RESOURCE AND PATIENT MANAGEMENT SYSTEM

Electronic Clinical Quality Measures Engine

(ECQM)

User Manual

Version 6.0 Patch 1
August 2024

Office of Information Technology
Division of Information Technology

Table of Contents

Preface

Electronic Clinical Quality Measures (eCQM) are not just standardized metrics; they are the backbone of our healthcare system, playing a pivotal role in measuring and tracking the quality of healthcare services provided by eligible clinicians (EC), eligible hospitals (EH), and critical access hospitals (CAH). The results of these measures are instrumental in calculating a quality score, a key indicator of our system's effectiveness. This process is vital in ensuring that our healthcare system consistently delivers effective, safe, efficient, patient-centered, equitable, and timely care.

eCQM performance rates are used by various governing bodies to evaluate programs, and in the case of Centers for Medicare & Medicaid Services (CMS), payments for Medicare services may be affected.

eCQMs measure many aspects of patient care, including:

- Patient and Family Engagement
- Patient Safety
- Care Coordination
- Population/Public Health
- Efficient Use of Healthcare Resources
- Clinical Process/Effectiveness

Indian Health Service Resource Patient Management System Certified Electronic Health Records generate patient-based files containing the data needed to create CQM reports in a standardized format. These are called Quality Reporting Data Architecture Category I (QRDA I) files.

The ECQM Engine is not just a tool; it's a comprehensive solution. As a browser-enabled graphical user interface for the Indian Health Service (IHS), it extracts data from multiple QRDA I files and generates QRDA Category III (QRDA III) aggregated report files that can be submitted to CMS. The ECQM Engine also produces human-readable reports that can be used in quality improvement activities at individual sites. With its robust and all-encompassing capabilities, the ECQM Engine is a reliable and powerful solution for your reporting needs.

1.0 Introduction

This User Manual provides information on how to use the Electronic Clinical Quality Measure Engine (namespace: ECQM) application.

1.1 eCQM Overview

eCQMs are a component of the ONC Certification Criteria for Health IT necessary for participating in various CMS programs.

Each year, CMS makes updates to the eCQMs approved for CMS programs to reflect changes in:

- Evidence-based medicine
- Code sets
- Measure logic

A total of 13 EH/CAH eCQMs, 2 EH/CAH Hybrids, and 28 EC eCQMs were selected and are listed in Table 1-1, Table 1-2, and Table 1-3.

Table 1-1: IHS–Selected EH/CAH eCQM

CMS ID	Measure Type	Measure
CMS009v11	Process	Exclusive Breast Milk Feeding
CMS071v12	Process	Anticoagulation Therapy for Atrial Fibrillation/Flutter
CMS072v11	Process	Antithrombotic Therapy By End of Hospital Day 2
CMS104v11	Process	Stroke-2 Ischemic stroke–Discharged on Anti-thrombotic Therapy
CMS105v11	Process	Discharged on Statin Medication
CMS108v11	Process	Venous Thromboembolism Prophylaxis
CMS111v11	Process	Median Admit Decision Time to ED Departure Time for Admitted Patients
CMS190v11	Process	Intensive Care Unit Venous Thromboembolism Prophylaxis
CMS506v5	Outcome	Cesarean Birth
CMS871v2	Process	Safe Use of Opioids-Concurrent Prescribing
CMS816v2	Outcome	Hospital Harm–Severe Hyperglycemia
CMS334v4	Outcome	Hospital Harm–Severe Hyperglycemia
CMS1028v1	Outcome	Severe Obstetric Complications

Table 1-2: IHS Selected EH/CAH Hybrid

CMS ID	Measure Type	Measure
CMS 529v3	Hybrid-Cohort Administrative	Core Clinical Data Elements for the Hybrid Hospital-Wide (All-Condition, All-Procedure) Risk-Standardized Mortality Measure (HWM)
CMS 844v3	Hybrid-Cohort Administrative	Core Clinical Data Elements for the Hybrid Hospital-Wide Readmission (HWR) Measure with Claims and Electronic Health Record Data

Table 1-3: IHS–Selected EC eCQMs

CMS ID	Measure Type	Measure
CMS002v12	Process	Screening for Depression and Follow-Up Plan
CSM022v11	Process	Screening for High Blood Pressure and Follow-up
CMS050v11	Process	Closing Referral Loop
CMS069v11	Process	Body Mass Index (BMI) Screening and Follow-Up Plan
CMS117v11	Process	Childhood Immunization Status
CMS122v11	Intermediate Clinical Outcome	Diabetes: Hemoglobin A1c (HbA1c) Poor Control (> 9%)
CMS124v11	Process	Cervical Cancer Screening
CMS125v11	Process	Breast Cancer Screening
CMS127v11	Process	Pneumococcal Vaccination Status for Older Adults
CMS130v11	Process	Colorectal Cancer Screening
CMS131v11	Process	Diabetes: Eye Exam
CMS134v10 (retired)	Process	Diabetes: Medical Attention for Nephropathy
CMS137v11	Process	Initiation and Engagement of Alcohol and Other Drug Dependence Treatment
CMS138v11	Process	Tobacco Use: Screening and Cessation Intervention
CMS139v11	Process	Screening for Future Fall Risk
CMS144v11	Process	Heart Failure: Beta-Blocker Therapy for Left Ventricular Systolic Dysfunction
CMS145 v11	Process	Coronary Artery Disease (CAD): Beta-Blocker Therapy-Prior Myocardial Infarction (MI) or Left Ventricular Systolic Dysfunction (LVEF <40%)
CMS147v12	Process	Influenza Immunization
CMS154v11	Process	CMS154v10 Appropriate Treatment for Upper Respiratory Infection (URI)
CMS155v11	Process	Weight Assessment and Counseling for Nutrition and Physical Activity for Children and Adolescents
CMS156v11	Process	Use of High-Risk Medications in Older Adults

