification

1. The ONC-ACB verifies the health IT developer attests, “No, the Health IT Module does not support authentication, through multiple elements, of the user’s identity with the use of industry-recognized standards.”
2. If the health IT developer provides an explanation why the Health IT Module does not support authentication, through multiple elements, of the user’s identity with the use of industry-recognized standards, then the ONC-ACB verifies the health IT developer’s explanation.

System Under Test	ONC-ACB Verification
1. The health IT developer attests, “No, the Health IT Module does not support authentication, through multiple elements, of the user’s identity with the use of industry-recognized standards.” 2. The health IT developer may submit an explanation why the Health IT Module does not support authentication, through multiple elements, of the user’s identity with the use of industry-recognized standards.	1. The ONC-ACB verifies the health IT developer attests, “No, the Health IT Module does not support authentication, through multiple elements, of the user’s identity with the use of industry-recognized standards.” 2. If the health IT developer provides an explanation why the Health IT Module does not support authentication, through multiple elements, of the user’s identity with the use of industry-recognized standards, then the ONC-ACB verifies the health IT developer’s explanation.

Updated on 03-11-2024

Regulation Text

Regulation Text

§ 170.315 (d)(13) *Multi-factor authentication*.

Health IT developers must make one of the following attestations and, as applicable, provide the specified accompanying information:

1. Yes – the Health IT Module supports the authentication, through multiple elements, of the user’s identity with the use of industry-recognized standards. When attesting “yes,” the health IT developer must describe the use cases supported.
2. No – the Health IT Module does not support authentication, through multiple elements, of the user’s identity with the use of industry-recognized standards. When attesting “no,” the health IT developer may explain why the Health IT Module does not support authentication, through multiple elements, of the user’s identity with the use of industry recognized standards.

Standard(s) Referenced

None

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)(13) *Multi-factor authentication*.

Health IT developers must make one of the following attestations and, as applicable, provide the specified accompanying information:

1. Yes – the Health IT Module supports the authentication, through multiple elements, of the user's identity with the use of industry-recognized standards. When attesting "yes," the health IT developer must describe the use cases supported.
2. No – the Health IT Module does not support authentication, through multiple elements, of the user's identity with the use of industry-recognized standards. When attesting "no," the health IT developer may explain why the Health IT Module does not support authentication, through multiple elements, of the user's identity with the use of industry recognized standards.

Standard(s) Referenced

None

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: Multi-factor authentication

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 to attest “yes” or “no” to whether the Health IT Module supports multi-factor authentication. The criteria places no requirements on health IT customers, such as health care providers, to implement these capabilities (if present in their products) in their healthcare settings.
- Health IT developers attesting “yes” to supporting multi-factor authentication must provide a report outlining the use cases supported 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 must also provide a hyperlink to any required use cases or optional documentation to be published with the product on the ONC Certified Health IT Product List (CHPL).

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 to attest “yes” or “no” to whether the Health IT Module supports multi-factor authentication. The criteria places no requirements on health IT customers, such as health care providers, to implement these capabilities (if present in their products) in their healthcare settings.
- Health IT developers attesting “yes” to supporting multi-factor authentication must provide a report outlining the use cases supported 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 must also provide a hyperlink to any required use cases or optional documentation to be published with the product on the ONC Certified Health IT Product List (CHPL).

Paragraph (i) Attesting "yes"

Clarifications:

- If a health IT developer attests “yes” it must describe the use cases supported. For example, a health IT developer could attest “yes” to supporting multi-factor authentication and provide a summary that the Health IT Module supports multi-factor authentication for remote access by clinical users, thus providing clarity on the user roles to which multi-factor authentication applies for that particular Health IT Module.
- Health IT developers are not expected to provide specific technical details about how they support multi-factor authentication as that information could pose security risks. A succinct, high-level summary that gives an indication of the types of uses supported is adequate.

- If a health IT developer adds a new multi-factor authentication use case it must comply with this criterion’s “yes” attestation provisions and be part of the quarterly CHPL reporting by health IT developers and ONC-ACBs under § 170.523(m).

Clarifications:

- If a health IT developer attests “yes” it must describe the use cases supported. For example, a health IT developer could attest “yes” to supporting multi-factor authentication and provide a summary that the Health IT Module supports multi-factor authentication for remote access by clinical users, thus providing clarity on the user roles to which multi-factor authentication applies for that particular Health IT Module.
- Health IT developers are not expected to provide specific technical details about how they support multi-factor authentication as that information could pose security risks. A succinct, high-level summary that gives an indication of the types of uses supported is adequate.
- If a health IT developer adds a new multi-factor authentication use case it must comply with this criterion’s “yes” attestation provisions and be part of the quarterly CHPL reporting by health IT developers and ONC-ACBs under § 170.523(m).

Paragraph (ii) Attesting "no"

Clarifications:

Health IT developers will be permitted, but not required, to provide a reason for attesting “no,” which may be due to multi-factor authentication being inapplicable or inappropriate. In those cases, a health IT developer could, for example, state that the Health IT Module does not support multi-factor authentication because it is engaged in system-to-system public health reporting and multi-factor authentication is not applicable.

Clarifications:

Health IT developers will be permitted, but not required, to provide a reason for attesting “no,” which may be due to multi-factor authentication being inapplicable or inappropriate. In those cases, a health IT developer could, for example, state that the Health IT Module does not support multi-factor authentication because it is engaged in system-to-system public health reporting and multi-factor authentication is not applicable.

Was this page helpful?

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

Content last reviewed on March 11, 2024