



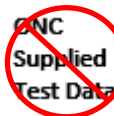


§170.315(g)(11) Consent management for APIs				
Testing Components:				
				
NPRM Draft				

Please consult the Notice of Proposed Rulemaking (NPRM) entitled: *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program* for a detailed description of the certification criterion with which these testing steps are associated.

Revision History

Version #	Description of Change	Version Date
1.0	NPRM Draft	04-05-2019

Regulation Text

§170.315 (g)(11) *Consent management for APIs*—

- (i) Respond to requests for data in accordance with:
 - (A) The standard adopted in § 170.215(c)(1); and
 - (B) The implementation specification adopted in § 170.215(c)(2).
- (ii) *Documentation*.
 - (A) The API(s) must include complete accompanying documentation that contains, at a minimum:
 - (1) API syntax, function names, required and optional parameters supported 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) All applicable technical requirements and attributes necessary for an application to be registered with an authorization server.
 - (B) The documentation used to meet paragraph (g)(11)(ii)(A) of this section must be available via a publicly accessible hyperlink.

Standard(s) Referenced

Paragraph (g)(11)(i)(A)

§ 170.215(c)(1) [Fast Healthcare Interoperability Resources \(FHIR\) Release 3 Standard for Trial Use \(STU\) \(v3.0.1\)](#)

Paragraph (g)(11)(i)(B)

§ 170.215(c)(2) [Consent2Share FHIR Consent Profile Design](#)

Required Tests

Paragraph (g)(11)(i)(B)

System Under Test	Test Lab Verification
<p><u>Consent FHIR Resource Requirements</u></p> <ol style="list-style-type: none"> The health IT developer supplies documentation on the storage mechanism used to store any references to patients, providers, and organizations with a consent statement in accordance with the implementation specification specified at § 170.215(c)(2) Health Level 7 (HL7®) Implementation Specification – FHIR Profile: Consent2Share FHIR Consent Profile Design. <p><u>Consent Data Requirements</u></p> <ol style="list-style-type: none"> The health IT developer supplies documentation value sets related to the management of the consent statement in accordance with the implementation specification specified at § 170.215(c)(2). The health IT developer supplies documentation on how consent policies are governed and how policy rules are executed. The user demonstrates the ability of the Health IT Module to create a consent statement with the information in accordance with the implementation specification specified at § 170.215(c)(2) and, at a 	<p><u>Consent FHIR Resource Requirements</u></p> <ol style="list-style-type: none"> The tester verifies that the Health IT Module stores all references to patients, providers, and organizations used in the consent is on the local server in accordance with the implementation specification at § 170.215(c)(2), which includes the definition of the: <ul style="list-style-type: none"> ○ Patient (as patient and/or consenting party); ○ RelatedPerson (as consenting party); ○ Practitioner (custodians, information recipients); and ○ Organization (custodian, custodians, information recipients). <p><u>Consent Data Requirements</u></p> <ol style="list-style-type: none"> The tester verifies the documentation for the value sets to manage the consent statement is complete and without omission, including, at a minimum, the value sets specified in the requirements at § 170.215(c)(2): <ul style="list-style-type: none"> ○ ConsentExceptType – deny/permit; and ○ ConsentState – proposed/active/rejected/inactive/entered-in-

System Under Test	Test Lab Verification
<p>minimum, including:</p> <ul style="list-style-type: none"> ○ <i>Identifier</i> - unique identifier for the consent statement; ○ <i>Status</i> - indicator of the current consent statement status; ○ <i>Patient</i> – reference to whom the consent statement concerns; ○ <i>Period</i> - <i>relevant</i> time period for the consent statement; ○ <i>Date/Time</i> - <i>Date</i> the consent was signed and made active; ○ <i>Consenting Party</i> reference entity signing the consent; ○ <i>Consent Actor(s)</i>- entities used to specify the custodian(s) and information recipient(s); ○ <i>Organization</i> – references the entity that manages the consents; ○ <i>Purpose</i> – coded value indication the consent purpose; and ○ <i>Exception</i> – list of protected information if the consent differs from the base policy. <p><u>Consent Statement Use Cases</u></p> <ol style="list-style-type: none"> 5. The user demonstrates the ability of the Health IT Module to create a consent statement for the following use case in accordance with the implementation specification at § 170.215(c)(2): <ul style="list-style-type: none"> ○ Use Case 1: Create an active, signed Consent Statement. 6. The user demonstrates the ability of the Health IT Module to create a consent statement for the following use case in accordance with the implementation specification at § 170.215(c)(2): <ul style="list-style-type: none"> ○ Use Case 2: Inactivate an existing Consent Statement. 7. The user demonstrates the ability of the Health IT Module to create the consent statement for the following use case in accordance with the implementation specification at § 170.215(c)(2): <ul style="list-style-type: none"> ○ Use Case 3: Create an active, signed Consent Statement with multiple Intended Recipients and a variety of actions controlled by the consent (as specified by the Consent ConsentExceptType 	<p>error.</p> <ol style="list-style-type: none"> 3. The tester verifies the documentation for the handling of policies as they relate to consent statements is in accordance with the implementation specification specified at § 170.215(c)(2) and includes a default action for data elements (e.g. disclose) and a computable policy (e.g. XACML engine). 4. The tester verifies the following information is present as part of the creation of the consent statement in accordance with the implementation specification specified at § 170.215(c)(2): <ul style="list-style-type: none"> ○ Identifier - unique identifier for the consent statement maintained by the Health IT Module’s Consent Management system; ○ Status - indicator of the current consent statement status (e.g. active, inactive); ○ Patient - reference to whom the consent statement concerns; ○ Period – start date that the consent becomes active (cannot be earlier than the date/time the consent is issued) and end date the consent becomes inactive, expired, or revoked; ○ Date/Time - Date the consent was signed and made active, unsigned consents will not have dates; ○ Consenting Party reference entity signing the consent; ○ Consent Actor(s) - entities used to specify the custodian(s) (CST role) and information recipient(s) (IRCP role), where at least one of each role must be present in the consent; ○ Organization - references the entity that manages the consents; ○ Purpose - coded value indication the consent purpose (e.g. treatment, research); and ○ Exception - list of protected information if the consent differs from the base policy according to the applicable consent(s).