CMS ID	Measure Type	Measure
CMS159v11	Outcome	Depression Remission at Twelve Months
CMS161v11	Process	Adult Major Depressive Disorder: Suicide Risk Assessment
CMS165v11	Intermediate Clinical Outcome	Controlling High Blood Pressure
CMS177v11	Process	Child and Adolescent Major Depressive Disorder: Suicide Risk Assessment
CMS347v6	Process	Statin Therapy for the Prevention and Treatment of Cardiovascular Disease
CMS349v5	Process	HIV Screening
CMS160v7 (retired)	Process	Depression Utilization of the PHQ-9 Tool

Note: The measure was not updated for 2023 and is not eligible to submit to CMS.

CMS134v10 uses logic from 2022.

CMS160v7 uses logic from 2019.

1.2 More Information

The following websites provide additional CQM information:

- CMS: https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/ClinicalQualityMeasures.html
- eCQI Resource Center: https://ecqi.healthit.gov/
- U.S. National Library of Medicine Value Set Authority Center: https://vsac.nlm.nih.gov/
- Agency for Healthcare Research and Quality: https://ushik.ahrq.gov/

2.0 ECQM Engine

The Electronic Clinical Quality Measure ECQM Engine is a Web application that receives QRDA I and generates QRDA III files. There are two versions of the ECQM Engine available. One version is a centralized service hosted out of the IHS/OIT Albuquerque Data Center for Federal Sites authenticating through the D1 and for Tribal/Urban Sites authenticating through D1/E1. The other version is a locally, site-installed application to be used by Tribal and Urban Sites authenticating through their directory server (LDAP).

Central installation eliminates the need for initial site installation and future patching. There will be no need to monitor the availability of new patches/versions and no need to provision new or occupy existing site server resources. On the other hand, a local site install does not need Tribal/Urban sites to review and enter into the legal agreement, including BAA and ISA. Sites do not need to worry about the risk of server/resource bandwidth constraints during the peak reporting times. Sites will have control of their system's availability, thus avoiding system outages and being in charge of their timetable.

The ECQM Engine receives securely transmitted QRDA I files in XML format for clinical quality measure calculations. It then authenticates users against a directory service with LDAP (Lightweight Directory Access Protocol), one example of which is Microsoft Active Directory. This authentication is necessary to support sites in various locations, including the Federal D1 network, the Tribal E1 network, and others outside the D1/E1 boundaries.

Access to the ECQM Engine features is dependent on the role assigned to the user. Table 2-1 Shows the roles available in the ECQM Engine.

Table 2-1: ECQM Engine Role Definition

ECQM Role	Definition
Super Admin	An individual who performs the following ECQM functions: • Install the Engine for the first time using D1/E1 credentials • Specify Super Auditor (other than self) • Create Site accounts • Specify Site Admin User • Specify Site Auditor (other than Site Admin User)
Super Auditor	An individual who tracks and monitors all activities performed

ECQM Role	Definition
Site Admin	An individual who performs the following ECQM functions: • Upload QRDA I zip files • Setup compute/reporting groups • Download reports/results • Manage provider lists • Delete/Purge data
Site Auditor	An individual who tracks and monitors site activities

2.1 Log In/Log Out

1. Open your internet browser (Google Chrome® Version 80 or higher) and type in the **IP address** of the server where the ECQM application has been installed (https://IPaddressOFecqmApplicationServer).

2. The **Login** screen displays.

Figure 2-1: ECQM Engine Login Screen

3. Enter your **User Name** and **Password**.

4. To log out, click the Logout () icon and select **Logout**.

2.2 Super Admin Menu Options

The Engine Super Admin installs the ECQM Engine for the first time using their D1/E1 credentials. The Super Admin creates sites and defines users in the system.

2.2.1 Sites

Use the **Sites** tab to define/modify site information. Only Super Admin users have access to create sites. The Super Admin creates each site with a distinct profile based on the information in the QRDA I file and the identifying information used to create the QRDA III files.

