Authentication, access control, authorization | HealthIT.gov

healthit.gov/test-method/authentication-access-control-authorization

§170.315(d)(1) Authentication, access control, authorization

- Certification Companion Guide (CCG)
- Conformance Method

Updated on 03-11-2024

Regulation Text

Regulation Text

§ 170.315 (d)(1) *Authentication, access control, authorization—*

1. Verify against a unique identifier(s) (e.g., username or number) that a user seeking access to electronic health information is the one claimed; and
2. Establish the type of access to electronic health information a user is permitted based on the unique identifier(s) provided in paragraph (d)(1)(i) of this section, and the actions the user is permitted to perform with the technology.

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)(1) *Authentication, access control, authorization—*

1. Verify against a unique identifier(s) (e.g., username or number) that a user seeking access to electronic health information is the one claimed; and
2. Establish the type of access to electronic health information a user is permitted based on the unique identifier(s) provided in paragraph (d)(1)(i) of this section, and the actions the user is permitted to perform with the technology.

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

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)(1) *Authentication, access control, authorization* requirements.	The ONC-ACB verifies the health IT developer attests conformance to the §170.315(d)(1) *Authentication, access control, authorization* requirements.

Archived Version:
§170.315(d)(1) Test Procedure
Updated on 03-11-2024

Regulation Text

Regulation Text

§ 170.315 (d)(1) *Authentication, access control, authorization*—

1. Verify against a unique identifier(s) (e.g., username or number) that a user seeking access to electronic health information is the one claimed; and
2. Establish the type of access to electronic health information a user is permitted based on the unique identifier(s) provided in paragraph (d)(1)(i) of this section, and the actions the user is permitted to perform with the technology.

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)(1) *Authentication, access control, authorization*—

1. Verify against a unique identifier(s) (e.g., username or number) that a user seeking access to electronic health information is the one claimed; and
2. Establish the type of access to electronic health information a user is permitted based on the unique identifier(s) provided in paragraph (d)(1)(i) of this section, and the actions the user is permitted to perform with the technology.

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

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

Certification Companion Guide: Authentication, access control, authorization

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:

- There is no standard required for this certification criterion.
- This criterion focuses on users that would be able to access electronic health information in the technology and not on external users that may make requests for access to health information contained in the technology for the purpose of electronic health information exchange. The latter case could require a different/additional security approach(es). [see also 77 FR 54249]
- While this criterion does not specify a level of assurance, one-factor authentication would be minimally needed to satisfy this criterion. The developer has the discretion to satisfy this criterion above and beyond one-factor authentication. [see also 77 FR 54249]

- A user could be a healthcare professional or office staff, someone who might interact directly with the technology, or be a software program or service. [see also 75 FR 44598]

Clarifications:

- There is no standard required for this certification criterion.
- This criterion focuses on users that would be able to access electronic health information in the technology and not on external users that may make requests for access to health information contained in the technology for the purpose of electronic health information exchange. The latter case could require a different/additional security approach(es). [see also 77 FR 54249]
- While this criterion does not specify a level of assurance, one-factor authentication would be minimally needed to satisfy this criterion. The developer has the discretion to satisfy this criterion above and beyond one-factor authentication. [see also 77 FR 54249]

- A user could be a healthcare professional or office staff, someone who might interact directly with the technology, or be a software program or service. [see also 75 FR 44598]

Paragraph (d)(1)(i) Verify user

Technical outcome – A user’s unique identifier(s) (e.g., username or number) is/are verified as the one claimed prior to receiving access to electronic health information.

Clarifications:

No additional clarifications.

Technical outcome – A user’s unique identifier(s) (e.g., username or number) is/are verified as the one claimed prior to receiving access to electronic health information.

Clarifications:

No additional clarifications.

Paragraph (d)(1)(ii) Establish permissions

Technical outcome – Following the user’s authentication, the technology establishes permissions associated with the user’s ability to access electronic health information and the actions the user is permitted to perform with the technology.

Clarifications:

No additional clarifications.

Technical outcome – Following the user’s authentication, the technology establishes permissions associated with the user’s ability to access electronic health information and the actions the user is permitted to perform with the technology.

Clarifications:

No additional clarifications.

Was this page helpful?

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

Content last reviewed on March 11, 2024