System Under Test	Test Lab Verification
<p>(deny/permit)) based upon the base policy.</p> <p>8. The user demonstrates the ability of the Health IT Module to create the consent statement for the following use case in accordance with the implementation specification at § 170.215(c)(2):</p> <ul style="list-style-type: none"> ○ Use Case 4: Consent Statement with an Intended Recipient and a variety of actions controlled by the consent which override the base policy for protected information (as specified by the Consent ConsentExceptType securityLabel (deny/permit)). 	<p><u>Consent Statement Use Cases</u></p> <p>5. The tester verifies that the consent statement created by the Health IT Module and made active (per Use Case 1) is accurate and complete in accordance with the implementation specification specified at § 170.215(c)(2) and includes the following information:</p> <ul style="list-style-type: none"> ○ The status of the consent statement is “active”; ○ The period contains the start date/time the consent statement was made active; ○ The date/time of the consent statement is set to the time when the consent statement was signed; and ○ The actions applied to the data elements matches the base policy. <p>6. The tester verifies that the consent statement created by the Health IT Module and made inactive (per Use Case 2) is accurate and complete in accordance with the implementation specification specified at § 170.215(c)(2) and includes the following information:</p> <ul style="list-style-type: none"> ○ The status of the consent statement is “inactive”; and ○ The period contains the end date/time the consent statement was made inactive. <p>7. The tester verifies that an active consent statement created by the Health IT Module with multiple Intended Recipients with different types (e.g. admitting officer, provider) (per Use Case 3) is accurate and complete in accordance with the implementation specification specified at § 170.215(c)(2) and includes the following information:</p> <ul style="list-style-type: none"> ○ The status of the consent statement is “active”; ○ The period contains the start date/time the consent statement was made active; ○ The date/time of the consent statement is set to the time when

System Under Test	Test Lab Verification
	<p>the consent statement was signed;</p> <ul style="list-style-type: none"> ○ The list of multiple intended recipients matches what was provided; and ○ The actions applied to the data elements matches the base policy for each of the intended recipients. <p>8. The tester verifies that an active consent statement created by the Health IT Module with the protected information action overriding the base policy for an intended recipient (per Use Case 4) is accurate and complete in accordance with the implementation specification specified at § 170.215(c)(2) and includes the following information:</p> <ul style="list-style-type: none"> ○ The status of the consent statement is “active”; ○ The period contains the start date/time the consent statement was made active; ○ The date/time of the consent statement is set to the time when the consent statement was signed; and ○ The actions applied to the data elements matches the ConsentExceptType securityLabel for each of the resources controlled by the consent.

Paragraph (g)(11)(i)(A)

System Under Test	Test Lab Verification
<p><u>Allow Access to FHIR Resource</u></p> <p>1. The user demonstrates that the Health IT Module gives access to a FHIR resource based upon the active consent statement in accordance with the standard specified at § 170.215(c)(1) HL7 Fast Healthcare Interoperability Resources (FHIR®) STU Release 3 when an intended recipient has the applicable consent to access the</p>	<p><u>Allow Access to FHIR Resource</u></p> <p>1. The tester verifies that the Health IT Module returns the FHIR resource content as specified in the standard at § 170.215(c)(1) when an intended recipient has the applicable consent and the information is complete and without omissions.</p> <p>2. The tester verifies the documentation for the handling of patients</p>

