Official Website of The Office of the National Coordinator for Health Information Technology (ONC)

HealthIT.gov

§170.315(g)(9) Application access – all data request

2015 Edition CCGs

Updated on 07-12-2021

Revision History

Version #	Description of Change	Version Date
1.0	Initial Publication	10-30-2015
1.1	Certification requirement revised to include that C-CDA creation performance (§ 170.315(g)(6)) is required for this criterion. Clarifications added relating to "third-party API" definition, additional audit record user access details, data exclusions related to patient data accessed within a specific date range, terms of use details related to third party applications, API access, and hyperlink, and details around the meaning of token as a patient identifier.	02-05-2016
1.2	Further adjustments to clarifications included with version 1.1 were made and to also be consistent with clarifications included in the CCGs for (g)(7) and (g)(8) certification criteria. Terms of use documentation and hyperlink clarifications added. HIPAA specific bullet removed from general clarifications section to avoid confusion.	03-28-2016
1.3	Added clarification in the "applies to entire criterion section" related	11-09-2016

	to the product update requirements.	
1.4	Added clarification regarding the number of CCD documents that may be returned for a specific date range. Added clarification on API Registration requirements and removed guidance on API registration mechanism (dynamic registration). Added clarification on the definition of a “trusted connection”. Clarification added to subparagraph (i)(B) on the method used to identify a patient.	07-07-2017
1.5	Added clarification for paragraph (g)(9)(ii)(B) that documentation must be available to the public via a hyperlink without any additional access requirements.	08-25-2017
1.6	Revised clarification for paragraph (g)(9)(ii)(B) that the hyperlink provided for all of the documentation must reflect the most recent version of all the documentation, not just the terms of use. Provided notification of March 2017 Validator Update of C-CDA 2.1 Corrections adoption and compliance requirements for paragraph (g)(9)(i)(A).	09-29-2017
1.7	Made revisions to a prior clarification in paragraph (g)(9)(ii)(A) regarding the terms of use. Added a new clarification for paragraph (g)(9)(ii)(A) regarding enforcement of the health IT developer’s terms of use, which is out of scope for this criterion. Additionally, noted CMS guidance that providers may not prohibit patients from using the app of the patient’s choice.	02-01-2018
1.8	Provides notification of April 2018 Validator Update of C-CDA 2.1 Corrections adoption and compliance requirements within paragraph (g)(9)(i)(A). Note: Due to an error in calculation ONC is also updating the dates for compliance with the March 2017 Validator	05-02-2018

	Update of C-CDA 2.1 Corrections that were adopted September 29, 2017.	
1.9	Provides notification of August 2018 Validator Update of C-CDA 2.1 Corrections adoption and compliance requirements within paragraph (g)(9)(i)(A).	09-21-2018
2.0	Updated the Security requirements per 21st Century Cures Act. Updated the data element requirements per 21st Century Cures Act (use of USCDI rather than CCDS). Removed Terms of Use (ii)(A)(3).	06-15-2020
2.1	Removed footnotes and included the links/references in line with the clarifications.	07-12-2021

Regulation Text

Regulation Text

§ 170.315 (g)(9) *Application access – all data request—*

The following technical outcome and conditions must be met through the demonstration of an application programming interface.

(i) *Functional requirements.*

(A) Respond to requests for patient data (based on an ID or other token) for all of the data categories specified in the Common Clinical Data Set at one time and return such data (according to the specified standards, where applicable) in a summary record formatted according to the standard specified in § 170.205(a)(4) following the CCD document template.

(B) Respond to requests for patient data associated with a specific date as well as requests for patient data within a specified date range.

(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)(9)(ii)(A) of this section must be available via a publicly accessible hyperlink.

Standard(s) Referenced

Paragraph (g)(9)(i)(A)

§ 170.205(a)(4) Health Level 7 (HL7®) Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use Release 2.1, August 2015

Please refer to the Data Elements and Vocabularies applicable to the Common Clinical Data Set (CCDS) as outlined in the CCDS Reference Document.

Resource Documents

Resource Document

- Privacy and Security Certification Companion Guide [PDF - 281 KB]
- 2015 Edition Network Time Protocol (NTP) [PDF - 157 KB]
- CHPL SED Guide [PDF - 690 KB]
- Master Table of Related and Required Criteria [PDF-251 KB]
- CCDS Reference [PDF - 655 KB]
- CCDS Guide [PDF - 349 KB]

Revision History

Version #	Description of Change	Version Date
1.0	Initial Publication	10-30-2015
1.1	Certification requirement revised to include that C-CDA creation performance (§ 170.315(g)(6)) is required for this criterion. Clarifications added relating to "third-party API" definition, additional audit record user access details, data exclusions related to patient data accessed within a specific date range, terms of use details related to third party applications, API access, and hyperlink, and details around the meaning of token as a patient identifier.	02-05-2016
1.2	Further adjustments to clarifications included with version 1.1 were made and to also be consistent with clarifications included in the CCGs for (g)(7) and (g)(8) certification criteria. Terms of use documentation and hyperlink clarifications added. HIPAA specific bullet removed from general clarifications section to avoid confusion.	03-28-2016