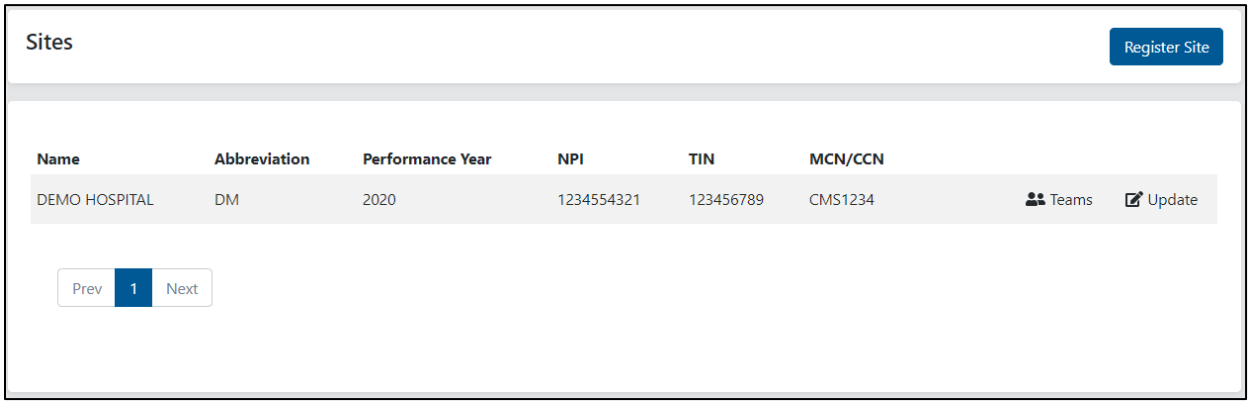


Figure 2-2: Sites screen

2.2.1.1 Create Site

1. Click the **Register Site** button to register a new site.

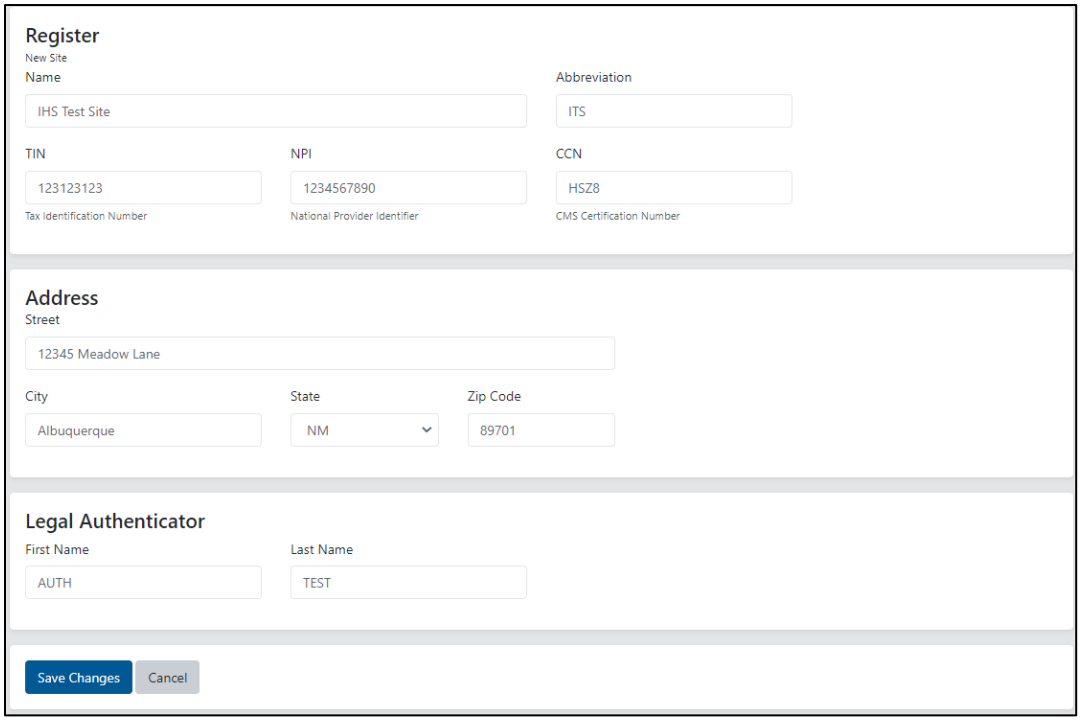


Figure 2-3: Register screen

2. On the **Register** screen, populate the following fields (all fields are required).

3. Under **New Site**:
    a. Enter a **Name** (maximum of 50 characters).
    b. Enter an **Abbreviation** (maximum of 3 characters).
    c. Enter a **TIN** (9-digit numeric, no dash required).
    d. Enter an **NPI** (10-digit numeric).
    e. Enter **CCN** (Certification Number).
4. Under **Address**:
    a. Enter a **Street**.
    b. Enter a **City**.
    c. Enter a **State**.
    d. Enter a **Zip Code** (5 or 9 digits).
5. Under **Legal Authentication**:
    a. Enter a **First Name**.
    b. Enter a **Last Name**.

> **Note**: The Legal Authenticator is the person associated with the QRDA submission. This could be the site's Quality Coordinator or Health Records Management officer. This is a required field.

