# Clinical Quality Metrics Registry (CQMR) Policies and Procedures

Contents



## Section 1: Who Must Comply with the Policies and Procedures

These Policies and Procedures represent an important safeguard for protecting information from various internal and external risks, including unauthorized access.

1. All Participating Entities that have signed an organizational Participation Agreement ("Agreement") and wish to use the Clinical Quality Metrics Registry (CQMR) must comply with these Policies and Procedures. A Participating Entity's failure to comply with these Policies and Procedures constitutes a breach of the Agreement and may result in termination of the Agreement, denial of access to the System, or other sanctions as may be designated in the Agreement and in these Policies and Procedures.
2. All Authorized Users must comply with the provisions of these Policies and Procedures that are applicable to Authorized Users. An Authorized User's failure to comply with the provisions of these Policies and Procedures applicable to Authorized Users constitutes a breach of the Authorized User Agreement and may result in termination of the Authorized User Agreement, denial of access to the System by the Authorized User, or other sanctions as may be designated in the Authorized User Agreement and in these Policies and Procedures.

## Section 2: Definitions

1. "**Adverse Security Event**" means the unauthorized acquisition, access, disclosure, or use of unencrypted CQM Data by anyone who is not an Authorized User or by an Authorized User in any manner that is not permitted under this Agreement.
2. "**Authorized User**" means an individual or a Participating Entity using the CQMR System in a manner consistent with Permitted Uses.
3. "**Clinical Quality Measure Data**" or "**CQM Data**" means reported data elements such as numerators, denominators, exceptions, exclusions, and supplemental data, such as patient race, ethnicity, and payer, as contained in the measure specifications. Depending on the requirements of the Quality Reporting Program, CQM Data can be reported as in the aggregate (for example, totals for a provider or clinic for each data element in a CQM) or at the individual patient level.

   As used in this Agreement, CQM Data also may include additional data that is used to enrich the CQM Data reported by healthcare providers. Such data may include, for example, health plan enrollment data, which can be used to attribute patient data to health plans who are authorized to reimburse for patient care, so that when healthcare providers report CQM Data at the individual patient level, the CQMR System can filter the CQM Data by health plan.

4. "**Clinical Quality Metrics Registry**" or "**CQMR**" means the Service and System provided by OHA for the collection, analysis, display, and export of CQM Data. The Service will support reporting to Quality Reporting Programs as identified by OHA in the CQMR Policies and Procedures. OHA has contracted with Vendors for the provision of the CQMR Service and System.
5. "**HIPAA**" means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Public Law 111-5 ("ARRA") and its implementing Privacy Rule and Security Rule, 45 CFR Parts 160 and 164, each as may be amended from time to time.
6. "**Participating Entity**" means a HIPAA Covered Entity or Business Associate that meets the requirements for use of the CQMR as set forth in the Policies and Procedures and is a signatory to this Participation Agreement. Participating Entities may include healthcare providers; health plans, including Coordinated Care Organizations (CCOs); and health care providers' or health plans' Business Associates, such as a health information exchange (HIE) or a quality registry.
7. "**Quality Reporting Programs**" means programs that are intended to assess healthcare quality, whether as the program's primary focus or a component of a larger program. Examples of Quality Reporting Programs

include Oregon's Coordinated Care Organization (CCO) incentive measures, Oregon's Medicaid Electronic Health Record (EHR) Incentive Program, the Centers for Medicare & Medicaid Services (CMS) Merit-based Incentive Payment System (MIPS), and Comprehensive Primary Care Plus (CPC+).

## Section 3: Quality Reporting Programs

OHA is implementing the CQMR to support reporting of clinical quality measures used in Quality Reporting Programs. Intended initial uses are to support Coordinated Care Organization (CCO) incentive measures, Oregon's Medicaid Electronic Health Record (EHR) Incentive Program, and Comprehensive Primary Care Plus (CPC+) in Oregon. The CQMR also may be used to support the Merit-based Incentive Payment System (MIPS) for Participating Entities that also participate in CCO incentive measures, Oregon's Medicaid EHR Incentive Program, or CPC+.

OHA intends to make the CQMR available to support additional Quality Reporting Programs. OHA's intention is to support quality improvement efforts and decrease administrative burdens of quality reporting by:

- enabling Oregon health care providers to report clinical quality measures data to the CQMR,
- collecting supplemental data from health plans and potentially additional sources over time to enrich the clinical quality measure data set,
- providing functionality to filter the reported clinical quality measure data by fields such as payer and practice location, as needed for quality reporting and quality improvement activities,
- offering the ability to send reports meet quality reporting obligations, for example, submitting data to the Quality Payment Program (QPP) portal to satisfy certain Centers for Medicare and Medicaid Services (CMS) reporting requirements for programs such as the Merit-based Incentive Payment System (MIPS) and Comprehensive Primary Care Plus (CPC+).

