Oregon Clinical *Quality* Metrics Registry
Sponsored by the Oregon Health Authority

Oregon Health Authority

CQMR Implementation Guide

Contents

INTRODUCTION

The purpose of this implementation guide is to describe how end users connect to, submit data to, and access the Oregon Clinical Quality Metrics Registry (CQMR). This document is targeted toward technical analysts and onboarding coordinators representing providers, practices, or organizations that will be submitting data to the CQMR.

The CQMR is a centralized system to submit and view quality measure information. For 2019 reporting, the CQMR supports

- Oregon Medicaid EHR Incentive Program electronic clinical quality measures (eCQMs),
- Merit-Based Incentive Payment System (MIPS) eCQMs,
- Comprehensive Primary Care Plus (CPC +) eCQMs, and
- Coordinated Care Organization (CCO) eCQMs and home-grown EHR-based measures (smoking prevalence and SBIRT).

Figure 1 below illustrates the CQMR concept and data flows. The CQMR architecture lies on the Salesforce and Amazon Web Service (AWS) platforms to deliver a scalable cloud based technology.

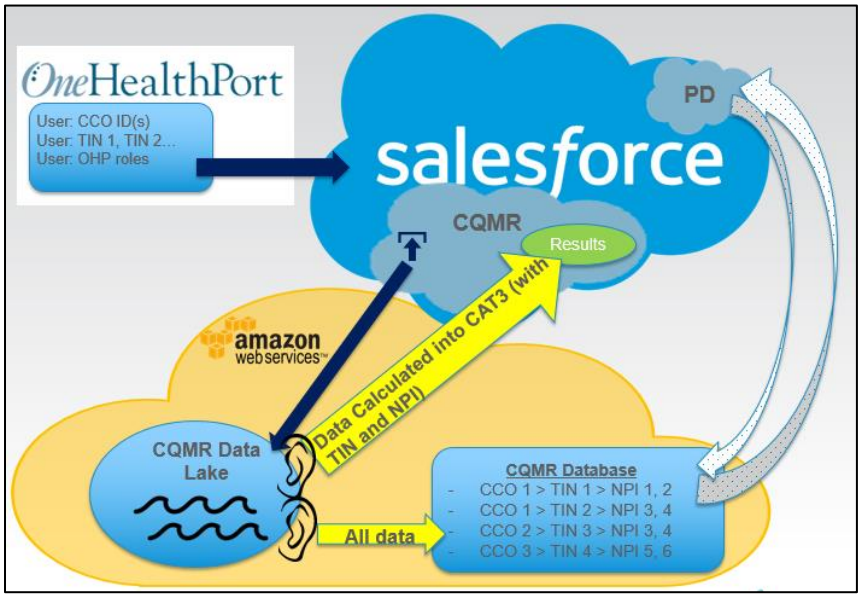


Figure 1 CQMR Concept

ONBOARDING TO THE CQMR

Legal Agreements

CQMR users must complete onboarding. For organizations, onboarding requires a fully executed Organizational Participation Agreement with the Oregon Health Authority, as well as the Michigan Health Information Network Shared Services (MiHIN) Terms of Service (ToS) and Business Associate Agreement (BAA). Once an organization has completed the contracts portion of onboarding, OHA will send MiHIN the organization's name and Tax Identification Number (TIN), as provided by the organization on the signature page of the Participation Agreement and used by the organization for OneHealthPort registration, so the organization can be added to the approved list to access the CQMR.

After a user completes the OneHealthPort signup and verification process, they may access the CQMR through OneHealthPort single sign-on (SSO). The CQMR system will check the user's organization TIN against the approved TIN list provided by OHA.

If the user's organization is not on the approved TIN list, a splash page will appear upon attempted login redirecting the user to the OHA CQMR onboarding website. The organization will need to complete onboarding with OHA before users access the CQMR.

If the user's organization is on the approved TIN list, the user will be prompted to electronically sign the OHA Authorized User Agreement and the MiHIN ToS on their own behalf. After electronically

signing those agreements, the user will enter the CQMR portal. The user will need to sign the agreements only once; they will not be prompted to sign again upon subsequent logins.

Onboarding – Account Setup

User registration and role-based access to the CQMR is provided via OneHealthPort. OneHealthPort does not provide any additional CQMR features or functions beyond user authorization and access to the CQMR solution. The following sections describe OneHealthPort onboarding requirements and processes for end users to access the CQMR.

OneHealthPort Single Sign-On

Access to the CQMR is granted through OneHealthPort. OneHealthPort provides Single Sign-on (SSO) capability to CQMR end users, including those who already have an account for OneHealthPort's other services. It also provides Identity Verification and Multi-Factor Authentication (MFA) options.

To access the CQMR, users must use one of the two MFA options:

- Use of Google Authenticator application, available for use on iOS and Android devices. If selected, an email is sent to the user with instructions on how to download, install, and set up the application. When launched, the Google Authenticator application will randomly generate an alphanumeric sequence to be entered for authentication.
- The use of a One Time Password (OTP). If selected, an email is sent to the user with a single use password (password can be any randomly generated alphanumeric sequence) to use for authentication.

OneHealthPort User Account Setup

OneHealthPort has provided a step-by-step setup guide to create subscriber accounts within OneHealthPort as applicable to the Oregon CQMR system. Each organization must designate at least one user account as an administrator within OneHealthPort; the administrator role then has the ability to add, manage, and update subscriber (individual end user) accounts within OneHealthPort. Additional resources and FAQs are available on OneHealthPort's website and technical support is available from the OneHealthPort Help Desk.

OneHealthPort Roles and Permission Sets

User roles, organizational affiliations, and permission sets are assigned in OneHealthPort. These session attributes are passed to the CQMR through a Security Assertion Markup Language (SAML) 2.0 connection upon login. The CQMR allows end users to access data and functionality of the CQMR only as authorized by the account role and affiliation information passed by OneHealthPort.

- Each organization's OneHealthPort administrator will assign one of four standard roles to the organization's CQMR users. Roles that do not include at least one of the four indicated OneHealthPort roles will not be granted access to the solution.
- Organization administrators are identified through data attributes passed from OneHealthPort to the CQMR that trigger the organization administrator permission set to be added to that individual's user account.
- Tax Identification Number (TIN) is the unique identifier that provides user affiliation and access to organizational information.
- OneHealthPort roles are mapped to CQMR functions in Table 1 below. Please review CQMR Training Materials for more information on CQMR roles and affiliations.

Table 1 CQMR Role Mapping

OneHealthPort Role	Definition/Permission Sets*
Quality Reports and Data Entry + OneHealthPort Administrator	**Submit** patient-level and aggregated data, **View** patient-level and aggregated data, Export data. For CCO users, **submit** data proposal and data submission to OHA. Administrator permissions in OneHealthPort.
Quality Reports and Data Entry	**Submit** patient-level and aggregated data, **View** patient-level and aggregated data, Export data.
Quality Manager	**View** patient-level and aggregated data. Export data.
Quality Reports (View Only)	**View** aggregated data. Export data.

