Clinical quality measures (CQMs) — report

healthit.gov/test-method/clinical-quality-measures-cqms-report

- Certification Companion Guide (CCG)
- Test Procedure

Updated on 12-17-2024

Regulation Text

Regulation Text

§ 170.315(c)(3) *Clinical quality measures—report—*

Enable a user to electronically create a data file for transmission of clinical quality measurement data:

(i) In accordance with the applicable implementation specifications specified by the CMS implementation guides for Quality Reporting Document Architecture (QRDA), category I, for inpatient measures in § 170.205(h)(3) and CMS implementation guide for QRDA, category III for ambulatory measures in § 170.205 (k)(3); or

(ii) In accordance with the standards specified in § 170.205(h)(2) and § 170.205(k)(1) and (2) for the period until December 31, 2022.

Standard(s) Referenced

Paragraph (c)(3)

§ 170.205(h)(3) CMS Implementation Guide for Quality Reporting Document Architecture: Category I; Hospital Quality Reporting; Implementation Guide for 2020

§ 170.205(k)(3) CMS Implementation Guide for Quality Reporting Document Architecture: Category III; Eligible Clinicians and Eligible Professionals Programs; Implementation Guide for 2020

Standards Version Advancement Process (SVAP) Version(s) Approved

CMS Implementation Guide for Quality Reporting Document Architecture Category I Hospital Quality Reporting; Implementation Guide for 2024 (Updated August 2023)

CMS Implementation Guide for Quality Reporting Document Architecture Category III Eligible Clinicians Programs; Implementation Guide for 2024 (Updated November 2023)

For more information, please visit the Standards Version Advancement Process (SVAP) Version(s) page.

Certification Dependencies

Conditions and Maintenance of Certification Requirements

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)(4) and § 170.315(g)(5)) 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, when different QMS are used, each QMS needs to be separately 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(c)(3). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to a § 170.315(c) “paragraph (c)” 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 paragraph (c) 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, an exception exists 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 2:

For each applicable privacy and security certification criterion not certified for 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 that enable the Health IT Module 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
1.1	Updated tests with 2024 SVAP adopted standards.	11-14-2024
1.2	Corrected reference to 2024 SVAP adopted standards in test steps.	12-17-2024

Regulation Text

Regulation Text

§ 170.315(c)(3) *Clinical quality measures—report—*

Enable a user to electronically create a data file for transmission of clinical quality measurement data:

(i) In accordance with the applicable implementation specifications specified by the CMS implementation guides for Quality Reporting Document Architecture (QRDA), category I, for inpatient measures in § 170.205(h)(3) and CMS implementation guide for QRDA, category III for ambulatory measures in § 170.205 (k)(3); or

(ii) In accordance with the standards specified in § 170.205(h)(2) and § 170.205(k)(1) and (2) for the period until December 31, 2022.

Standard(s) Referenced

Paragraph (c)(3)

§ 170.205(h)(3) CMS Implementation Guide for Quality Reporting Document Architecture: Category I; Hospital Quality Reporting; Implementation Guide for 2020

§ 170.205(k)(3) CMS Implementation Guide for Quality Reporting Document Architecture: Category III; Eligible Clinicians and Eligible Professionals Programs; Implementation Guide for 2020

Standards Version Advancement Process (SVAP) Version(s) Approved

CMS Implementation Guide for Quality Reporting Document Architecture Category I Hospital Quality Reporting; Implementation Guide for 2024 (Updated August 2023)

CMS Implementation Guide for Quality Reporting Document Architecture Category III Eligible Clinicians Programs; Implementation Guide for 2024 (Updated November 2023)

For more information, please visit the Standards Version Advancement Process (SVAP) Version(s) page.

Certification Dependencies
Conditions and Maintenance of Certification Requirements

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)(4) and § 170.315(g)(5)) 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, when different QMS are used, each QMS needs to be separately 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(c)(3). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to a § 170.315(c) “paragraph (c)” 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 paragraph (c) 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, an exception exists 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))
  - Auditable events and tamper-resistance (§ 170.315(d)(2))
  - Audit reports (§ 170.315(d)(3))
  - Automatic access time-out (§ 170.315(d)(5))
  - 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 for 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 that enable the Health IT Module 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.