6. Click **Save Changes**.
7. Click **Cancel** to exit the **Register** screen.

2.2.1.2 Modify Site

1. Click the **Update** button next to the site to update/modify the site information.

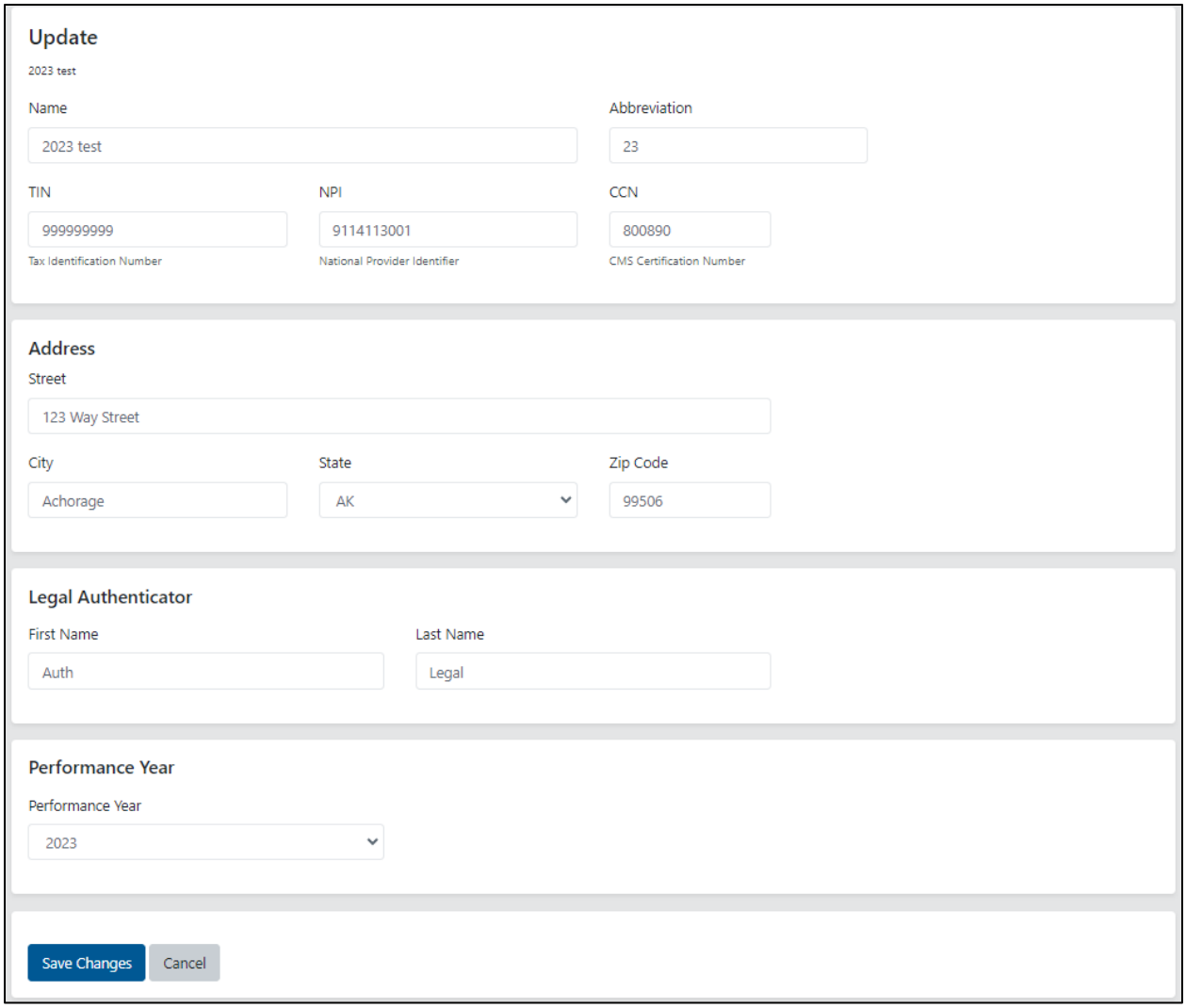


Figure 2-4: Update Site screen

2. Click the fields to update the site, address, and legal authenticator information on the **Update** screen.
3. Select the correct **Performance Year** based on the current reporting period.
4. Click **Save Changes** or click **Cancel** to discard any changes.

2.2.2 Users

Select the **Users** tab to create, modify, or deactivate users. Only Super Admin users can create user profiles, including other Super Admin users, Super Auditor users, Site Admin users, etc. Super Admin users cannot be Super Audit users. See Table 2-1 for the list of roles available.

2.2.2.1 Create User

Use the **Register User** button to create, modify, or deactivate a user.

1. Click the **Register User** button to create a user.

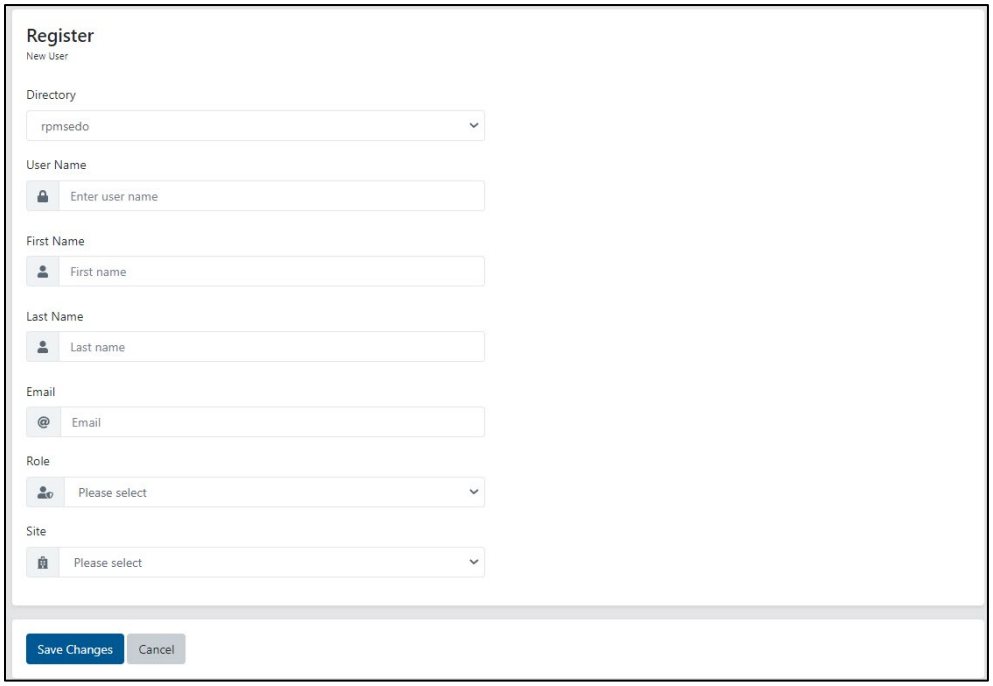


Figure 2-5: Register User screen

2. On the **Register** screen:
   a. Select **Directory** from the list (this is the server directory).
   b. Enter a **User Name**.
   c. Enter a **First Name**.
   d. Enter a **Last Name**.
   e. Enter an **Email**.
   f. Select a **Role**.
   g. Select **Site**.
3. Click **Save Changes**.
4. Click **Cancel** to discard all changes.