** Users can only view the data of the organization(s) for which they have a TIN association.*

END USER TECHNICAL ONBOARDING PROCESS

Transport Mechanism Onboarding

Additional technical onboarding support is needed if users choose to submit data via Secure File Transport Protocol (SFTP), Application Programming Interface (API), and Direct Secure Message (DSM) transport methods, as described below. Technical onboarding support is not required to use the Web Upload option in the CQMR. Once other onboarding (including legal agreements) is complete, users may use the Web Upload as described in the CQMR Training Materials.

All traffic inbound to CQMR is required to be TLS v1.2 or higher. The CQMR solution provides encryption of data at rest and in motion via native encryption (AES 256) within the Salesforce platform. CQMR does not accept any protocol of lower versions.

Secure File Transport Protocol (SFTP)

Secure File Transfer Protocol (SFTP) is a network protocol for secure data transfer via a Secure Shell (SSH) data stream connection.

Onboarding

If an organization chooses to submit files through SFTP, a representative user in a Quality Reports and Data Entry (QRDE) role for that organization will submit a ticket via the CQMR user interface. To submit an SFTP ticket:

1. Log into OneHealthPort, navigate to the CQMR Portal, and click on the "SFTP Transport Request" option in the "Support" tab drop-down menu.
2. Click "Initiate SFTP onboarding".
3. Fill out the required ticket fields, including contact phone number and a description of the request.
4. Click "Confirm" to submit the ticket.
    a. Once submitted, ticket status and progress can be viewed in the "My Profile" section of the user account.

User information, including user name and email address, will be collected from the user's account upon form submission. When an onboarding coordinator receives the SFTP initiation ticket, they will contact the user to coordinate a kick-off call, during which the onboarding coordinator will gather the required intake items for SFTP onboarding, including provide the user an SFTP request form to be completed. A sample SFTP Request Form is available in Appendix A.

Using the information provided on the SFTP Request Form, the CQMR infrastructure team initiates the SFTP internal account setup process.

Authentication and Testing

SFTP access requests must begin from an authenticated CQMR account. No further authentication or testing is required for SFTP.

Implementation

Once an SFTP account has been created for the user, the CQMR onboarding team emails the user a confirmation of account setup. The username and port for the SFTP account are included in the confirmation email. A password for the account will be texted to the user.

At this point, the user may take action to send files to the CQMR via SFTP for quality reporting using the provided credentials. Users sending files through SFTP should work with their infrastructure department to determine the SFTP tool their entity will use.

To submit files via SFTP:

1. Log into the provided SFTP account
2. Use an SFTP tool to drag and drop files into the provided secure location

When an SFTP file submission is received, the file will be automatically loaded into the CQMR database and validated for conformance and acceptance by the schematron. A confirmation email detailing the validation status of the file will be returned to the practice or file owner associated with the SFTP account. Details regarding the acceptance or rejection of the file will be included in the email. For more information on file submission status and notifications, please see the CQMR Training Materials.

Note that a user can send more than one file if each file is for a separate data submission. However, if **multiples of the same file are sent for a single submission (based on file name), only the last file received will be used.**

Application Programming Interface (API)

Application Programming Interfaces (APIs) allow unrelated programs to communicate with the CQMR system. The CQMR currently supports Representational State Transfer (REST) APIs. REST APIs can return formats such as XML, JSON, and YAML for transactional record update as well as data retrieval.

Onboarding

If an organization chooses to submit files through API, a representative user in a Quality Reports and Data Entry (QRDE) role for that organization will submit a ticket via the CQMR user interface.

To submit an API ticket:

1. Log into OneHealthPort, navigate to the CQMR Portal, and click on the “API Transport Request” option in the “Support” tab drop-down menu.
2. Click “Initiate API onboarding.”
3. Fill out the required ticket fields, including contact phone number and a description of the request.
4. Click “Confirm” to submit the ticket.
    a. Once submitted, ticket status and progress can be viewed in the “My Profile” section of the user account.

User information, including user name and email address, will be collected from the user's account upon form submission. When an onboarding coordinator receives the API initiation ticket, they will contact the user to coordinate a kick-off call, during which the onboarding coordinator will gather the required intake items for API onboarding, including a Virtual Private Network (VPN) setup form. A sample VPN form is available in Appendix B. Using the information provided by the VPN form, the CQMR onboarding team initiates the internal API onboarding process.

Authentication and Testing

Authentication:

API access requests must begin from an authenticated CQMR account.

The CQMR infrastructure team will create OAuth user credentials and VPN user credentials for the onboarded entity and provide these credentials to the respective entity. The VPN and OAuth usernames will be provided via email. A password for each account will be texted to the user. Before calling the CQMR API, users must authenticate with the OAuth server to get a security token, which will be passed in subsequent requests. For background information about OAuth authentication, see the OAuth documentation at: https://oauth.net/2/.

Testing:

The CQMR onboarding team will coordinate a time to conduct connectivity testing with the user. Exchange of non-production messages to confirm connectivity is required before a user can submit data to the CQMR.

To conduct connectivity testing:

1. User transmits a test Excel or QRDA file to CQMR via REST API
    a. Every message must declare the content type to be application/json and be authenticated using the OAuth token.
2. An HTTP 200 OK response will post back to the user, indicating the API message has been accepted into the CQMR system. This response will include an ID that can be used to retrieve the status of the document.
3. The CQMR support team performs validations on the Excel or QRDA document received from the user
4. The user makes a second call to retrieve the status of the document.
    a. An HTTP 200 response will post back to the user with a JSON body that contains validation errors (if any), along with additional metadata.
    b. If any fields were missing from the message (i.e., document ID), a 301 response will post back to the user and indicate that the document could not be found.

Implementation

Once successful connectivity testing is complete, the user or entity may take action to send quality files to the CQMR via REST API for quality reporting.

To call the CQMR API:

- Include an HTTP method to indicate the desired action (GET/POST).
- Include the OAuth token in the header. This is required to authenticate the request.
- Declare the "Content-Type" to be "application/json".
- Include the Salesforce user ID in the "userID" field. This will be provided by the CQMR Salesforce team.

The API endpoints are described in an additional API-specific documentation provided upon onboarding, see Appendix B – Sample VPN Form for API.

The submitted file will be automatically loaded into the CQMR database and validated for conformance with accepted schematron.

