

2015 Edition Certification Companion Guide

Integrity - 45 CFR 170.315(d)(8)

[Final Rule Preamble](#) – [Test Procedure](#)

Version 1.1 – Last Updated 4/20/2016

New/Revised/Unchanged Compared to 2014 Edition	Gap Certification Eligible	Base EHR Definition	Certified EHR Technology Definition	Associated EHR Incentive Program Objective(s)
Revised	No	No	Not included	N/A

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.

Regulation Text

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.

Criterion Subparagraph	Technical Explanations and Clarifications	Standard(s) Referenced
Applies to entire criterion	<p>Clarifications:</p> <ul style="list-style-type: none"> • 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] 	§ 170.210(c)(2). A hashing algorithm with a security strength equal to or greater than SHA-2 as specified by NIST in FIPS PUB 180-4, Secure Hash Standard, 180-4 (August 2015) ;

Continued on next page

Criterion Subparagraph	Technical Explanations and Clarifications	Standard(s) Referenced
Applies to entire criterion, continued	<ul style="list-style-type: none"> • Certification only ensures that a Health IT Module can create hashes using SHA-2, and it does not require the <u>use</u> 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] 	See previous page
(i)	<ul style="list-style-type: none"> • Technical outcome – The health IT can create a message digest using a hashing algorithm with security strength equal or greater than SHA-2. <p>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).</p>	See above reference to SHA-2.
(ii)	<ul style="list-style-type: none"> • 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. <p>Clarifications:</p> <ul style="list-style-type: none"> • 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) 	See above reference to SHA-2.

Note: 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.

Version History

Version #	Change(s) Summary	Date Made
1.0	Initial Publication	Oct 22, 2015
1.1	Clarification added regarding hashing algorithm options	April 20, 2016,