

§170.315(d)(8) Integrity

2015 Edition CCGs

Version 1.1 Updated on 04-20-2016

Revision History

Version #	Description of Change	Version Date
1.0	Initial Publication	10-22-2015
1.1	Clarification added regarding hashing algorithm options.	04-20-2016

Regulation Text

Regulation Text

§170.315 (d)(8) *Integrity*—

- (i) Create a message digest in accordance with the standard specified in §170.210(c)(2).
- (ii) 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 NIST in [FIPS Publication 180-4, Secure Hash Standard, 180-4 \(August 2015\)](#)

Certification Companion Guide: Integrity

This Certification Companion Guide (CCG) is an informative document designed to assist with health IT product development. The CCG is not a substitute for the 2015 Edition final regulation. It extracts key portions of the rule's preamble and includes subsequent clarifying interpretations. To access the full context of regulatory intent please consult the 2015 Edition final rule or other included regulatory reference. The CCG is for public use and should not be sold or redistributed.

[Link to Final Rule Preamble](#)

[Link to Correction Notice Preamble](#)

Edition Comparison	Gap Certification Eligible	Base EHR Definition	In Scope for CEHRT Definition
Revised	No	Not Included	No

Certification Requirements

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.

- 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.
- 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.

Table for Design and Performance

- [Quality management system \(§ 170.315\(g\)\(4\)\)](#)
- [Accessibility-centered design \(§ 170.315\(g\)\(5\)\)](#)

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]mplement 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, we do not believe that it is necessary or appropriate for us 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)

Technical outcome – The health IT 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)

Technical outcome – The health IT 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](#)]

Content last reviewed on September 21, 2018