Testing

Testing Tool

Cypress

Criterion Subparagraph	Test Data

Criterion Subparagraph	Test Data
(c)(3)	Cypress Gold Standard Test Data created using Cypress - generated to match the submitted exported CMS QRDA Category I IG files created during section (c)(1)(ii) and generated CMS QRDA Category I IG files created as a result of section (c)(2)(i) Import of Clinical Quality Measures (CQMs).

Revision History

Version #	Description of Change	Version Date
1.0	Initial publication	03-11-2024
1.1	Updated tests with 2024 SVAP adopted standards.	11-14-2024
1.2	Corrected reference to 2024 SVAP adopted standards in test steps.	12-17-2024

This Test Procedure illustrates the test steps required to certify a Health IT Module to this criterion. Please consult the most recent ONC Final Rule on the Certification Regulations page for a detailed description of the certification criterion with which these testing steps are associated. ONC also encourages developers to consult the Certification Companion Guide in tandem with the test procedure as it provides clarifications that may be useful for product development and testing.

Note: The test step order does not necessarily prescribe the order in which the tests should take place.

Testing components

ONC Supplied Test Data

Paragraph (c)(3) Clinical quality measures—report

System Under Test

CMS Quality Reporting Document Architecture (QRDA) Category III Implementation Guide (IG) Report

1. The user can generate an aggregate report with calculated summary data for the patient population of the clinical quality measures calculated in the Execute test (§ 170.315(c)(2)), which at a minimum is in accordance with the standard specified in § 170.205(k)(3). CMS Implementation Guide for Quality Reporting Document Architecture: Category III; Eligible Clinicians and Eligible Professionals Programs; Implementation Guide for 2020, or

Approved SVAP Version(s)

CMS Implementation Guide for Quality Reporting Document Architecture Category III Eligible Clinicians Programs; Implementation Guide for 2024 (Updated November 2023)

CMS QRDA Category I IG Report

2. A user can generate a de-duplicated archive of patient documents in the CMS QRDA Category I IG format of the clinical quality measures calculated in the Execute test (§ 170.315(c)(2)), which at a minimum is in accordance with the standard specified in: § 170.205(h)(3). CMS Implementation Guide for Quality Reporting Document Architecture: Category I; Hospital Quality Reporting; Implementation Guide for 2020, or

Approved SVAP Version(s)

CMS Implementation Guide for Quality Reporting Document Architecture Category I Hospital Quality Reporting; Implementation Guide for 2024 (Updated August 2023)

Data File for Transmission

3. The health IT developer submits the quality measurement data file consisting of the data created by the generation of the CMS QRDA Category III IG aggregate report(s) and the de-duplicated CMS QRDA Category I IG report(s) for verification.

Test Lab Verification

Test Lab Setup

1. Prior to beginning this test, the tester creates and exports data using Cypress, and the health IT developer imports the data into its Health IT Module.

CMS QRDA Category III IG Report

2. Using the Cypress supplied XML Schema validation, the tester:
    1. uploads the aggregate report(s) submitted by the health IT developer; and
    2. runs the Cypress supplied XML schema validation for each aggregate report.
3. The tester verifies that all of the QRDA Category III aggregate report(s) submitted by the health IT developer are at a minimum in accordance with the standard specified in § 170.205(k)(3) through evaluation of the Cypress validation report.

CMS QRDA Category I IG Report

4. The tester verifies all of the de-duplicated CMS QRDA Category I IG report(s), submitted by the health IT developer are at a minimum in accordance with the standard specified in § 170.205(h)(3) through evaluation of the Cypress validation report.

Data File for Transmission

5. The tester verifies via visual inspection that the data file for transmission submitted with clinical quality measurement data includes both de-duplicated CMS QRDA Category I IG and aggregate CMS QRDA Category III IG report(s).