2.2.2.2 Modify User

1. Click the **Update** button next to a user to modify or update.

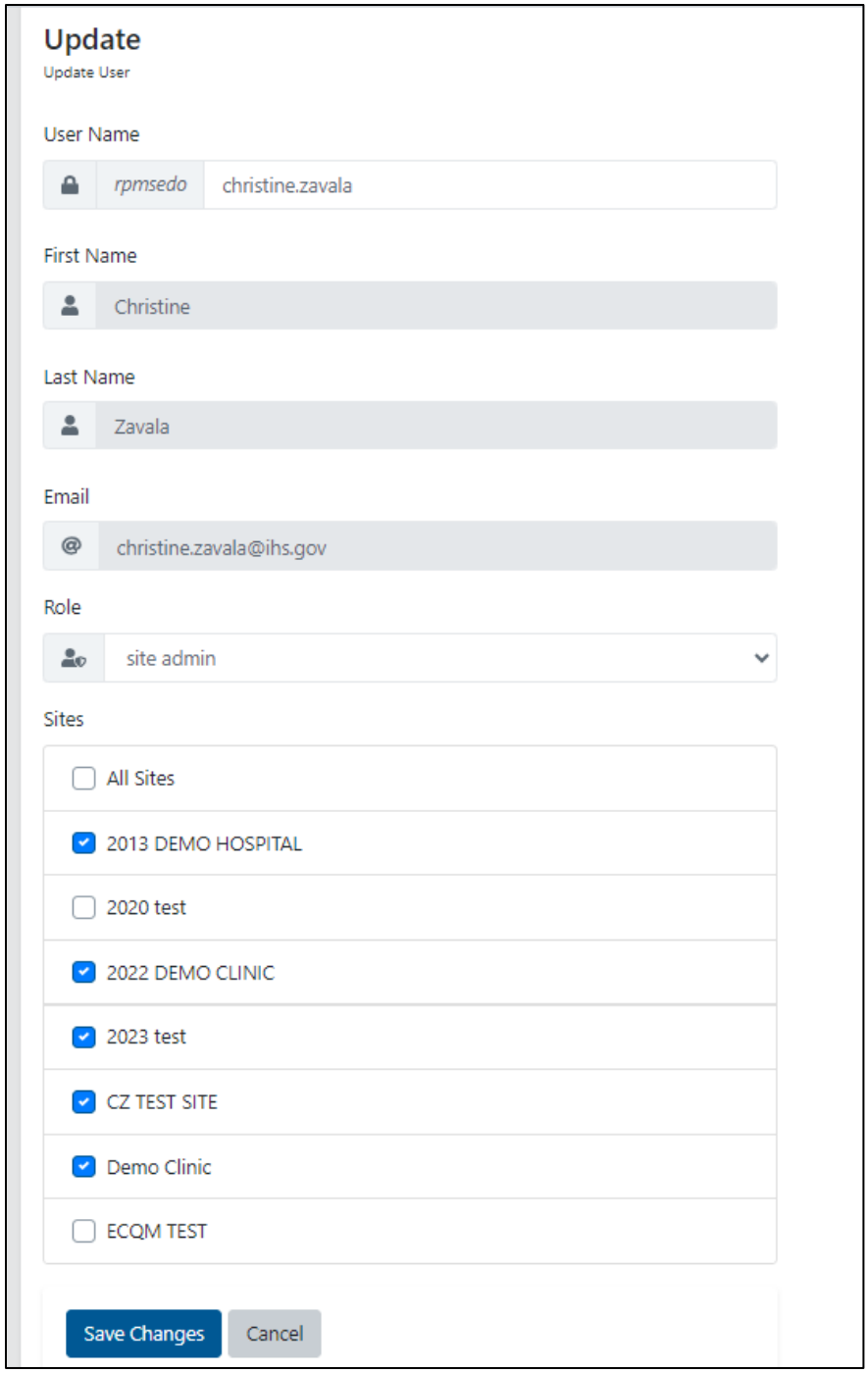


Figure 2-6: Update User screen

2. Only the **User Name**, **Role**, and **Site** can be edited.
3. Click **Save Changes** or click **Cancel** to discard all changes.

2.2.2.3 Deactivate a User

Click the **Deactivate** button next to a user who needs to be deactivated.

2.2.2.4 Reactivate a User

1. Click the **Activate** button next to the user to reactivate that user.
2. Click the **Update** button to review information and make changes as needed.
3. Click **Save Changes** to save the changes or click **Cancel** to discard all changes.

2.2.2.5 Users Filter

1. Enter username in the search box to view a specific user.
2. Select a Site from the list to view users for the selected site only.
3. Select a Role from the list to view users with the selected role.
4. Use a combination of the three filters to narrow the list further.

2.2.3 Diagnostic

Only users in the Super Admin role can view the Diagnostic tab. It was initially created for the package development team to troubleshoot issues reported by site users but may deliver valuable insights for Super Admins.

