Application access — patient selection

healthit.gov/test-method/application-access-patient-selection

Updated on 03-11-2024

Regulation Text

Regulation Text

§ 170.315 (g)(7) *Application access – patient selection—*

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

1. *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.
2. *Documentation—*
    1. 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).
    2. The documentation used to meet paragraph (g)(7)(ii)(A) of this section must be available via a publicly accessible hyperlink.

Standard(s) Referenced

None

Certification Dependencies

Conditions and Maintenance of Certification

Real World Testing:Products certified to this criterion must complete requirements outlined for the Real World Testing Conditions and Maintenance of Certification.

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.

- 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.

Privacy & Security Requirements

This certification criterion was adopted at § 170.315(g)(7). 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 presented 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.

For more information on the approaches to meet these Privacy and Security requirements, please review the Privacy and Security CCG.

- 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.

Revision History

Version #	Description of Change	Version Date
1.0	Initial publication	03-11-2024

Regulation Text

Regulation Text

§ 170.315 (g)(7) *Application access – patient selection*—

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

1. *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.
2. *Documentation*—
   1. 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).
   2. The documentation used to meet paragraph (g)(7)(ii)(A) of this section must be available via a publicly accessible hyperlink.

Standard(s) Referenced

None

Certification Dependencies

Conditions and Maintenance of Certification

Real World Testing:Products certified to this criterion must complete requirements outlined for the Real World Testing Conditions and Maintenance of Certification.

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.

- 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.

Privacy & Security Requirements

This certification criterion was adopted at § 170.315(g)(7). 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 presented 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.

For more information on the approaches to meet these Privacy and Security requirements, please review the Privacy and Security CCG.

- 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.

Revision History

Version #	Description of Change	Version Date
1.0	Initial publication	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	Test Lab Verification
The health IT developer will attest directly to the ONC-ACB to conformance with the § 170.315 (g)(7) *Application access — patient selection* requirements..	The ONC-ACB verifies the health IT developer attests conformance to the § 170.315 (g)(7) *Application access — patient selection* requirements.

Archived Version:
§170.315(g)(7) Test Procedure
Updated on 03-11-2024

Regulation Text

Regulation Text

§ 170.315 (g)(7) *Application access – patient selection—*

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

1. *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.
2. *Documentation*—
    1. 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).
    2. The documentation used to meet paragraph (g)(7)(ii)(A) of this section must be available via a publicly accessible hyperlink.

Standard(s) Referenced

None

Certification Dependencies

Conditions and Maintenance of Certification

Real World Testing:Products certified to this criterion must complete requirements outlined for the Real World Testing Conditions and Maintenance of Certification.

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.

- 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.

Privacy & Security Requirements

This certification criterion was adopted at § 170.315(g)(7). 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 presented 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.

For more information on the approaches to meet these Privacy and Security requirements, please review the Privacy and Security CCG.

- 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.

Revision History

Version #	Description of Change	Version Date
1.0	Initial publication	03-11-2024

Regulation Text

Regulation Text

§ 170.315 (g)(7) *Application access – patient selection—*

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

1. *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.
2. *Documentation—*
    1. 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).
    2. The documentation used to meet paragraph (g)(7)(ii)(A) of this section must be available via a publicly accessible hyperlink.

Standard(s) Referenced
None

Certification Dependencies
Conditions and Maintenance of Certification

Real World Testing:Products certified to this criterion must complete requirements outlined for the Real World Testing Conditions and Maintenance of Certification.

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.

- 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.

Privacy & Security Requirements
This certification criterion was adopted at § 170.315(g)(7). 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 presented 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.

For more information on the approaches to meet these Privacy and Security requirements, please review the Privacy and Security CCG.

- 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.

Revision History

Version #	Description of Change	Version Date
1.0	Initial publication	03-11-2024

Certification Companion Guide: Application access — patient selection

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**
Included	Yes	No	No	No

Certification Requirements

Technical Explanations and Clarifications

Applies to entire criterion

Clarifications:

- 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:*
    - For the purposes of certification there is no conformance requirement related to the registration of third party applications that use the 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. [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. 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 6267]
    - 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 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]
- 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]
- 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)(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, 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).

Clarifications:

- 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:*
    - For the purposes of certification there is no conformance requirement related to the registration of third party applications that use the 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. [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. 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 6267]
    - 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 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]
- 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]
- 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)(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, 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).

Paragraph (g)(7)(i) Functional requirement

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.

Clarifications:

- 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.

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.

Clarifications:

- 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.

Paragraph (g)(7)(ii)(A)(*1*) Documentation

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.

Clarifications:

No additional clarifications.

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.

Clarifications:

No additional clarifications.

Paragraph (g)(7)(ii)(A)(*2*) API

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).

Clarifications:

No additional clarifications.

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).

Clarifications:

No additional clarifications.

Paragraph (g)(7)(ii)(B) Public accessibility

Technical outcome – The documentation used to meet the provisions in (g)(7)(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)(7)(ii)(A) must reflect the most current version of the Health IT developer’s documentation.
- All of the documentation referenced by provision (g)(7)(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.

Technical outcome – The documentation used to meet the provisions in (g)(7)(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)(7)(ii)(A) must reflect the most current version of the Health IT developer’s documentation.
- All of the documentation referenced by provision (g)(7)(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.