System Under Test

CMS Quality Reporting Document Architecture (QRDA) Category III Implementation Guide (IG) Report

1. The user can generate an aggregate report with calculated summary data for the patient population of the clinical quality measures calculated in the Execute test (§ 170.315(c)(2)), which at a minimum is in accordance with the standard specified in § 170.205(k)(3). CMS Implementation Guide for Quality Reporting Document Architecture: Category III; Eligible Clinicians and Eligible Professionals Programs; Implementation Guide for 2020, or

Approved SVAP Version(s)

CMS Implementation Guide for Quality Reporting Document Architecture Category III Eligible Clinicians Programs; Implementation Guide for 2024 (Updated November 2023)

CMS QRDA Category I IG Report

2. A user can generate a de-duplicated archive of patient documents in the CMS QRDA Category I IG format of the clinical quality measures calculated in the Execute test (§ 170.315(c)(2)), which at a minimum is in accordance with the standard specified in: § 170.205(h)(3). CMS Implementation Guide for Quality Reporting Document Architecture: Category I; Hospital Quality Reporting; Implementation Guide for 2020, or

Approved SVAP Version(s)

CMS Implementation Guide for Quality Reporting Document Architecture Category I Hospital Quality Reporting; Implementation Guide for 2024 (Updated August 2023)

Data File for Transmission

Test Lab Verification

Test Lab Setup

1. Prior to beginning this test, the tester creates and exports data using Cypress, and the health IT developer imports the data into its Health IT Module.

CMS QRDA Category III IG Report

2. Using the Cypress supplied XML Schema validation, the tester:
    1. uploads the aggregate report(s) submitted by the health IT developer; and
    2. runs the Cypress supplied XML schema validation for each aggregate report.
3. The tester verifies that all of the QRDA Category III aggregate report(s) submitted by the health IT developer are at a minimum in accordance with the standard specified in § 170.205(k)(3) through evaluation of the Cypress validation report.

CMS QRDA Category I IG Report

System Under Test

3. The health IT developer submits the quality measurement data file consisting of the data created by the generation of the CMS QRDA Category III IG aggregate report(s) and the de-duplicated CMS QRDA Category I IG report(s) for verification.

Test Lab Verification

4. The tester verifies all of the de-duplicated CMS QRDA Category I IG report(s), submitted by the health IT developer are at a minimum in accordance with the standard specified in § 170.205(h)(3) through evaluation of the Cypress validation report.

Data File for Transmission

5. The tester verifies via visual inspection that the data file for transmission submitted with clinical quality measurement data includes both de-duplicated CMS QRDA Category I IG and aggregate CMS QRDA Category III IG report(s).

Archived Version:
§ 170.315(c)(3) Clinical quality measures (CQMs) — report TP

Updated on 08-19-2024

Regulation Text

Regulation Text

§ 170.315(c)(3) *Clinical quality measures—report—*

Enable a user to electronically create a data file for transmission of clinical quality measurement data:

(i) In accordance with the applicable implementation specifications specified by the CMS implementation guides for Quality Reporting Document Architecture (QRDA), category I, for inpatient measures in § 170.205(h)(3) and CMS implementation guide for QRDA, category III for ambulatory measures in § 170.205 (k)(3); or

(ii) In accordance with the standards specified in § 170.205(h)(2) and § 170.205(k)(1) and (2) for the period until December 31, 2022.

Standard(s) Referenced

Paragraph (c)(3)

§ 170.205(h)(3) CMS Implementation Guide for Quality Reporting Document Architecture: Category I; Hospital Quality Reporting; Implementation Guide for 2020

§ 170.205(k)(3) CMS Implementation Guide for Quality Reporting Document Architecture: Category III; Eligible Clinicians and Eligible Professionals Programs; Implementation Guide for 2020

Standards Version Advancement Process (SVAP) Version(s) Approved

CMS Implementation Guide for Quality Reporting Document Architecture Category I Hospital Quality Reporting; Implementation Guide for 2024 (Updated August 2023)

CMS Implementation Guide for Quality Reporting Document Architecture Category III Eligible Clinicians Programs; Implementation Guide for 2024 (Updated November 2023)

For more information, please visit the Standards Version Advancement Process (SVAP) Version(s) page.