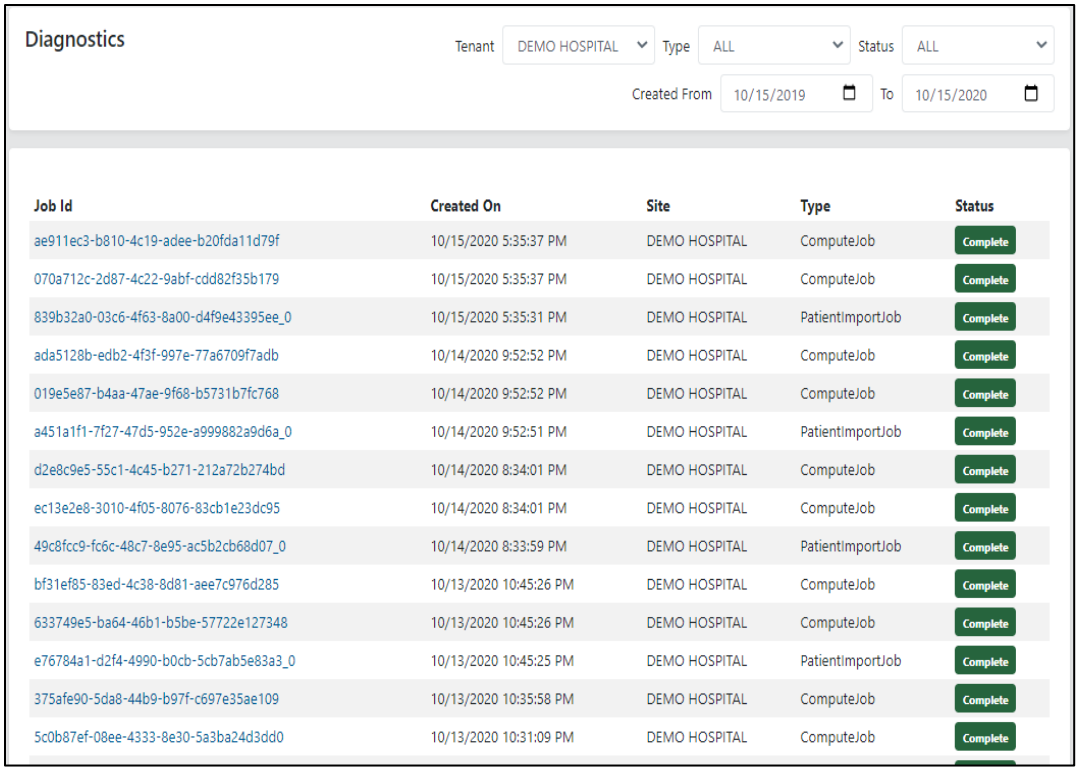


Figure 2-7: Diagnostic tab

The tab displays information about ECQM jobs that are currently running, have completed running, are scheduled to run, or have errored out related to patient import, QRDA III Export, and computation. The list can be filtered using the filter options.

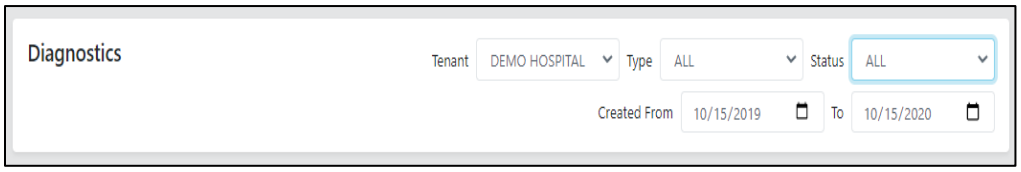


Figure 2-8: Diagnostics tab–Filter Options

Figure 2-9: Diagnostics tab–Job Status

The **Diagnostics** tab also allows for filtering by job type.

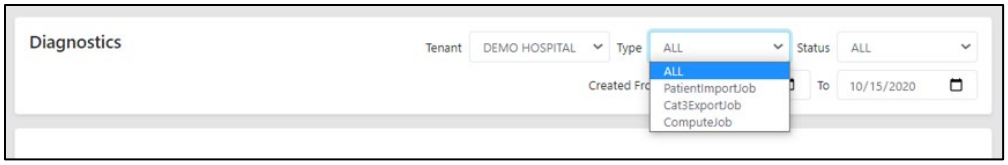


Figure 2-10: Diagnostic tab–Job Type

2.3 Site Admin Menu Options

Site Admins upload QRDA I zip files, download reports and results, define the reporting groups (Teams), and update their site information. Site Admins manage the patient data and provider lists.

2.3.1 Dashboard

Use the **Dashboard** tab to view previously generated reports. Site Admin users will default to their Dashboard upon log-in. Based on the selected team and reporting period, the dashboard displays the selected team's individual measures and calculations. Calculations will include percentage or average time, numerator counts, denominator counts, and stratifications for each measure.

The icon ( ) for each measure displays further detail about the measure. The **Detail** window provides more information on the selected measure. It will show the list of patients and which population criteria are met for each patient. Users will also have the option to download the data in Excel or PDF format.

New calculations will be performed when a new QRDA CAT I file(s) is imported, a new Team is created, or changes are made to existing Teams.

1. Click the **Teams** list to view a specific Team's measure calculation.
2. Select the **Team** from the list.

Note:	Both active and inactive teams will be displayed in the list. Any inactive team will display (Inactive) next to the team's name. Calculations will only be performed on active teams.