For each quality file submitted through the API, an email with the validation status of the submitted file will be sent to the user associated with the "userID" included in the header of the API submission request. Additionally, API users may manually retrieve the validation status of a submitted file, immediately after the file submission, by sending a CQMR API validation status request as shown in Figure 4. Manual API validation status requests returns the status of the API user's most recently submitted data file. The CQMR API will post back to the user an HTTP 200 response with a JSON body that contains validation errors (if any), along with additional metadata. If any fields were missing from validation status request (i.e., document ID), an HTTP 301 response will post back to the user and indicate that the document could not be found.

If a replacement quality data file is submitted for a previously submitted data file, the data in the replacement file will supersede the data in the previous data file. The CQMR will match incoming eCQM data files to previously submitted eCQM data files on the practice TIN and/or provider TIN/NPI.

Sample API calls are shown in Figures 2, 3 and 4 below. Figure 2 shows the CQMR API request for an OAuth2 token to be included in API requests. This OAuth2 token is valid for approximately 30 minutes, after which a new token must be acquired and used in requests. Figure 3 shows the CQMR API request to submit a quality data file and Figure 4 shows the corresponding manual CQMR API request for the validation status of the submitted file.

Specification

POST -u <ClientID>:<clientSecret> --url https://prod.oregon-ha.org/mihin/mud/o/token/ --header header 'content-type: multipart/form-data; boundary=----WebKitFormBoundary7MA4YWxkTrZu0gW' --form grant_type=password --form username=<OAuth2 user> --form 'password=<OAuth2 user Password>'

Sample

curl --request POST -u <clientID>:<clientSecret> --url https://prod.oregon-ha.org .mihin.net/mihin/mud/o/token/ --header 'content-type: multipart/form-data; boundary=----WebKitFormBoundary7MA4YWxkTrZu0gW' --form grant_type=password --form username=<OAuth2 user> --form 'password=<OAuth2 user Password>'

Response:

{"access_token": "E9cwM10mqHwR4fawiEFGg2lLeHJ6JO", "expires_in": 36000, "token_type": "Bearer", "scope": "groups read write", "refresh_token": "tUOD5HfQ9fNr5k4K15f3VnlcD9ip2p"}

*This is the token to use

Figure 2 Sample CQMR API OAuth2 Token Request

Specifications:

POST https://prod.oregon-ha.org/mihin/skyoregon/api/doc_upload

OAuth2 Token required in header.

POST DATA as "application/json":

"doc_type": "<string>",
"file_name": "<filename string>",
"userID": "<SF UserID String>",
"file_data": "<base64 encoded file data>"

Example:

```
curl -X POST \
 https://prod.oregon-ha.org.mihin.net/mihin/skyoregon/api/doc_upload \
 -H 'Cache-Control: no-cache' \
 -H 'Content-Type: application/json' \
 -H 'Authorization: bearer 037f4bf3-116a-4d79-a8bc-076f968b6e15' \
 -d '{
        "doc_type": "data-sub-csv",
        "file_name": "Master_CCO_data_submissions.csv",
        "userID": "005n0000002jJEQAA2",
        "file_data": "Q0NPIFRJTixDQ08sT3JnYW5pemF0aW9uIFRJTixPcmdhbmI6YXRpb24gTmFtZ
}'
```

Response:

```
{
"doc_id": "jIPqBXt8D1Hu",
"bundle_id": "ar3oi4g"
}
```

Figure 3 Sample CQMR API Quality File Submission Request

Specifications:

GET https://prod.oregon-ha.org/mihin/skyoregon/api/doc_status/<bundle>-<transactionId>--

Example

curl --request GET --url https://prod.oregon-ha.org/mihin/skyoregon/api/doc_status/ar3oi4gj-jlPqBXt8D1Hu --header "Authorization: Bearer tdw2jkIaqS9UcYbZymZWm9SH9sW3vP"

RESPONSE:


```
{
   "transactionId": "jlPqBXt8D1Hu",
   "bundle": "ar3oi4gj",
   "document": "data-prop/2018/10/24/data-prop-10_24_2018_wLgEBah.csv",
   "doc_removed": "",
   "doc_removed_ts": null,
   "user": 9,
   "org": null,
   "org_name": null,
   "doc_type": 11,
   "completed": "2018-10-24T15:12:33.068Z",
   "failed": false,
   "error": null,
   "cur_step": 3,
   "status": "Validated",
   "msg": "",
   "deleted": null,
   "datasource": ""
}
```


Figure 1 Sample CQMR API Validation Status Request

Direct Secure Message (DSM)

Direct Secure Messaging (DSM) is a national encryption standard that utilizes a secure email type of communication to electronically transport healthcare data. A Direct Secure Messaging address is similar to a typical email address and can be issued to an individual, organization, or system, but all addresses must have a primary owner.

Onboarding

If an organization chooses to submit files through DSM, a representative user in a Quality Report and Data Entry (QRDE) role for that organization will submit a form via the CQMR user interface.

To submit a DSM form:

1. Log into OneHealthPort, navigate to the CQMR Portal, and click on the “DSM Transport Request” option in the “Support” tab drop-down menu.
2. Click “Initiate DSM onboarding.”

3. Enter the DSM address to be whitelisted.
4. Click "Confirm" to submit the form.

User information, including user name and email address will be collected from the user's account upon form submission. Once the requested DSM address is submitted, there is no further formal onboarding process for users to submit files through DSM.

Authentication and Testing

DSM access requests must begin from an authenticated CQMR account. When a CQMR user submits the DSM onboarding form with the requested DSM address to be whitelisted, an entry is automatically created on the list of whitelisted addresses for the CQMR. No further authentication or testing is required for DSM.

Implementation

Once a user's DSM address is whitelisted, the user will receive a confirmation email informing them that their DSM address has been whitelisted and is now approved to send files to the CQMR for quality reporting. The confirmation email will include the DSM addresses to send data to for each quality program supported by the CQMR.

At this point, the user or entity may take action to send quality files to the CQMR via DSM for quality reporting using their preferred DSM tool. When sending a file via DSM, include the file as an attachment to the message.

When a DSM file submission is received by the CQMR, the sending address will be checked against the list of whitelisted addresses. If the sending address is confirmed whitelisted, the CQMR receiving address will accept the file submission. The file will be automatically loaded into the CQMR database and validated for conformance and acceptance by the schematron. A confirmation email detailing the validation status of the file will be returned to the submitting DSM address. Details regarding the acceptance or rejection of the file will be included in the email. For more information, please see the CQMR Training Materials.

If the sending address is not whitelisted, the file will be rejected.

Note that a user can send more than one file if each file is for a separate data submission. However, if multiples of the same file are sent for a single submission (based on file name), the last file received will be used.

CPC + AND MIPS ONBOARDING

In addition to the CQMR onboarding described above, CQMR users reporting eCQMs to CMS for CPC+ or MIPS must also complete program-specific onboarding before submitting data for these programs.

