Integrity | HealthIT.gov

§170.315(d)(8) Integrity

- Certification Companion Guide (CCG)
- Conformance Method

Updated on 03-11-2024

Regulation Text

Regulation Text

§ 170.315 (d)(8) *Integrity*—

1. Create a message digest in accordance with the standard specified in § 170.210(c)(2).
2. Verify in accordance with the standard specified in § 170.210(c)(2) upon receipt of electronically exchanged health information that such information has not been altered.

Standard(s) Referenced

Applies to entire criterion

§ 170.210(c)(2) A hashing algorithm with a security strength equal to or greater than SHA-2 as specified by the National Institute of Standards and Technology (NIST) in FIPS Publication 180-4, Secure Hash Standard, 180-4 (August 2015)

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	Final Conformance Method	03-11-2024

Regulation Text

Regulation Text

§ 170.315 (d)(8) *Integrity*—

1. Create a message digest in accordance with the standard specified in § 170.210(c)(2).
2. Verify in accordance with the standard specified in § 170.210(c)(2) upon receipt of electronically exchanged health information that such information has not been altered.

Standard(s) Referenced

Applies to entire criterion

§ 170.210(c)(2) A hashing algorithm with a security strength equal to or greater than SHA-2 as specified by the National Institute of Standards and Technology (NIST) in FIPS Publication 180-4, Secure Hash Standard, 180-4 (August 2015)

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	Final Conformance Method	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)(8) *Integrity* requirements.	The ONC-ACB verifies the health IT developer attests conformance to the §170.315(d)(8) *Integrity* requirements.

Archived Version:
§170.315(d)(8) Test Procedure
Updated on 03-11-2024

Regulation Text

Regulation Text

§ 170.315 (d)(8) *Integrity*—

1. Create a message digest in accordance with the standard specified in § 170.210(c)(2).
2. Verify in accordance with the standard specified in § 170.210(c)(2) upon receipt of electronically exchanged health information that such information has not been altered.

Standard(s) Referenced

Applies to entire criterion

§ 170.210(c)(2) A hashing algorithm with a security strength equal to or greater than SHA-2 as specified by the National Institute of Standards and Technology (NIST) in FIPS Publication 180-4, Secure Hash Standard, 180-4 (August 2015)

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	Final Conformance Method	03-11-2024

Regulation Text
Regulation Text

§ 170.315 (d)(8) *Integrity*—

1. Create a message digest in accordance with the standard specified in § 170.210(c)(2).
2. Verify in accordance with the standard specified in § 170.210(c)(2) upon receipt of electronically exchanged health information that such information has not been altered.

Standard(s) Referenced

Applies to entire criterion

§ 170.210(c)(2) A hashing algorithm with a security strength equal to or greater than SHA-2 as specified by the National Institute of Standards and Technology (NIST) in FIPS Publication 180-4, Secure Hash Standard, 180-4 (August 2015)

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: Integrity

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:

- This criterion is intended to support the HIPAA Security Rule implementation specification provided at 45 CFR 164.312 (e)(2)(i) “[i]implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.” Because this certification criterion specifies a capability that certified health IT must include, ONC does not believe that it is necessary or appropriate to address whether hashing is applicable to public and private networks. [see also 75 FR 44620]
- Certification only ensures that a Health IT Module can create hashes using SHA-2, and it does not require the use of SHA-2. For example, users of certified health IT may find it appropriate to continue to use SHA-1 for backwards compatibility if their security risk analysis justifies the risk. [see also 80 FR 62657]

Clarifications:

- This criterion is intended to support the HIPAA Security Rule implementation specification provided at 45 CFR 164.312 (e)(2)(i) “[i]implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.” Because this certification criterion specifies a capability that certified health IT must include, ONC does not believe that it is necessary or appropriate to address whether hashing is applicable to public and private networks. [see also 75 FR 44620]
- Certification only ensures that a Health IT Module can create hashes using SHA-2, and it does not require the use of SHA-2. For example, users of certified health IT may find it appropriate to continue to use SHA-1 for backwards compatibility if their security risk analysis justifies the risk. [see also 80 FR 62657]

Paragraph (d)(8)(i) Create a message digest

Technical outcome – The Health IT Module can create a message digest using a hashing algorithm with security strength equal or greater than SHA-2.

Clarifications:

A Health IT Module must demonstrate integrity protection controls for data received during an exchange (e.g., by generating a hash upon receipt of a summary record in order to ensure the integrity of the information exchanged).

Technical outcome – The Health IT Module can create a message digest using a hashing algorithm with security strength equal or greater than SHA-2.

Clarifications:

> A Health IT Module must demonstrate integrity protection controls for data received during an exchange (e.g., by generating a hash upon receipt of a summary record in order to ensure the integrity of the information exchanged).

Paragraph (d)(8)(ii) Enable a user to verify upon receipt

Technical outcome – The Health IT Module must be able to verify, in accordance with a hashing algorithm with security strength equal or greater than SHA-2, that information has not been altered or changed in any way.

Clarifications:

> A Health IT Module does not need to differentiate between internal and external transmissions as the capability's subsequent use (post-certification) is at the discretion of the implementation setting's policies. [77 FR 54251]

Technical outcome – The Health IT Module must be able to verify, in accordance with a hashing algorithm with security strength equal or greater than SHA-2, that information has not been altered or changed in any way.

Clarifications:

> A Health IT Module does not need to differentiate between internal and external transmissions as the capability's subsequent use (post-certification) is at the discretion of the implementation setting's policies. [77 FR 54251]

Was this page helpful?

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

Content last reviewed on June 4, 2024