3. Select **Year** (current year is defaulted) or one of the quarter options (Q1, Q2, Q3, or Q4).
4. The dashboard displays the measures and their calculations.

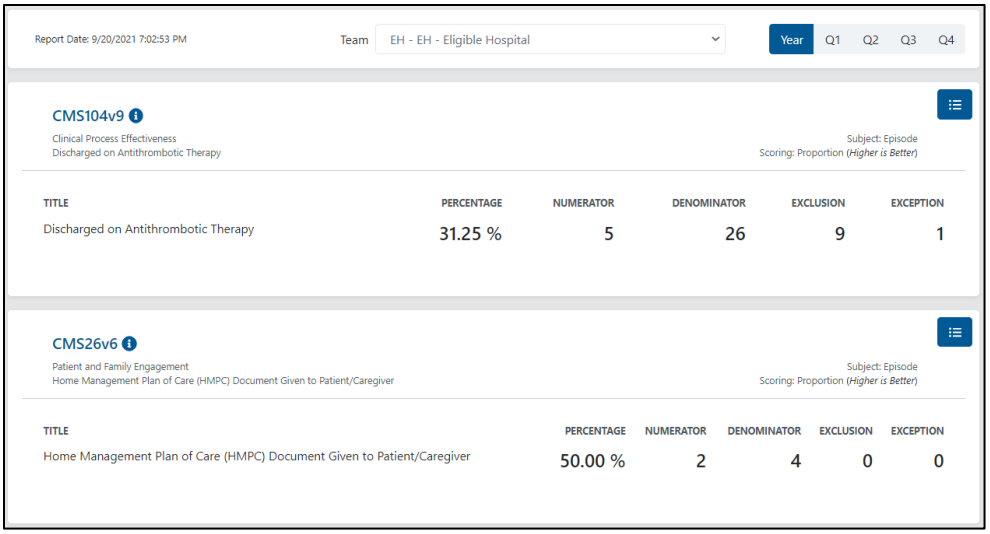


Figure 2-11: Dashboard example

5. Click the icon ( ) to display the measure description, calculation summary, and list of patients that met the measure criteria.

   - IPOP is Initial Population
   - DENOM is Denominator
   - NUMER is Numerator
   - DENEX is Denominator Exclusion
   - DENEXCEP is a Denominator Exception.

     A green circle with a check mark ( ) under each column means the patient met that population criteria.

     A red circle with a red X ( ) means the patient did not meet that population criteria.

   - NUMER/DENOM counts the number of patients that met the numerator criteria and the number of patients that met the denominator criteria. The Denominator subtracts the number of patients that met the denominator exclusion/exception.

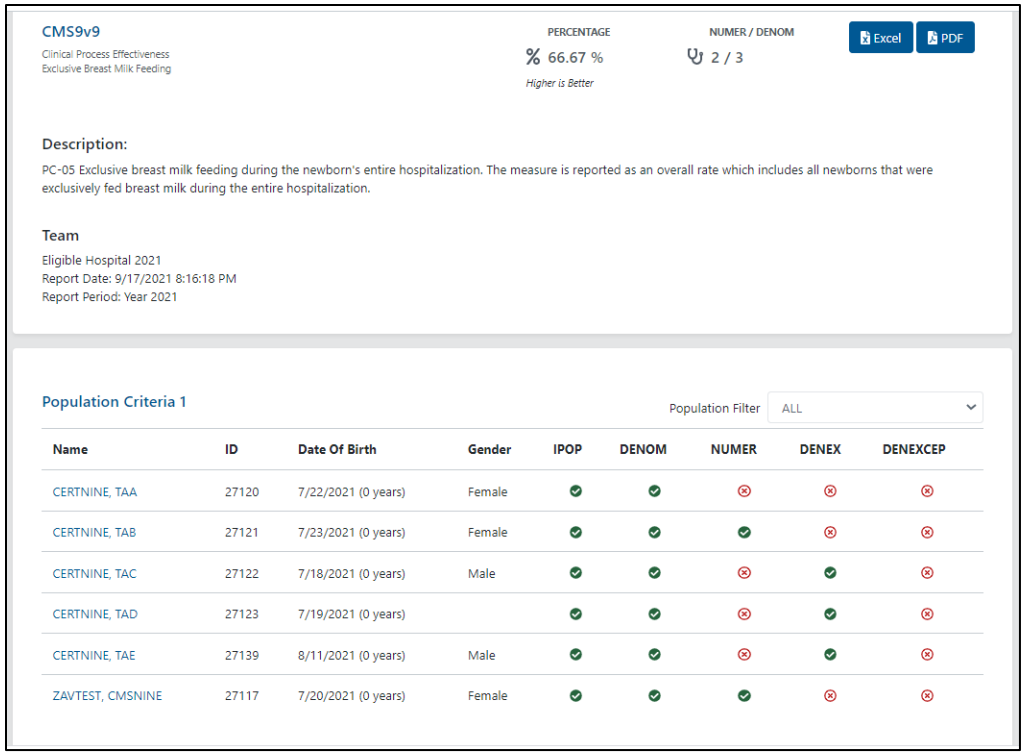


Figure 2-12: Measure Detail Screen example

6. Select options from the Population Filter drop-down list to filter patients by measure criteria. For example, selecting IN DENEX from the list displays patients included in Denominator Exclusion only.