System Under Test	Test Lab Verification
<p>protected information (per Use Case 1).</p> <ol style="list-style-type: none"> 2. The health IT developer supplies documentation on how the Health IT Module gives access to a FHIR resource when no active consent statement exists, because a consent has been inactivated, expired, or has never been activated (per Use Case 2). 3. The user demonstrates that the Health IT Module only gives access to a FHIR resource if the intended recipient(s) within an active consent statement have the applicable consent to access the protected information in accordance with the standard specified at § 170.215(c)(1) and the implementation specification specified at § 170.215(c)(2) Health Level 7 (HL7®) Implementation Specification – FHIR Profile: Consent2Share FHIR Consent Profile Design (Affirmative Case 3). 4. The user demonstrates that the Health IT Module only gives access to a FHIR resource if securityLabel within the consent statement for the resource allows the intended recipient to access the protected information in accordance with the standard specified at § 170.215(c)(1) and the implementation specification specified at § 170.215(c)(2) (Affirmative Case 4). <p><u>Deny Access to FHIR Resource</u></p> <ol style="list-style-type: none"> 5. Negative Testing: The user demonstrates that the Health IT Module denies access to a FHIR resource when an intended recipient does not have the applicable consent to access the protected information in accordance with the standard at § 170.215(c)(1) and the implementation specification at § 170.215(c)(2) (Negative Case 1/3). 6. Negative Testing: The user demonstrates that the Health IT Module denies access to a FHIR resource when no resource is found in accordance with the standard at § 170.215(c)(1). 	<p>without active consent statements is in accordance with the implementation specification specified at § 170.215(c)(2) and minimally includes a default action for FHIR resources as specified in the standard at § 170.215(c)(1).</p> <ol style="list-style-type: none"> 3. The tester verifies that the Health IT Module returns the FHIR resource content as specified in the standard at § 170.215(c)(1) for an intended recipient who has the applicable consent and the information is complete and without omissions. 4. The tester verifies that the Health IT Module returns the FHIR resource content as specified in the standard at § 170.215(c)(1) only if the intended recipient has permission to access protected information based upon the intended recipient’s securityLabel for the resource within the consent statement in accordance with the implementation specification specified at §170.215(c)(2) and that the information returned is complete and without omissions. <p><u>Deny Access to FHIR Resource</u></p> <ol style="list-style-type: none"> 5. Negative Testing: The tester verifies that the Health IT Module denies access to a FHIR resource when an intended recipient does not have the applicable consent in accordance with the implementation specification specified at § 170.215(c)(2) and that the error reported does not expose the patient’s consent status in accordance with the implementation specification specified at § 170.215(c)(2). 6. Negative Testing: The tester verifies that the Health IT Module does not return data when no FHIR resource exists in accordance with the standard specified at § 170.215(c)(1) and that the error reported is the same as the error reported when a user does not have access to a FHIR resource, as to not expose the patient’s consent status in accordance with the implementation specification specified at §

System Under Test	Test Lab Verification
<p>7. Negative Testing: The user demonstrates that the Health IT Module denies access to a FHIR resource when the securityLabel associated with protected information for an intended recipient does not allow access to the protected information in accordance with the implementation specification specified at § 170.215(c)(2) (Negative Case 4).</p>	<p>170.215(c)(2).</p> <p>7. Negative Testing: The tester verifies that the Health IT Module denies access to a FHIR resource when the securityLabel associated with protected information for an intended recipient does not allow access to the protected information in accordance with the implementation specification specified at § 170.215(c)(2) and that the error reported does not expose the patient’s consent status in accordance with the implementation specification specified at § 170.215(c)(2).</p>

Paragraph (g)(11)(ii)(A)

System Under Test	Test Lab Verification
<p>1. The health IT developer supplies documentation describing the Consent Management for API, with the intended audience of developers, and includes at a minimum:</p> <ul style="list-style-type: none"> ○ API syntax; ○ Function names; ○ Required and optional parameters and their data types; ○ Return variables and their types/structures; and ○ Exceptions and exception handling methods and their returns. <p>2. The health IT developer supplies accompanying documentation describing the Health IT Module’s Consent Management for API implementation requirements, with the intended audience of developers, which must include:</p> <ul style="list-style-type: none"> ○ The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the Health IT Module’s Consent Management for API and process its response(s). 	<p>1. The tester verifies that the identified documentation for the Health IT Module’s Consent Management for API definition is accurate and without omission and that it matches the version of the software release.</p> <p>2. The tester verifies that the identified documentation for interfacing with the Health IT Module’s Consent Management for API (including both the software components and the configuration) is accurate and without omission and that it matches the version of the software release.</p> <p>3. The tester verifies that the identified documentation necessary for an application to register with an authorized server is accurate and without omission and that it matches the version of the software release</p>

System Under Test	Test Lab Verification
3. The health IT developer supplies accompanying documentation describing all of the technical requirements and attributes necessary for an application to be registered with an authorized server.	

Paragraph (g)(11)(ii)(B)

System Under Test	Test Lab Verification
The documentation used to meet paragraph (g)(11)(ii)(A) of this section must be available via a publicly accessible hyperlink.	The tester verifies that the supplied documentation is publicly accessible by hyperlink.