

2015 Edition Certification Companion Guide

Application Access – Patient Selection - 45 CFR 170.315(g)(7)

Links will be updated as available: [Final Rule Preamble](#) – [Test Procedure](#) – [MU Specification Sheet](#)

Version 1.2 – Last Updated 11/09/2016

New/Revised/Unchanged Compared to 2014 Edition	Gap Certification Eligible	Base EHR Definition	Certified EHR Technology Definition	Associated EHR Incentive Program Objective(s)
New	No	Yes	Included	Objective 5 Objective 6

Certification Requirements

Privacy and Security: This certification criterion was adopted at § 170.315(g)(7). As a result, an ONC-ACB must ensure that a product presented for certification to this criterion includes the privacy and security criteria (adopted in § 170.315(d)) within the overall scope of the certificate issued to the product.

- The privacy and security criteria (adopted in § 170.315(d)) do not need to be explicitly tested with this specific criterion unless it is the only criterion for which certification is requested.
- As a general rule, a product presented for certification only needs to be tested once to each applicable privacy and security criterion (adopted in § 170.315(d)) so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification. However, exceptions exist for § 170.315(e)(1) “VDT” and (e)(2) “secure messaging,” which are explicitly stated.

Design and Performance: The following design and performance certification criteria (adopted in § 170.315(g)) must also be certified in order for the product to be certified.

- 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.

Privacy and Security (§ 170.315(d))	Design and Performance (§ 170.315(g))
<ul style="list-style-type: none"> • If choosing Approach 1: <ul style="list-style-type: none"> ○ Authentication, access control, and authorization (§ 170.315(d)(1)) ○ Trusted connection (§ 170.315(d)(9)) ○ Either auditable events and tamper-resistance (§ 170.315(d)(2)) or auditing actions on health information (§ 170.315(d)(10)). • If choosing Approach 2: <ul style="list-style-type: none"> ○ For each applicable P&S certification criterion not certified for approach 1, the health IT developer may certify for the criterion using system documentation which provides a clear description of how the external services necessary to meet the P&S criteria would be deployed and used. 	<ul style="list-style-type: none"> • Quality management system (§ 170.315(g)(4)) • Accessibility-centered design (§ 170.315(g)(5))

Regulation Text

Application access - patient selection. The following technical outcome and conditions must be met through the demonstration of an application programming interface (API).

(i) Functional requirement. The technology must be able to receive a request with sufficient information to uniquely identify a patient and return an ID or other token that can be used by an application to subsequently execute requests for that patient's data.

(ii) Documentation.

(A) The API must include accompanying documentation that contains, at a minimum:

(1) API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.

(2) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).

(3) Terms of use. The terms of use for the API must be provided, including, at a minimum, any associated developer policies and required developer agreements.

(B) The documentation used to meet paragraph (g)(7)(ii)(A) of this section must be available via a publicly accessible hyperlink.

Criterion Subparagraph	Technical Explanations and Clarifications	Standard(s) Referenced
Applies to entire criterion	<p>Clarifications:</p> <ul style="list-style-type: none"> • While no standard is required for this criterion, we intend to adopt a standards-based approach for certification in a future rulemaking. We encourage the use of the Fast Healthcare Interoperability Resources (FHIR) specification. • Security: <ul style="list-style-type: none"> ○ Our intention is to encourage dynamic registration (e.g., OAuth 2.0 Connect Dynamic Client Registration Protocol) and strongly believe that registration should not be used as a means to block information sharing via APIs. That is, applications should not be required to pre-register (or be approved in advance) with the provider or their Health IT Module developer before being allowed to access the API. Under the 2015 Edition privacy and security (P&S) certification framework, health IT certified to the API criteria must support an application connecting to the API. The P&S certification framework for the API criteria requires that a Health IT Module certified to this criterion be capable of ensuring that: valid user credentials such as a username and password are presented (that match the credentials on file at the provider for that user); the provider can authorize the user to view the patient’s data; the application connects through a trusted connection; and the access is audited (§ 170.515(d)(1); (d)(9); and (d)(2) or (d)(10); respectively). These certification requirements should be sufficient to allow access without requiring further application pre-registration. [see also 80 FR 62676] This criterion does not currently include any security requirements beyond the privacy and security approach detailed above, but we encourage organizations to follow security best practices and implement security controls, such as penetration testing, encryption, audits, and monitoring as appropriate. We expect health IT developers to include information on how to securely use their APIs in the public documentation required by the certification criteria and follow industry best practices. [see also 80 FR 62676] ○ We strongly encourage developers to build security into their APIs following best practice guidance, such as the Department of Homeland Security’s Build Security In initiative.¹ [see also 80 FR 62677] <p style="text-align: right;"><i>Continued on next page</i></p>	N/A