Additional programs may be supported at OHA's discretion. OHA may consider factors such as alignment of clinical quality measures and reporting parameters in additional programs; availability of funding to support any needed development or operational costs; any approvals needed from CMS as a consequence of federal financial participation in the CQMR or other necessary approvals; consistency with the purposes of the CQMR; and timing considerations for implementation. If OHA changes programs supported by the CQMR, OHA will provide notice by amending these Policies and Procedures using the process set forth in Section 10 below.

1. OHA will use the CQMR System to support its Quality Reporting Program needs, such as calculating measure performance and determining eligibility for incentive payments. OHA also may use CQM Data on Medicaid members for quality assessment and analytics.

2. Providers may use the CQMR System to meet reporting obligations for Quality Reporting Programs and to analyze and export their CQM Data through dashboard and report functions, such as filtering functions to roll up and drill down on data elements.
    a. Oregon Medicaid providers who participate in Oregon's Medicaid EHR Incentive Program or CCO incentive measure reporting may send CQM Data to the CQMR to meet program requirements.
    b. Oregon providers who participate in CPC+ may send CQM Data to the CQMR to meet CMS's, OHA's, or other payers' CPC+ CQM reporting requirements.
    c. Oregon providers participating in CCO incentive measure reporting, Oregon's Medicaid EHR Incentive Program, or CPC+ may send CQM Data to the CQMR to be submitted to CMS to meet MIPS reporting requirements.
3. CCOs and other health plans/ payers may use the CQMR System for quality assessment and improvement activities and to analyze and export CQM Data about their members through dashboard and report functions, such as filtering functions to roll up and drill down on data elements.
    a. Functionality may be offered to allow CCOs and other payers participating in CPC+ to send member enrollment data to the CQMR to help enable accurate attribution of patients to their respective payers.
    b. A CCO may access the CQMR for purposes related to CCO incentive measure reporting, including submitting data proposals, submitting CQM Data on behalf of providers in the CCO's network, and accessing CQM Data submitted by the CCO's network of providers as part of the CCO's data submission.
4. If a Participating Entity chooses to have CQM Data sent to the Centers for Medicare and Medicaid Services (CMS) or to another recipient to meet quality reporting requirements, then the Participating Entity agrees to comply with applicable program requirements of CMS or the other recipient. For example, if a Participating Entity chooses to have the CQMR System send CQM Data to CMS to meet Merit-based Incentive Payment System (MIPS) reporting requirements, the Participating Entity agrees to provide documentation that the Participating Entity has authorized the CQMR vendor to submit data on its behalf and to cooperate with data validation audits as requested.

## Section 4: Permitted Uses

1. The CQMR System and Services may be used consistently with healthcare operations purposes under HIPAA. Parties may access and use the CQMR and CQM Data only as permissible under HIPAA and other applicable laws and regulations.
2. OHA may use CQM Data for operations of its Quality Reporting Programs, such as Oregon's Medicaid EHR Incentive Program and CCO incentive

measures, including, but not limited to, calculation of performance, eligibility for incentives, and public reports.

3. Participating Entity may use the CQMR System and Services to meet additional reporting requirements under Quality Reporting Programs that are supported by the CQMR. For example, if the Merit-based Incentive Payment System (MIPS) is a Quality Reporting Program supported by the CQMR, then a Participating Entity could choose to have its CQM Data sent by the CQMR Vendor to the Centers for Medicare & Medicaid Services (CMS) to meet the Participating Entity's MIPS reporting requirements.
4. Parties may use CQM Data and may combine CQM Data with other data sets, such as claims and administrative data, for quality assessment and improvement activities, including quality comparisons and analytics.
5. CQM Data may be used for research purposes, provided that Participating Entity engages in applicable request and review processes and Participating Entity's use of CQM Data complies with HIPAA and any other applicable laws and regulations.
6. CQM Data may be archived for audit, trending, and quality control purposes.
7. CQM Data may be enriched by OHA vendors for the purposes of standardizing data and enhancing its usability, for example, by supporting patient matching and attribution.
8. OHA and its vendor may extract non-protected, otherwise publicly available information from the CQMR System about Participating Entity and its Authorized Users' affiliations – for example, information that a clinic participates in a particular Quality Reporting Program or information that a physician practices at a particular clinic – and may incorporate that information into Oregon's statewide provider directory.