Onboarding

If an organization wishes to use the CQMR to submitting eCQM data to CMS for CPC + or MIPS, a representative user in a Quality Report and Data Entry (QRDE) role for that organization will submit a ticket via the CQMR user interface. The onboarding user should be the user who will be submitting data to the CQMR for the respective program. **For 2019 reporting, tickets to initiate CPC+ onboarding must be submitted by January 31, 2020, and tickets to initiate MIPS onboarding, by March 9, 2020**.

To submit a CPC + and MIPS onboarding initiation ticket:

1. Log into OneHealthPort, navigate to the CQMR Portal, and click on the "CPC + / MIPS Onboarding" option in the "Support" tab drop-down menu.
2. Click "Initiate CPC+/MIPS".
3. Fill out the required ticket fields, including contact phone number and a description of the request.
4. Click "Confirm" to submit the ticket.
    a. Once submitted, ticket status and progress can be viewed in the "My Profile" section of the user account.

User information, including user name and email address, will be collected from the user's account upon form submission. When an onboarding coordinator receives the CPC + / MIPS initiation ticket, they will contact the user to coordinate a kick-off call, during which the onboarding coordinator provides instructions, next steps, and an estimated timeline for onboarding.

For CPC +, the user must authorize MiHIN as a data intermediary for that organization's CPC + reporting. Authorization occurs on the Center for Medicare and Medicaid Services (CMS) website. The MiHIN CQMR team will work with the user on how to complete the authorization.

The CQMR team will grant access to the CPC + or MIPS file uploader within two business days of receiving all prerequisites requested during the onboarding kick-off call (and notification of authorization for CPC + users). A confirmation of successful onboarding will be emailed to the user.

Authentication and Testing

CPC + and MIPS program onboarding requests must begin from an authenticated CQMR account.

CPC + and MIPS files can be tested using the Web Upload test submission feature. This allows users to upload a file for validation without sending the file to a reporting program and will allow users to work with their EHR vendor if necessary to update the file. Please see the CQMR Training Materials for more information and instructions on the Test Submissions feature.

Implementation

Consistent with CMS reporting requirements, the CQMR system allows users to submit QRDA Category III files for CPC + and MIPS; these files may be submitted via DSM, SFTP, API, or web upload. Please see the CQMR Training Materials for more information on data submission options and other information on using the CQMR.

Note that for CPC + and MIPS, providers are required by Centers for Medicare and Medicaid Services (CMS) to adhere to most current CMS requirements for Certified EHR Technology (CEHRT) and QRDA Category III file submissions.

CONFIGURATION GUIDE

Account Management

Account management occurs within OneHealthPort. The OneHealthPort administrator for an organization is responsible for user account management, including adding, managing, and updating subscriber (individual end user) accounts. See OneHealthPort User Account Setup for more information.

Security and Access

All technologies included in the CQMR system are located in a HITRUST-certified environment hosted in Amazon Web Services (AWS). This multi-layered security model consistently monitors and adjusts system performance, applies patches, security updates and service packs, and repairs/upgrades for the CQMR service. In addition, CQMR has robust security implementation, detection, and prevention mechanisms, which incorporate next generation firewalls, Web Application Firewalls (WAFs), and a zero trust architecture.

The hosting environment is Service Organization Controls 2 (SOC 2) and Federal Risk and Authorization Management Program (FedRAMP) certified. It is a highly secure environment that is compliant with industry security guidelines (ISO 27001, SSAE16/ISAE 3402 SOC-1, SOC-3, HIPAA, NIST). Lists of certifications can be found at the link provided below:
https://aws.amazon.com/compliance/programs/.

All system resources are continuously monitored using automated monitoring tools that provide - but are not limited to - the following services: system log analysis, file integrity monitoring, intrusion

prevention and detection, and anti-malware. AWS currently supports TLS 1.2 to protect data in transit, and utilizes role-based access control following the principle of least privilege. AWS security best practices, firewalls, VPN connections, and multi-factor authentication provide additional layers of security.

All software releases will be internally scanned for security vulnerabilities prior to promotion to the production environment. All transport methodologies listed in the transport mechanism section conform to secure encrypted protocol, ensuring data integrity.

Configuration Management

The CQMR Configuration Management (CM) process follows industry standards including interface management, role-based access, release changes, and version control. The Oregon HIT CM Plan can also be found in the Oregon HIT Program Management Plan (PMP). Through the use of populations and profile templates, user privileges can be administered at large scale. The configurable Salesforce platform adheres to this CM Plan for this project. Only CQMR administrators are permitted to configure Salesforce. All changes going into a release are tracked through the ticketing system.

Additional requests should be submitted through the CQMR ticketing system in the CQMR user interface or by emailing help@oregon-cqmr.org.

Configuration management is an essential part of system maintenance. It is aided with version control tools to control configuration versions (currently BitBucket for code and configuration version management) or patch management (OS dependent).

Release Management

The CQMR uses a system development life cycle (SDLC) for managing software releases. It includes configuring (agile), implementing, and retiring information systems through a multistep process from initiation, analysis, design, implementation, and maintenance to disposal. The CQMR system ensures appropriate protection for the information that the system will transmit, process, and store.

The CQMR reserves a monthly release window for security and performance releases. Monthly releases are aligned with CQMR sprint cycles. The CQMR reserves a weekly maintenance window for security patches and bug fixes which will also align with feature releases.

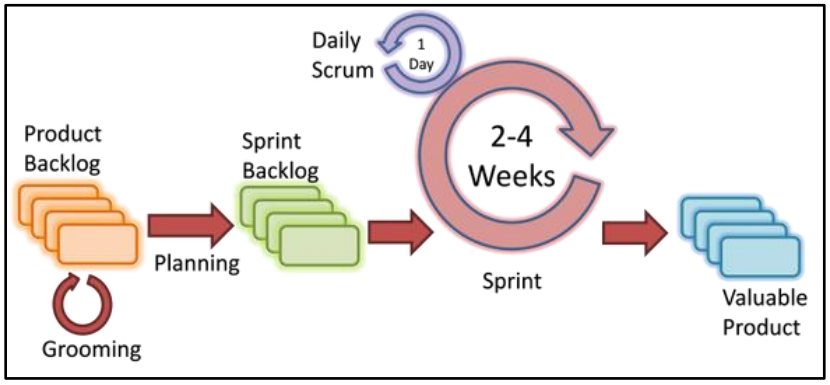


Figure 5 Software Release Process

If a change is needed, the request is entered through the Change Management process for the product. The CQMR support team ensures that testers and implementers have independent roles and user interface changes are encapsulated in "change sets" which isolates the change being promoted. As part of the Change Management process for the product, the change needs a rollback plan prior to approval for change to occur. All changes going into a release are reviewed by the development infrastructure team, a production and operations change panel, and finally by the CQMR Product Manager and or HIT Director.