1.3	Added clarification in the "applies to entire criterion section" related to the product update requirements.	11-09-2016
1.4	Added clarification regarding the number of CCD documents that may be returned for a specific date range. Added clarification on API Registration requirements and removed guidance on API registration mechanism (dynamic registration). Added clarification on the definition of a "trusted connection". Clarification added to subparagraph (i)(B) on the method used to identify a patient.	07-07-2017
1.5	Added clarification for paragraph (g)(9)(ii)(B) that documentation must be available to the public via a hyperlink without any additional access requirements.	08-25-2017
1.6	Revised clarification for paragraph (g)(9)(ii)(B) that the hyperlink provided for all of the documentation must reflect the most recent version of all the documentation, not just the terms of use. Provided notification of March 2017 Validator Update of C-CDA 2.1 Corrections adoption and compliance requirements for paragraph (g)(9)(i)(A).	09-29-2017
1.7	Made revisions to a prior clarification in paragraph (g)(9)(ii)(A) regarding the terms of use. Added a new clarification for paragraph (g)(9)(ii)(A) regarding enforcement of the health IT developer's terms of use, which is out of scope for this criterion. Additionally, noted CMS guidance that providers may not prohibit patients from using the app of the patient's choice.	02-01-2018
1.8	Provides notification of April 2018 Validator Update of C-CDA 2.1 Corrections adoption and	05-02-2018

	compliance requirements within paragraph (g)(9)(i)(A). Note: Due to an error in calculation ONC is also updating the dates for compliance with the March 2017 Validator Update of C-CDA 2.1 Corrections that were adopted September 29, 2017.	
1.9	Provides notification of August 2018 Validator Update of C-CDA 2.1 Corrections adoption and compliance requirements within paragraph (g)(9)(i)(A).	09-21-2018
2.0	Updated the Security requirements per 21st Century Cures Act. Updated the data element requirements per 21st Century Cures Act (use of USCDI rather than CCDS). Removed Terms of Use (ii)(A)(3).	06-15-2020
2.1	Removed footnotes and included the links/references in line with the clarifications.	07-12-2021

Regulation Text

Regulation Text

§ 170.315 (g)(9) *Application access – all data request—*

The following technical outcome and conditions must be met through the demonstration of an application programming interface.

(i) *Functional requirements.*

(A) Respond to requests for patient data (based on an ID or other token) for all of the data categories specified in the Common Clinical Data Set at one time and return such data (according to the specified standards, where applicable) in a summary record formatted according to the standard specified in § 170.205(a)(4) following the CCD document template.

(B) Respond to requests for patient data associated with a specific date as well as requests for patient data within a specified date range.

(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)(9)(ii)(A) of this section must be available via a publicly accessible hyperlink.

Standard(s) Referenced

Paragraph (g)(9)(i)(A)

§ 170.205(a)(4) Health Level 7 (HL7®) Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use Release 2.1, August 2015

Please refer to the Data Elements and Vocabularies applicable to the Common Clinical Data Set (CCDS) as outlined in the CCDS Reference Document.

Testing

Testing Tool

Edge Testing Tool (ETT): Message Validators

Test Tool Documentation

Test Tool Supplemental Guide

Certification Companion Guide: Application access – all data request

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

Edition Comparision	Gap Certification Eligible	Base EHR Definition	In Scope for CEHRT Definition
New	No	Included	Yes

Certification Requirements

Privacy and Security: This certification criterion was adopted at § 170.315(g)(9). As a result, an ONC Authorized Certification Body (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) “View, download, and transmit to 3rd party (VDT)” and (e)(2) “Secure messaging,” which are explicitly stated.
- § 170.315(d)(2)(i)(C) is not required if the scope of the Health IT Module does not have end-user device encryption features.

Table for Privacy and Security

- If choosing Approach 1:
  - 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)).
  - Encrypt Authentication Credentials (§ 170.315(d)(12))
  - Multi-factor Authentication (MFA) (§ 170.315(d)(13))
- If choosing Approach 2:
  - For each applicable privacy and security certification criterion not certified using Approach 1, the health IT developer may certify using system documentation which is sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces to access external services necessary to meet the requirements of the privacy and security certification criterion. Please see the ONC Cures Act Final Rule at 85 FR 25710 for additional clarification.

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.
- Consolidated Clinical Document Architecture (C-CDA) creation performance (§ 170.315(g)(6)) does not need to be explicitly tested with this criterion unless it is the only criterion within the scope of the requested certification that includes C-CDA creation capabilities. Note that the application of § 170.315(g)(6) depends on the C-CDA templates explicitly required by the C-CDA-referenced criterion or criteria included within the scope of the certificate sought. Please refer to the C-CDA Creation Performance CCG for more details.