## Section 5: Authentication

1. **Purpose**. Authentication is the process of verifying the identity of a Participating Entity, and verifying that its designated Administrator(s) is who he or she claims to be. This is accomplished by Participating Entity and the Administrator(s) providing proof of identity.
2. **Policies and Procedures**. OHA's vendor, OneHealthPort, is responsible for authorizing and authenticating a Participating Entity and its designated Administrator(s). The process of authorizing and authenticating includes verifying the identity of Participating Entity, its Administrator(s), and his/her affiliation with Participating Entity based on the information provided to OneHealthPort.

## Section 6: Training

Authorized Users must be trained on how to use the CQMR System properly and their duty to understand and comply with their responsibilities under the Authorized User Agreement, these Policies and Procedures and applicable laws.

1. OHA will provide training materials to Participating Entity on the technical aspects on how to use the System. Participating Entity shall ensure that its Authorized Users review the training materials provided before they begin to use the System.
2. Participating Entity shall ensure that its Authorized Users review and execute Authorized User Agreement, and review these Policies and Procedures before they begin to use the System.
3. Participating Entity shall ensure that its Authorized Users are trained, prior to commencing use of the System and periodically thereafter, on their obligations regarding privacy and security under HIPAA and other applicable laws.

## Section 7: Access

1. **Purpose**. Access controls govern when and how Authorized Users may access the CQMR System and CQM Data. Participating Entity shall implement the minimum controls set forth in this section, and ensure that: (1) only Authorized Users access information via the System; and (2) they do so only in accordance with the requirements (specified herein) that limit their access to specified information. These access policies are designed to minimize any risk of unauthorized access and ensure that the CQMR and CQM Data are used for permissible purposes.
2. **Process**. Each Participating Entity must enter into a Participation Agreement prior to being granted access to and use of the System.
   a. **Authorized Users**. Participating Entity is responsible for facilitating its Authorized Users' access to the System.
      - Participating Entity will identify individuals within its organization that need access to the System to carry out their professional responsibilities. This may include, but is not limited to, health care providers, employees, staff, contractors, or agents of an organization.
      - Participating Entity will identify an individual as the Organization's Administrator ("Administrator") who will be responsible for granting access to all other Authorized Users, and ensuring that Authorized Users agree to terms in the Authorized User Agreement and take the steps necessary to obtain a user name and password. Authorized Users will be informed of the Administrator as the point of contact for all questions, training, and to whom reports of any potential unauthorized access shall be made. This contact information must be readily available to all Authorized Users within the organization. OneHealthPort's policies that describe responsibilities of an Administrator can be found on their website: http://www.onehealthport.com/.
      - Participating Entity shall maintain all records of access and training for the duration of this Agreement and for seven (7)

years following termination. Records include but are not limited to names of Authorized Users, dates when access was granted, dates when training was completed, details if user has violated their Agreement, dates if access is terminated and reason for termination, and dates if access is reinstated.

3. **Termination of Access and Other Sanctions**. Participating Entity shall ensure that an Authorized User's access to the System is terminated in the following situations and in accordance with the processes described:
   a. Promptly, and in any event within one business day of termination of a Participating Entity's Participation Agreement with OHA;
   b. Immediately following an Authorized User's failure to comply with the Authorized User Agreement, including an Adverse Security Event; or
   c. Immediately, and in any event within one business day, of termination of an Authorized User's employment or affiliation with the Participating Entity.
   d. Participating Entity shall notify OHA immediately upon termination of an Authorized User's access to the System due to an Adverse Security Event.

## Section 8: Audit

1. This section relates to OHA's ability to audit Participating Entities' use of CQMR System and Services. In addition, Quality Reporting Programs may have additional audit standards, such as standards related to data quality and completeness. Nothing in these Policies and Procedures is intended to alter or displace any audit provisions established by the Quality Reporting Programs.
2. **Purpose**. Audits are useful oversight tools for recording and examining access to information through the CQMR System (e.g., who accessed what data and when) and are necessary for verifying compliance with access controls, developed to prevent/limit inappropriate access to information. Participating Entity shall follow the minimum requirements for audits set forth in this Section regarding access to CQM Data via the System.
3. **Compliance Audits**. OHA (or a third party engaged by OHA) may audit Participating Entity on a periodic basis. The purpose of the audits will be to confirm compliance and proper use of the System in accordance with this Agreement and these Policies and Procedures.
4. **Conduct of Audits**. Audits will take place during normal business hours and at agreed upon times, and will be limited to such records, personnel and other resources of Participating Entity as are necessary to determine proper use of the System, compliance with this Agreement, including the Policies and Procedures, and compliance with applicable state and federal requirements. Each party will bear its own expenses relating to such audits. OHA will conduct any audit in a manner designed to reasonably minimize interference with Participating Entity's day-to-day operations.