The Oregon HIT CM Plan can be found in the Oregon HIT Program Management Plan (PMP).

TECHNICAL GUIDE

Data Specifications

Quality Reporting Document Architecture (QRDA) Category I

A QRDA Category I file contains individual patient quality results and thus contains Protected Health Information (PHI). For 2019 reporting, the CQMR will make dashboard available for users to review the contents of their QRDA I submissions without doing a formal submission to a program. The QRDA I tab of the CQMR portal will also be used for the CCO sample submission of QRDA I files.

For an overview of QRDA Category I files, visit the eCQM QRDA guide at the eCQM library hosted by the Centers for Medicare and Medicaid Services (CMS) at: https://ecqi.healthit.gov/qrda.

Category I file document structure and examples can be found on the HL7 website at: www.hl7.org.

Quality Reporting Document Architecture (QRDA) Category III

CQMR users may submit quality data to any of the supported quality programs using a QRDA Category III file. QRDA Category III files contain aggregate quality results and do not contain PHI.

For an overview of QRDA Category III files, visit the eCQM QRDA guide at the eCQM library hosted by CMS at: https://ecqi.healthit.gov/qrda.

Category III file document structure and examples can be found on the HL7 website at: www.hl7.org.

MEHRIP Excel Template

Medicaid Electronic Health Records Incentive Program (MEHRIP) eligible providers may submit quality data to the CQMR using the MEHRIP Excel Template. OHA provides this template on its website https://www.oregon.gov/oha/HPA/OHIT-MEHRIP/pages/index.aspx on the page for the applicable program year.

Follow the instructions provided in the OHA guidance document to understand how to correctly format the MEHRIP Excel Template and what information should be included in each field. Also reference the CQMR Training Materials.

CCO Excel Template

CCO incentive measures may be submitted to the CQMR using the CCO Excel Template.

Follow the instructions provided in the template to understand how to correctly format it and what information should be included in each field. Also reference the CQMR Training Materials.

Report Specifications

Report access is available for all CQMR end users. The CQMR user interface has a tab for viewing reports accessible from the CQMR home page. The standard list of reports available within the CQMR is outlined in Table 2 below:

Table 2 CQMR Standard Reports

Report	Data description

1. MEHRIP Operational report	• Organization-level view of providers who have submitted MEHRIP eCQM data
	• Tracks that eCQMs have been submitted for providers under the organization's TIN
	  ○ Filterable by reporting period
	  ○ Filterable by measure

2. MEHRIP Organizational Report	• Organization-level view of eCQM performance for providers who have submitted MEHRIP eCQM data • Provides view of the eCQM performance reported ○ Filterable by reporting period

	○ Filterable by measure ○ Stratification by organization or other payer, practice, practice physical location, provider, race, ethnicity, gender, and age (assuming QRDA Category 3 data was submitted)
3. CCO Operational Report	• CCO-level view of data submission status (whether data has been submitted for each organization, practice and provider listed in the CCO's data proposal)
4. CCO Organizational Report	• CCO-level view of the quality measure data reported • Filterable by organization, practice, provider, and reporting period • Filterable by measure selection
5. Dashboard views[1]	Available to organizations, clinics and providers • Organization provider performance grid • Inter-clinic performance grid • Intra-clinic provider performance grid • Provider performance by measure • Organization provider performance drill-down (includes Measure Performance Drilldown, Organization Performance Drilldown, Provider Performance) • Quality measure drill-down • eMeasure practice views • Provider Performance by Payer • Provider Performance by Demographic

Operational Reports

CQMR Operational Reports are standard reports that show the measure submission status of organizations, practices, and providers. Operational Reports are populated as soon as data is submitted

[1] For more information on dashboard views, including information on using the target configurator to set targets and caution margins to be displayed, please see the CQMR training materials.

by users. The data displayed in the reports is regularly updated to reflect the most current data submission information.

The MEHRIP Operational Report (Figure 6 below) shows the measure submission status of CQMR users reporting to the Medicaid EHR Incentive Program. Information within the report can be configured to view by: Reporting period, level of aggregation, CMS measure(s).