Certification Dependencies

Conditions and Maintenance of Certification Requirements

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)(4) and § 170.315(g)(5)) 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, when different QMS are used, each QMS needs to be separately 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(c)(3). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to a § 170.315(c) “paragraph (c)” 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 paragraph (c) 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, an exception exists 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))
  - Auditable events and tamper-resistance (§ 170.315(d)(2))
  - Audit reports (§ 170.315(d)(3))
  - Automatic access time-out (§ 170.315(d)(5))
  - 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 for 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 that enable the Health IT Module 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

Version #	Description of Change	Version Date
1.0	Initial publication	03-11-2024
1.1	Updated tests with 2024 SVAP adopted standards.	11-14-2024
1.2	Corrected reference to 2024 SVAP adopted standards in test steps.	12-17-2024

Regulation Text

Regulation Text

§ 170.315(c)(3) *Clinical quality measures—report—*

Enable a user to electronically create a data file for transmission of clinical quality measurement data:

(i) In accordance with the applicable implementation specifications specified by the CMS implementation guides for Quality Reporting Document Architecture (QRDA), category I, for inpatient measures in § 170.205(h)(3) and CMS implementation guide for QRDA, category III for ambulatory measures in § 170.205 (k)(3); or

(ii) In accordance with the standards specified in § 170.205(h)(2) and § 170.205(k)(1) and (2) for the period until December 31, 2022.

Standard(s) Referenced

Paragraph (c)(3)

§ 170.205(h)(3) CMS Implementation Guide for Quality Reporting Document Architecture: Category I; Hospital Quality Reporting; Implementation Guide for 2020

§ 170.205(k)(3) CMS Implementation Guide for Quality Reporting Document Architecture: Category III; Eligible Clinicians and Eligible Professionals Programs; Implementation Guide for 2020

Standards Version Advancement Process (SVAP) Version(s) Approved

CMS Implementation Guide for Quality Reporting Document Architecture Category I Hospital Quality Reporting; Implementation Guide for 2024 (Updated August 2023)

CMS Implementation Guide for Quality Reporting Document Architecture Category III Eligible Clinicians Programs; Implementation Guide for 2024 (Updated November 2023)

For more information, please visit the Standards Version Advancement Process (SVAP) Version(s) page.

Certification Dependencies
Conditions and Maintenance of Certification Requirements

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)(4) and § 170.315(g)(5)) 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, when different QMS are used, each QMS needs to be separately 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(c)(3). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to a § 170.315(c) “paragraph (c)” 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 paragraph (c) 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, an exception exists 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 2:

For each applicable privacy and security certification criterion not certified for 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 that enable the Health IT Module 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
1.1	Standards Referenced updated to reflect 2024 Approved SVAP Standards	08-19-2024

Testing

Testing Tool

Cypress

Criterion Subparagraph	Test Data
(c)(3)	Cypress Gold Standard Test Data created using Cypress - generated to match the submitted exported CMS QRDA Category I IG files created during section (c)(1)(ii) and generated CMS QRDA Category I IG files created as a result of section (c)(2)(i) Import of Clinical Quality Measures (CQMs).

Certification Companion Guide: Clinical quality measures (CQMs) — report

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
Not Included	Yes	No	Yes	No

Certification Requirements

Technical Explanations and Clarifications

Applies to entire criterion

Technical outcome – Enable a user to electronically create a data file for transmission of CQM data in accordance with the CMS Quality Reporting Document Architecture (QRDA) Category I Implementation Guide (IG) for inpatient measures as adopted in § 170.205(h)(3) and CMS QRDA Category III IG for ambulatory measures as adopted in § 170.205(k)(3).

Clarifications:

- The specific version, number, and type of clinical quality measures (CQMs) presented for certification are determined at the developer’s discretion. We recommend developers consult any Centers for Medicare and Medicaid Services (CMS) or other programs’ requirements around the specific version, number, or type of CQMs required for providers in determining the CQMs presented for certification.
- Health IT developers are permitted to test and certify to the newest CMS QRDA Category I and Category III IGs, regardless of the versions approved by the National Coordinator via the Standards Version Advancement Process (SVAP).