## Section 9: Adverse Security Events

This section sets forth minimum standards that must be followed in the event of a Adverse Security Event. These standards are designed to promote accountability, assure all parties' commitment to privacy and security, and mitigate any harms.

1. **Notification**. As soon as reasonably practicable, but no later than five (5) business days after determining that an Adverse Security Event has occurred and is likely to have an adverse impact on the CQMR System or another entity or individual, Participating Entity shall notify in writing OHA and all participating entities that are likely impacted by the Adverse Security Event. Participating Entity shall supplement the information contained in the notification as additional information becomes available, and shall cooperate with OHA, other government oversight entities, OHA vendors, and other participating entities. The notification must not include any PHI. The notification should include sufficient information for OHA and affected participating entities to understand the nature of the Adverse Security Event. For instance, such notification could include, to the extent available at the time of the notification, the following information:
    a. One or two sentence description of the Adverse Security Event.
    b. Description of the roles of the people involved in the Adverse Security Event (e.g. employees, Authorized Users, service providers, unauthorized persons, etc.).
    c. The type of data involved in the Adverse Security Event.
    d. Participating entity or entities likely impacted by the Adverse Security Event.
    e. Number of individuals or records impacted/estimated to be impacted by the Adverse Security Event.
    f. Actions taken by the Participating Entity to mitigate any unauthorized access to, use or disclosure of PHI as a result of the Adverse Security Event.
    g. Current status of the Adverse Security Event (whether the event is under investigation or resolved).
    h. Corrective action taken and steps planned to be taken to prevent any similar Adverse Security Event.
2. **Use of Summaries**. If, on the basis of the notification, OHA determines that (i) other participating entities that have not been notified of the Adverse Security Event would benefit from a summary of the notification or (ii) a summary of the notification to the other participating entities would enhance privacy and security practices, then OHA may provide, in a timely manner, a summary to additional participating entities. Such a summary will not identify any of the participating entities or individuals involved in the Adverse Security Event.
3. Nothing in these Policies and Procedures supersedes an obligation (if any) under applicable law.

4. Compliance with these Policies and Procedures does not relieve Participating Entity of any other security incident or Adverse Security Event reporting requirements under applicable law including, but not limited to, HIPAA or laws related to consumers.
5. **Responsibilities of OHA**. In the event that OHA becomes aware of any Adverse Security Event, OHA will:
    a. Notify any Participating Entities whose data is affected by the Adverse Security Event.
    b. In the most expedient time possible and without unreasonable delay, investigate (or require the applicable Participating Entity to investigate) the scope and magnitude of such actual or suspected Adverse Security Event, and identify the root cause of the Adverse Security Event.
    c. Mitigate (or require the applicable Participating Entity to mitigate) to the extent practicable, any harmful effect of such Adverse Security Event that is known to OHA or the applicable Participating Entity. Mitigation efforts will correspond with and be dependent upon internal risk analyses.
    d. Notify the affected Participating Entity(ies) and any applicable regulatory agencies as required by and in accordance with applicable federal, state and local laws and regulations.
6. **Responsibility of Authorized User.** In the event that an Authorized User becomes aware of any Adverse Security Event, the Authorized User shall immediately notify the Organization Administrator of the Authorized User's Participating Entity.

## Section 10: Process for Amending the Policies and Procedures

OHA may implement new Policies and Procedures, or amend, or repeal and replace any existing Policies and Procedures, at any time by providing Participating Entity with notice of the change at least thirty (30) calendar days prior to the effective date of the change. Within fifteen (15) calendar days of receiving notice of the change, a Participating Entity may request that OHA delay implementation of the change based on unforeseen complications or other good cause. OHA will respond to a request to delay implementation within seven (7) calendar days of receiving the request unless OHA determines, in its sole discretion, that a longer response period is necessary. Continued use of the System by Participating Entity after the effective date of a change of the Policies and Procedures constitutes acceptance of such Policies and Procedures.

Participating Entity shall inform its Authorized Users of changes to the Policies and Procedures. An Authorized User has the responsibility to review changes to the Policies and Procedures upon receiving notice of the change from Participating Entity. Continued use of the System by an Authorized User after the effective date of a change of the Policies and Procedures constitutes acceptance of such Policies and Procedures.