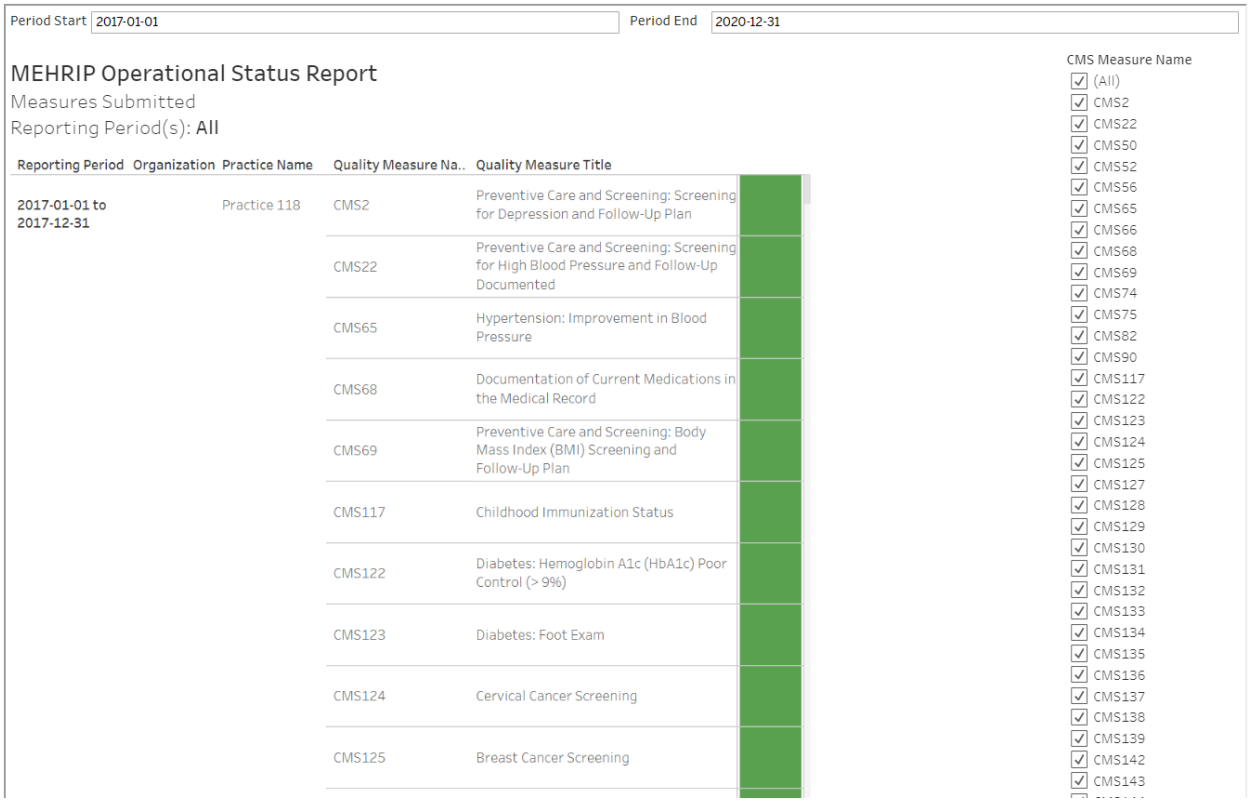


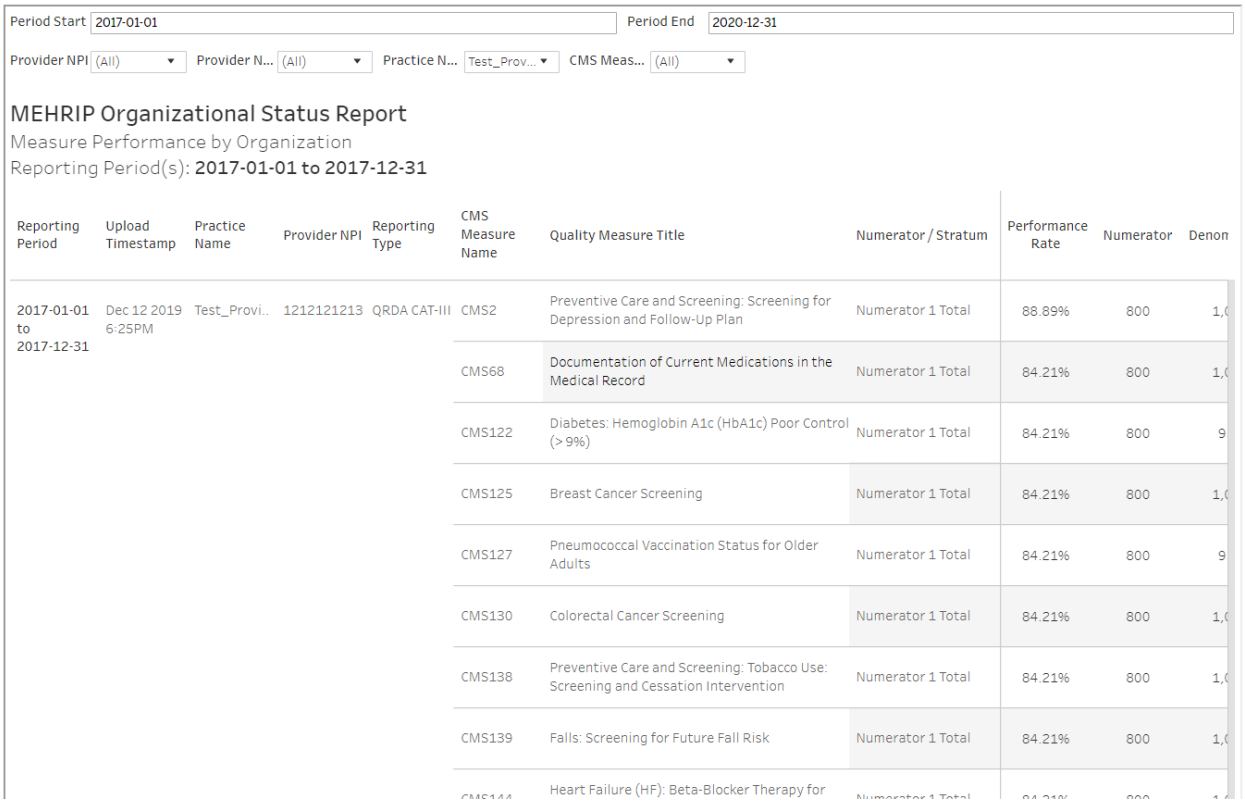
Figure 6 MEHRIP Operational Report

Organizational Reports

CQMR Organizational Reports are standard reports that show the measure performance details of organizations, practices, and providers. Organizational Reports are populated as soon as data is submitted by users. The data displayed in the reports is regularly updated to reflect the most current data submission information.

The MEHRIP Organizational Report (Figure 7 below) shows the measure performance details of CQMR users reporting to the MEHRIP. Information within the report can be filtered and configured to view

by: Reporting period, population, level of aggregation, organization(s), provider(s), and CMS measure(s).



Period Start 2017-01-01 Period End 2020-12-31

Provider NPI (All) Provider N... (All) Practice N... Test_Prov... CMS Meas... (All)

MEHRIP Organizational Status Report
Measure Performance by Organization
Reporting Period(s): 2017-01-01 to 2017-12-31

Reporting Period	Upload Timestamp	Practice Name	Provider NPI	Reporting Type	CMS Measure Name	Quality Measure Title	Numerator / Stratum	Performance Rate	Numerator	Denon
2017-01-01 to 2017-12-31	Dec 12 2019 6:25PM	Test_Provi..	1212121213	QRDA CAT-III	CMS2	Preventive Care and Screening: Screening for Depression and Follow-Up Plan	Numerator 1 Total	88.89%	800	1,(
					CMS68	Documentation of Current Medications in the Medical Record	Numerator 1 Total	84.21%	800	1,(
					CMS122	Diabetes: Hemoglobin A1c (HbA1c) Poor Control (> 9%)	Numerator 1 Total	84.21%	800	9
					CMS125	Breast Cancer Screening	Numerator 1 Total	84.21%	800	1,(
					CMS127	Pneumococcal Vaccination Status for Older Adults	Numerator 1 Total	84.21%	800	9
					CMS130	Colorectal Cancer Screening	Numerator 1 Total	84.21%	800	1,(
					CMS138	Preventive Care and Screening: Tobacco Use: Screening and Cessation Intervention	Numerator 1 Total	84.21%	800	1,(
					CMS139	Falls: Screening for Future Fall Risk	Numerator 1 Total	84.21%	800	1,(
					CMS144	Heart Failure (HF): Beta-Blocker Therapy for				

Figure 7 MEHRIP Organizational Report

Dashboards

Dashboards are pre-created but adjustable dynamic reports that illustrate the quality measure conformance information for organizations, practices, or providers. There are nine standard dashboard views, shown in Figures 8-14 below. See the CQMR Training Materials for more information on navigating and using each dashboard.