Table for Design and Performance

- Quality management system (§ 170.315(g)(4))
- Accessibility-centered design (§ 170.315(g)(5))
- Consolidated CDA creation performance (§ 170.315(g)(6))

Technical Explanations and Clarifications

Applies to entire criterion

Clarifications:

- *Security:*
  - For the purposes of certification there is no conformance requirement related to the registration of third-party applications that use application programming interfaces (APIs). If a Health IT Module requires registration as a pre-condition for accessing the APIs, then, the process must be clearly specified in the API documentation as

  - required by the criterion. ONC strongly believes that registration should not be used as a means to block information sharing via APIs.
  - This criterion does not currently include any security requirements beyond the privacy and security approach detailed above, but ONC encourages organizations to follow security best practices and implement security controls, such as penetration testing, encryption, audits, and monitoring as appropriate. ONC expects 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]
  - ONC strongly encourages developers to build security into their APIs following industry best practices. [see also 80 FR 62677]
  - A “trusted connection” means the link is encrypted/integrity protected according to § 170.210(a)(2) or (c)(2). As such, ONC does not believe it is necessary to specifically name HTTPS and/or SSL/TLS as this standard already covers encryption and integrity protection for data in motion. [see also 80 FR 62676]
  - 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 Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (45 CFR Part 160 and Part 164, Subparts A and E) 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]
- The audit record should be able to distinguish the specific user who accessed the data using a third-party application through the certified API in order to meet the requirements of § 170.315(d)(2) <u>or</u> (d)(10).
- 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.
- 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 (CHPL), ONC hopes 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]
- 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)(9) and § 170.315(g)(10) 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:
-   - 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 specifications and configuration requirements. 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)

Paragraph (g)(9)(i)(A)

Technical outcome – The API must be able to respond to requests for patient data (using an ID or other token) for <u>all</u> of the data categories specified in the USCDI at one time in a summary record formatted according to the C-CDA Release 2.1 CCD template.

Clarifications:

- Please refer to the 2015 Edition USCDI for the data standards that are required.
- The technology specifications should be designed and implemented in such a way as to return meaningful responses to queries, particularly with regard to exceptions and exception handling, and should make it easy for applications to discover what data exists for the patient. [see also 80 FR 62678]

- The term “token” that is used here is not to be interpreted as the token in the OAuth2 workflow, but simply as something that would uniquely identify a patient.
- In order to mitigate potential interoperability errors and inconsistent implementation of the HL7® Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes, Draft Standard for Trial Use, Release 2.1, ONC assesses, approves, and incorporates corrections as part of required testing and certification to this criterion. [see Health IT Certification Program Overview] Certified health IT adoption and compliance with the following corrections are necessary because they implement updates to vocabularies, update rules for cardinality and conformance statements, and promote proper exchange of C-CDA documents. There is a 90-day delay from the time the CCG has been updated with the ONC-approved corrections to when compliance with the corrections will be required to pass testing (i.e., C-CDA 2.1 Validator). Similarly, there will be an 18-month delay before a finding of a correction’s absence in certified health IT during surveillance would constitute a non-conformity under the Certification Program.
  - March 2017 Validator Update of C-CDA 2.1 Corrections [Effective for testing on December 28, 2017; Surveillance compliance date is March 29, 2019]
  - April 2018 Validator Update of C-CDA 2.1 Corrections [Effective for testing on July 31, 2018; Surveillance compliance date is November 2, 2019]
  - August 2018 Validator Update of C-CDA 2.1 Corrections [Effective for testing on December 20, 2018; Surveillance compliance date is March 21, 2020]

Paragraph (g)(9)(i)(B)

Technical outcome – The API must be able to respond to requests for patient data associated with a specific date as well as with a specific date range.

Clarifications:

- Health IT returning an entire patient record that does not reflect the specific date or date range requested is not permissible when a specific date or date range is requested. [see also 80 FR 62678]
- 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 API must be able to send, at minimum all required data for a specified date range(s). ONC acknowledges that there will be organizational policies and/or safety best practices that will dictate additional data to be sent and when data is considered complete and/or ready for being sent. This should be appropriately described in the API documentation.
- The approach used to provide the CCD document(s) is set by the API. An approach based on providing one or more CCD documents matching to the patient’s selected date or date range is a valid approach.

Paragraph (g)(9)(ii)(A)

Technical outcome – The API must include accompanying documentation which contains at a minimum:

- 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.
- 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)
- The terms of use for the API including, at a minimum, any associated developer policies and required developer agreements.

Clarifications:

- No additional clarifications.

Paragraph (g)(9)(ii)(B)

Technical outcome – The documentation used to meet the provisions in (g)(9)(ii)(A)(*1*)-(*3*) must be available through a publicly accessible hyperlink.

Clarifications:

- The hyperlink provided for all of the documentation referenced by provision (g)(9)(ii)(A) must reflect the most current version of the Health IT developer's documentation.
- All of the documentation referenced by provision (g)(9)(ii)(A) must be accessible to the public via a hyperlink without additional access requirements, including, without limitation, any form of registration, account creation, "click-through" agreements, or requirement to provide contact details or other information prior to accessing the documentation.

Content last reviewed on March 9, 2023