- Certain CMS programs require or provide the option for electronic CQM (eCQM) reporting. These programs include the Promoting Interoperability Program, the Physician Quality Reporting System, the Hospital Inpatient Quality Reporting Program, the Comprehensive Primary Care (CPC) initiative, CPC Plus, and the Value-Based Payment Modifier Program. Each year, CMS issues annual updates to eCQMs (herein referred to as the "CMS annual measure update(s)") which are published on the Electronic Clinical Quality Improvement (eCQI) Resource Center. The CMS annual measure updates rely upon specific versions of the HL7® Quality Reporting Document Architecture (QRDA) Category I and Category III standards. Each year's HL7® QRDA Category I and Category III standards are referenced in the corresponding CMS QRDA Implementation Guides (IGs) associated with that program year and CMS annual measure update. The CMS QRDA Category I and Category III IGs also contain additional programmatic form and manner requirements necessary for reporting to CMS programs, which make it necessary for the corresponding testing tools to keep pace with these measure updates and CMS reporting requirements.
- Compliance with this certification criterion is dependent on the update to the CMS QRDA Category I and Category III IGs. It is ONC's expectation that health IT developers will update Health IT Modules to align with the 2023 CMS QRDA Category I and Category III IGs in a timely fashion that allows users to report eCQMs to CMS in early 2024. Health IT developers should continue to update Health IT Modules to align with the CMS annual update to the CMS QRDA Category I and Category III IGs for continued compliance with this certification criterion.
- For details on the latest CMS QRDA Category I and Category III IGs, ONC refers readers to the eCQI Resource Center website.
- After technology is certified to specific CQMs for this § 170.315(c)(3) criterion, technology is not required to recertify to the annual measure specification updates CMS issues to maintain certification unless that product is relabeled. Said another way, other programs, such as the Promoting Interoperability Program, may require developers upgrade their technology to the newest CQM specifications, but the technology is not required to be retested or recertified unless explicitly specified in other program requirements. It is expected that all systems will test all measures and standards updates as a best practice. The testing tools are available for each CMS annual measure update and when there are late standards errata or CMS requirement changes to facilitate additional testing.
- While health IT developers are not required to re-certify to updated versions of CQMs, they must test and certify to newly added CQMs.
- For the purposes of automated testing to meet certification requirements, only errors (but not warnings) generated during testing would constitute a failure to meet certification requirements.

- To prevent unintended burden by tailoring the requirements to the type of measures being tested ONC has provided the following clarifications: For the updated certification criterion "CQMs—report" in § 170.315(c)(3) a Health IT Module testing only inpatient measures would test only with the CMS QRDA Category I IG and a Health IT Module testing only ambulatory measures would test only with the CMS QRDA Category III IG. A Health IT Module supporting both inpatient and ambulatory measures would be required to test to both the CMS QRDA Category I and Category III IGs.
- Health IT developers can choose to use the flexibility of the SVAP to use more advanced version(s) of standards than the version(s) incorporated by reference in the regulation for this certification criterion. To comply with the Maintenance of Certification requirement in §170.405(b), a developer that chooses to pursue such updates must include in their Real World Testing plan each Certified Health IT Module updated to newer version(s) of any standard(s) prior to August 31 of the year in which their updates were made and test each Module the following calendar year for conformance to all applicable criteria within its scope, including the newer version(s) of any standard(s).
- Health IT developers updating their already Certified Health IT Modules who choose to leverage the SVAP flexibility will be required to provide advance notice to all affected customers and its ONC-ACB. To be open and transparent to the public, health IT developers must also provide its ONC-ACB with a publicly accessible hyperlink to the SVAP Notice to be published with the Module on the ONC Certified Health IT Product List (CHPL).

Technical outcome – Enable a user to electronically create a data file for transmission of CQM data in accordance with the CMS Quality Reporting Document Architecture (QRDA) Category I Implementation Guide (IG) for inpatient measures as adopted in § 170.205(h)(3) and CMS QRDA Category III IG for ambulatory measures as adopted in § 170.205(k)(3).

Clarifications:

- The specific version, number, and type of clinical quality measures (CQMs) presented for certification are determined at the developer's discretion. We recommend developers consult any Centers for Medicare and Medicaid Services (CMS) or other programs' requirements around the specific version, number, or type of CQMs required for providers in determining the CQMs presented for certification.
- Health IT developers are permitted to test and certify to the newest CMS QRDA Category I and Category III IGs, regardless of the versions approved by the National Coordinator via the Standards Version Advancement Process (SVAP).