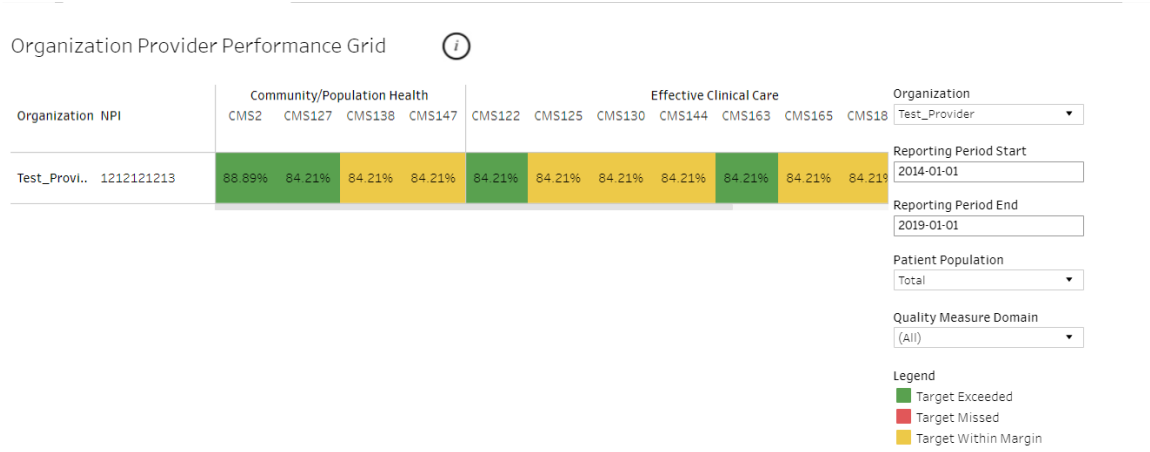


Figure 8 Organization Provider Performance Grid

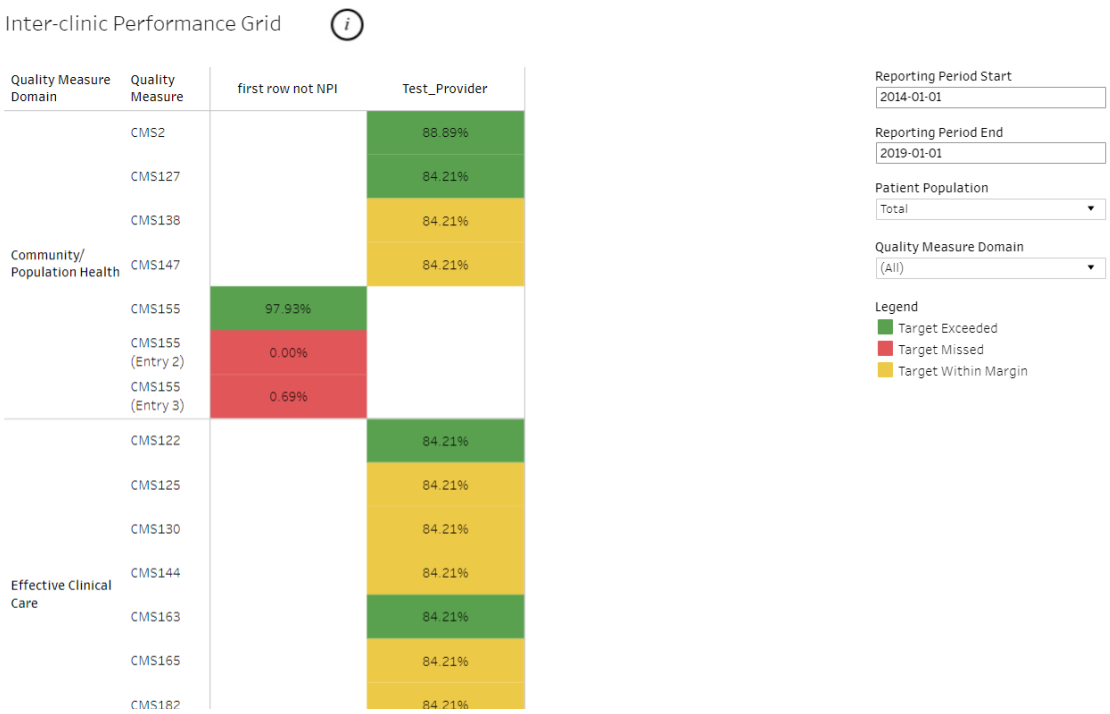


Figure 9 Inter-Clinic Performance Grid

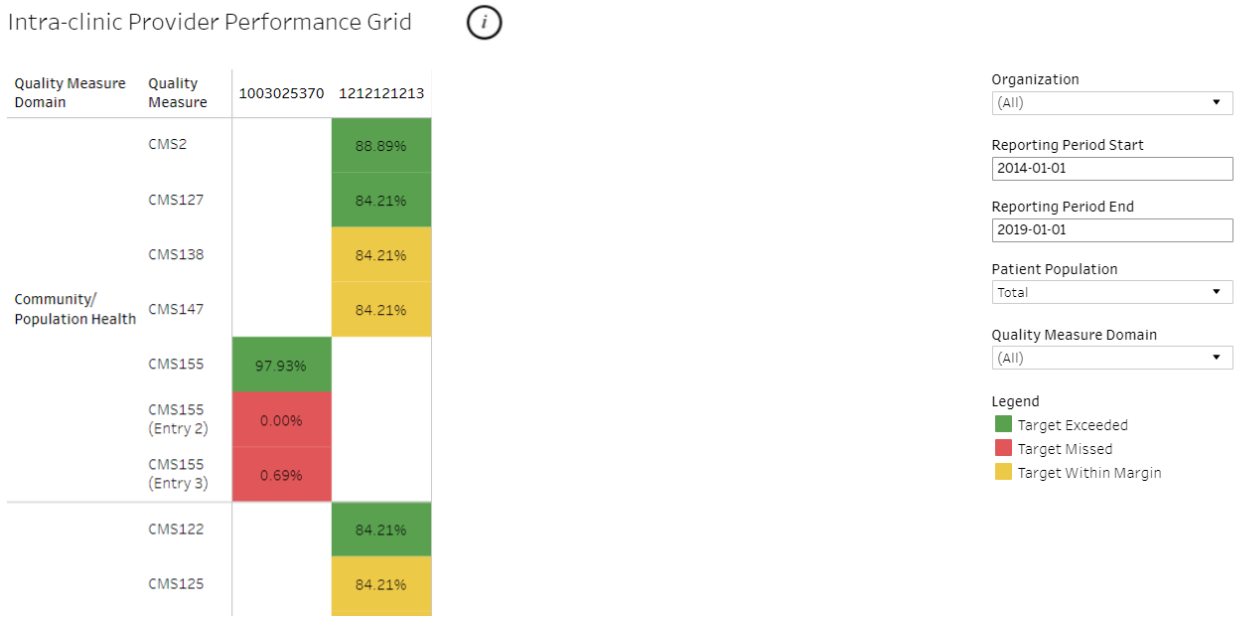


Figure 10 Intra-Clinic Provider Performance Grid

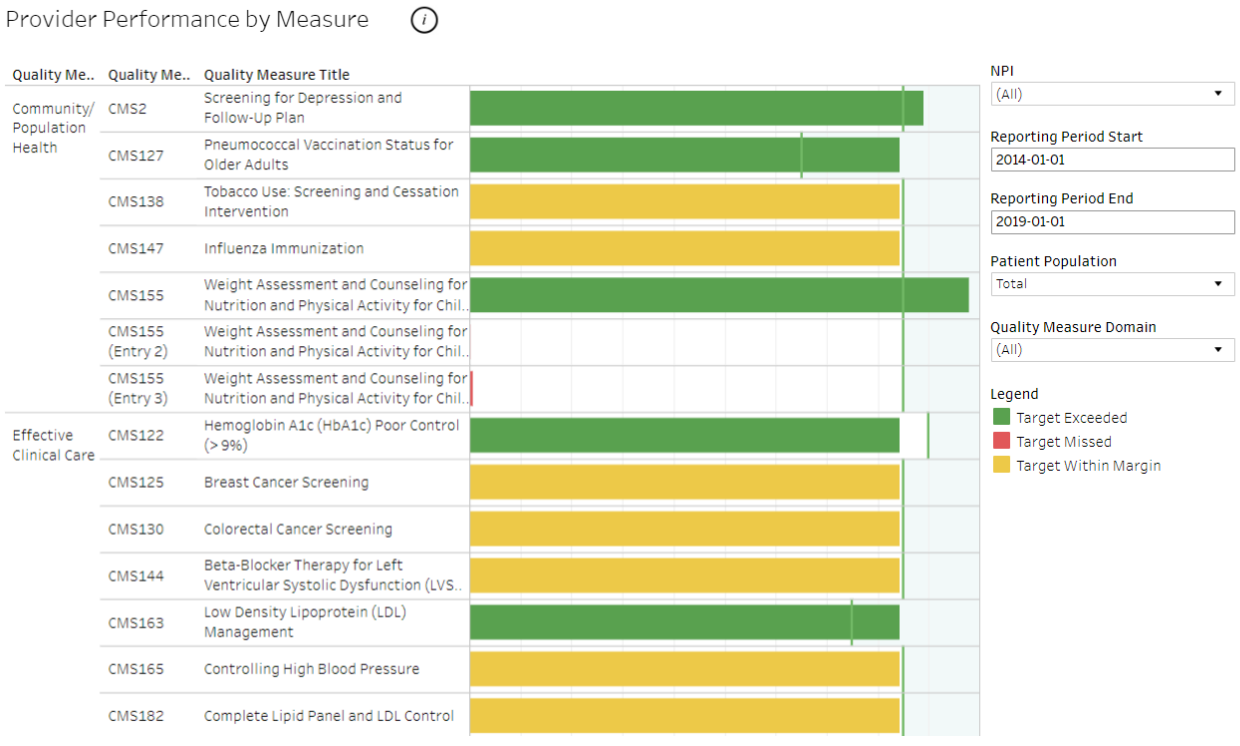


Figure 11 Provider Performance by Measure

Figure 12 Organization Provider Performance Drill-Down

(Includes Measure Performance Drill-down, Organization Performance Drill-down, Provider Performance)

Figure 13 Quality Measure Drill-down

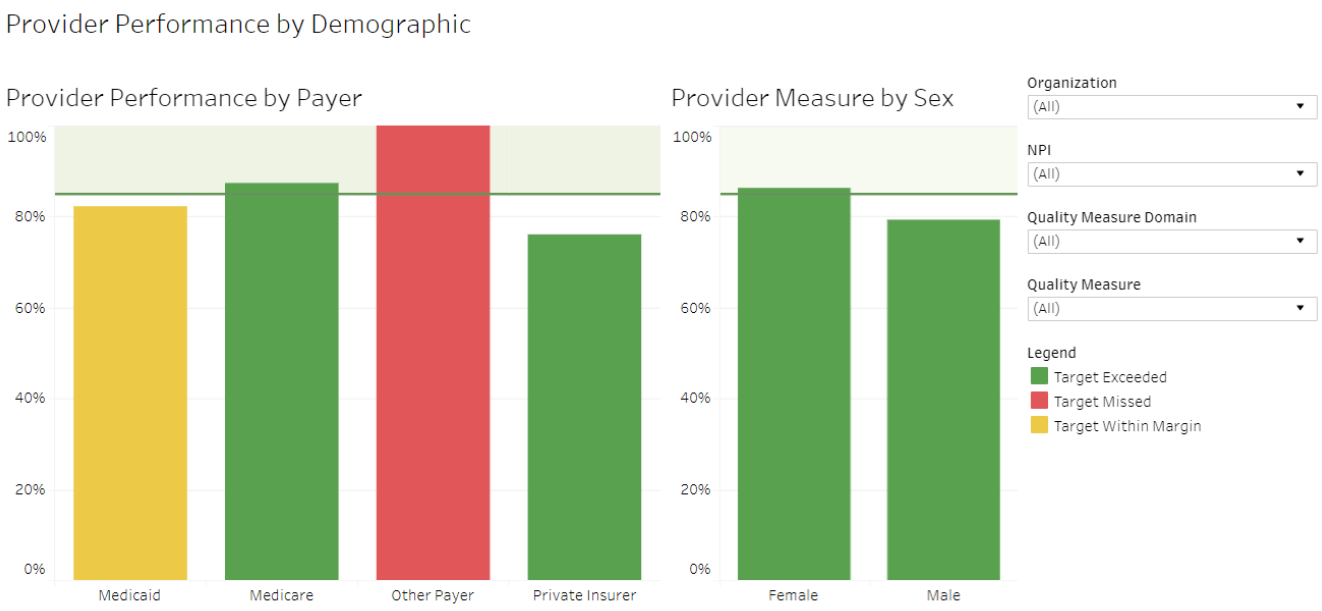


Figure 14 Provider Performance by Demographic

TEST DATA SUBMISSIONS

The CQMR solution allows users to upload a QRDA Category III quality file using the Web Upload and test its validation without sending the file to a reporting program. This will allow users to work with their EHR vendor if necessary to update the file. Please see the CQMR Training Materials for more information on the Test Submissions feature and instructions to submit a test file.

SUPPORT

All CQMR end users have access to support. If you are experiencing issues or need assistance with the CQMR portal, please contact the Oregon Help Desk by submitting a ticket through the user interface in the "Support" tab, by sending an email to help@oregon-cqmr.org, or by calling the Help Desk at: 1 (877) 285-1954.

APPENDIX A – SAMPLE SFTP REQUEST FORM

SAMPLE SFTP request form.pdf

APPENDIX B – SAMPLE VPN FORM FOR API

MiHIN Primary IPSec VPN Form.docx