¹ <https://buildsecurityin.us-cert.gov/>

Criterion Subparagraph	Technical Explanations and Clarifications	Standard(s) Referenced
Applies to entire criterion, <i>continued</i>	<p>Clarifications, continued</p> <ul style="list-style-type: none"> ○ APIs could be used when consent or authorization by an individual is required. In circumstances where there is a requirement to document a patient’s request or particular preferences, APIs can enable compliance with documentation requirements. The HIPAA Privacy Rule² permits the use of electronic documents to qualify as writings for the purpose of proving signature, e.g., electronic signatures. [see also 80 FR 62677] ● By requiring that documentation and terms of use be open and transparent to the public by requiring a hyperlink to such documentation to be published with the product on the ONC Certified Health IT Product List, we hope to encourage an open ecosystem of diverse and innovative applications that can successfully and easily interact with different Health IT Modules’ APIs. [see also 80 FR 62679] ● A health IT developer must demonstrate that its API functionality properly performs consistent with this certification criterion’s requirements. How this is done is up to the health IT developer. Doing so could include, but is not limited to, the health IT developer using existing tools or creating its own app or “client” to interact with the API as well as using a third-party application. ● Health IT developers are able to update/upgrade/improve functionality that’s within the scope of certification, provided that certain rules and conditions are followed. The “API criteria” § 170.315(g)(7), § 170.315(g)(8), and § 170.315(g)(9) are treated no different under this regulatory structure. If a developer seeks to update their API functionality post-certification a developer will need to consider the following: <ul style="list-style-type: none"> ○ If their ONC-ACB requires notification or updated documentation associated with the functionality they changed. This procedure is at the discretion of the ONC-ACB and may result in an additional CHPL listing. ○ Pursuant to the certification criteria, there is a documentation portion in each. Which would include (publicly available) technical specs, configuration requirements, and terms of use. Insofar as a developer updates their API post-certification, they are expected to keep all of this documentation up-to-date. Similarly, ONC-ACBs are expected to oversee/enforce/surveil that this action is taken and could find a non-conformity if those updates are not made. ○ If any of their changes would require updates to the developer’s 170.523(k)(1) disclosures (the broader product transparency disclosures). 	N/A

² 45 CFR Part 160 and Part 164, Subparts A and E

Criterion Subparagraph	Technical Explanations and Clarifications	Standard(s) Referenced
(i)	<ul style="list-style-type: none"> Technical outcome – The health IT can receive a request with sufficient information to uniquely identify a patient and return an ID or other token that can be used by an application to subsequently execute requests for that patient’s data. <p>Clarifications:</p> <ul style="list-style-type: none"> The developer can determine the method and the amount of data by which the health IT uniquely identifies a patient. [see also 80 FR 62678] The term “token” is not to be interpreted as the token in the OAuth2 workflow, but simply as an identifier for something that would uniquely identify a patient. 	N/A
(ii)(A)(1)	<ul style="list-style-type: none"> Technical outcome – The API must include accompanying documentation, which contains API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions, and exception handling methods and their returns. <p>Clarifications:</p> <ul style="list-style-type: none"> No additional clarifications available. 	N/A
(ii)(A)(2)	<ul style="list-style-type: none"> Technical outcome – The API must include accompanying documentation, which contains software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s). <p>Clarifications:</p> <ul style="list-style-type: none"> No additional clarifications available. 	N/A

Criterion Subparagraph	Technical Explanations and Clarifications	Standard(s) Referenced
(ii)(A)(3)	<ul style="list-style-type: none"> • Technical outcome – The API must include the terms of use for the API including, at a minimum, any associated developer policies and required developer agreements. <p>Clarifications:</p> <ul style="list-style-type: none"> • Health IT developers must be clear and transparent about the general terms of agreements or contracts that will typically apply to all prospective third-party applications. • Health IT developers that typically execute unique agreements or contracts with interested third-party applications using their API must disclose this practice as part of their terms of use. • For the purposes of certification, a health IT developer is accountable for the items within its API’s terms of use that are within its control to set. If, post-certification, a health IT developer permits its customers to deploy and integrate its API in ways where the customer would be able to layer on its own specific terms of use unique to that organization, the health IT developer would need to disclose this business practice in its terms of use. However, for the purposes of certification, a health IT developer is NOT expected to change or factor instances into its terms of use where its customers establish additional, organizational-specific terms for the API’s use. 	N/A
(ii)(B)	<ul style="list-style-type: none"> • Technical outcome – The documentation used to meet the provisions in (ii)(A)(1)-(3) must be available through a publicly accessible hyperlink. <p>Clarifications:</p> <ul style="list-style-type: none"> • The hyperlink provided for the terms of use must reflect the most current version of the Health IT developer’s terms of use. 	N/A

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 26, 2015
1.1	Header information updated Revisions made to remove Designated Record Set and HIPAA Security rule references Third-party API development clarification added Terms of use documentation and hyperlink clarifications added	Mar 22, 2016
1.2	Added clarification in the applies to entire criterion section related to the product update requirements.	Nov 09, 2016