- Certain CMS programs require or provide the option for electronic CQM (eCQM) reporting. These programs include the Promoting Interoperability Program, the Physician Quality Reporting System, the Hospital Inpatient Quality Reporting Program, the Comprehensive Primary Care (CPC) initiative, CPC Plus, and the Value-Based Payment Modifier Program. Each year, CMS issues annual updates to eCQMs (herein referred to as the "CMS annual measure update(s)") which are published on the Electronic Clinical Quality Improvement (eCQI) Resource Center. The CMS annual measure updates rely upon specific versions of the HL7® Quality Reporting Document Architecture (QRDA) Category I and Category III standards. Each year's HL7® QRDA Category I and Category III standards are referenced in the corresponding CMS QRDA Implementation Guides (IGs) associated with that program year and CMS annual measure update. The CMS QRDA Category I and Category III IGs also contain additional programmatic form and manner requirements necessary for reporting to CMS programs, which make it necessary for the corresponding testing tools to keep pace with these measure updates and CMS reporting requirements.
- Compliance with this certification criterion is dependent on the update to the CMS QRDA Category I and Category III IGs. It is ONC's expectation that health IT developers will update Health IT Modules to align with the 2023 CMS QRDA Category I and Category III IGs in a timely fashion that allows users to report eCQMs to CMS in early 2024. Health IT developers should continue to update Health IT Modules to align with the CMS annual update to the CMS QRDA Category I and Category III IGs for continued compliance with this certification criterion.
- For details on the latest CMS QRDA Category I and Category III IGs, ONC refers readers to the eCQI Resource Center website.
- After technology is certified to specific CQMs for this § 170.315(c)(3) criterion, technology is not required to recertify to the annual measure specification updates CMS issues to maintain certification unless that product is relabeled. Said another way, other programs, such as the Promoting Interoperability Program, may require developers upgrade their technology to the newest CQM specifications, but the technology is not required to be retested or recertified unless explicitly specified in other program requirements. It is expected that all systems will test all measures and standards updates as a best practice. The testing tools are available for each CMS annual measure update and when there are late standards errata or CMS requirement changes to facilitate additional testing.
- While health IT developers are not required to re-certify to updated versions of CQMs, they must test and certify to newly added CQMs.
- For the purposes of automated testing to meet certification requirements, only errors (but not warnings) generated during testing would constitute a failure to meet certification requirements.
- To prevent unintended burden by tailoring the requirements to the type of measures being tested ONC has provided the following clarifications: For the updated certification criterion "CQMs—report" in § 170.315(c)(3) a Health IT Module testing only inpatient measures would test only with the CMS QRDA Category I IG and a Health IT Module testing only ambulatory measures would test only with the CMS QRDA Category III IG. A Health IT Module supporting both inpatient and ambulatory measures would be required to test to both the CMS QRDA Category I and Category III IGs.

- The following links are references to CMS CQM reporting resources:
  - CMS and ONC eCQI Resource Center
  - CMS Quality Measure Basics
  - CMS Promoting Interoperability Program Resource Page (contains program requirements, reporting requirements, and other resources for each program year).
- Health IT developers can choose to use the flexibility of the SVAP to use more advanced version(s) of standards than the version(s) incorporated by reference in the regulation for this certification criterion. To comply with the Maintenance of Certification requirement in §170.405(b), a developer that chooses to pursue such updates must include in their Real World Testing plan each Certified Health IT Module updated to newer version(s) of any standard(s) prior to August 31 of the year in which their updates were made and test each Module the following calendar year for conformance to all applicable criteria within its scope, including the newer version(s) of any standard(s).
- Health IT developers updating their already Certified Health IT Modules who choose to leverage the SVAP flexibility will be required to provide advance notice to all affected customers and its ONC-ACB. To be open and transparent to the public, health IT developers must also provide its ONC-ACB with a publicly accessible hyperlink to the SVAP Notice to be published with the Module on the ONC Certified Health IT Product List (CHPL).

Archived Version:

§ 170.315(c)(3) Clinical quality measures (CQMs) — report CCG