7. Click the **Excel** (

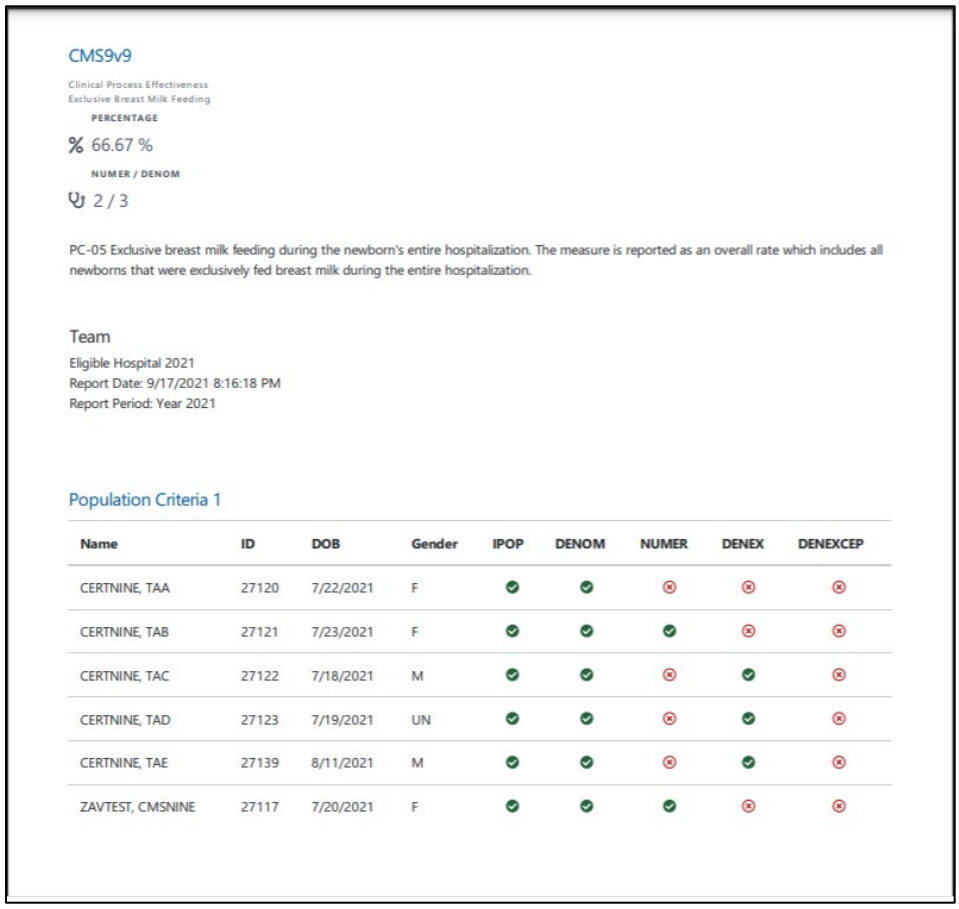
) button to generate the list of patients in Excel format. The Excel document is named automatically. The name format is the Team name, followed by the measure number and version, for example, Eligible Hospital-CMS9v11.xlsx.

	A	B	C	D	E	F	G	H	I	J
1	**Name**	**IEN**	**DOB**	**Gender**	**Race**	**Ethnicity**	**Denominator**	**Denominator Exclusion**	**Numerator**	**Denominator Exception**
2	ZAVTEST, CMSNINE	27117	7/20/2021	F	1002-5	2186-5	True	False	True	False
3	CERTNINE, TAA	27120	7/22/2021	F	1002-5	2186-5	True	False	False	False
4	CERTNINE, TAB	27121	7/23/2021	F	2054-5	2186-5	True	False	True	False
5	CERTNINE, TAC	27122	7/18/2021	M	2106-3	2186-5	True	True	False	False
6	CERTNINE, TAD	27123	7/19/2021	UN	2106-3	2186-5	True	True	False	False
7	CERTNINE, TAE	27139	8/11/2021	M	1002-5	2186-5	True	True	False	False

Figure 2-13: Sample Excel content

Note: If the QRDA I file imported is anonymized, patients' last and first names are replaced by XXX.

Click the **PDF** (PDF) button to generate a PDF summary report in PDF format. The PDF document is named automatically. The name format is the Team name, followed by the measure number and version, for example, Eligible Hospital-CMS9v11.xlsx.



CMS9v9

Clinical Process Effectiveness
Exclusive Breast Milk Feeding

PERCENTAGE

% 66.67 %

NUMER / DENOM

2 / 3

PC-05 Exclusive breast milk feeding during the newborn's entire hospitalization. The measure is reported as an overall rate which includes all newborns that were exclusively fed breast milk during the entire hospitalization.

Team

Eligible Hospital 2021
Report Date: 9/17/2021 8:16:18 PM
Report Period: Year 2021

Population Criteria 1

Name	ID	DOB	Gender	IPOP	DENOM	NUMER	DENEX	DENEXCEP
CERTNINE, TAA	27120	7/22/2021	F	✓	✓	✗	✗	✗
CERTNINE, TAB	27121	7/23/2021	F	✓	✓	✓	✗	✗
CERTNINE, TAC	27122	7/18/2021	M	✓	✓	✗	✓	✗
CERTNINE, TAD	27123	7/19/2021	UN	✓	✓	✗	✓	✗
CERTNINE, TAE	27139	8/11/2021	M	✓	✓	✗	✓	✗
ZAVTEST, CMSNINE	27117	7/20/2021	F	✓	✓	✓	✗	✗

Figure 2-14: Sample PDF

8. Click the patient's name for the patient-specific measure detail and the general eCQM information.

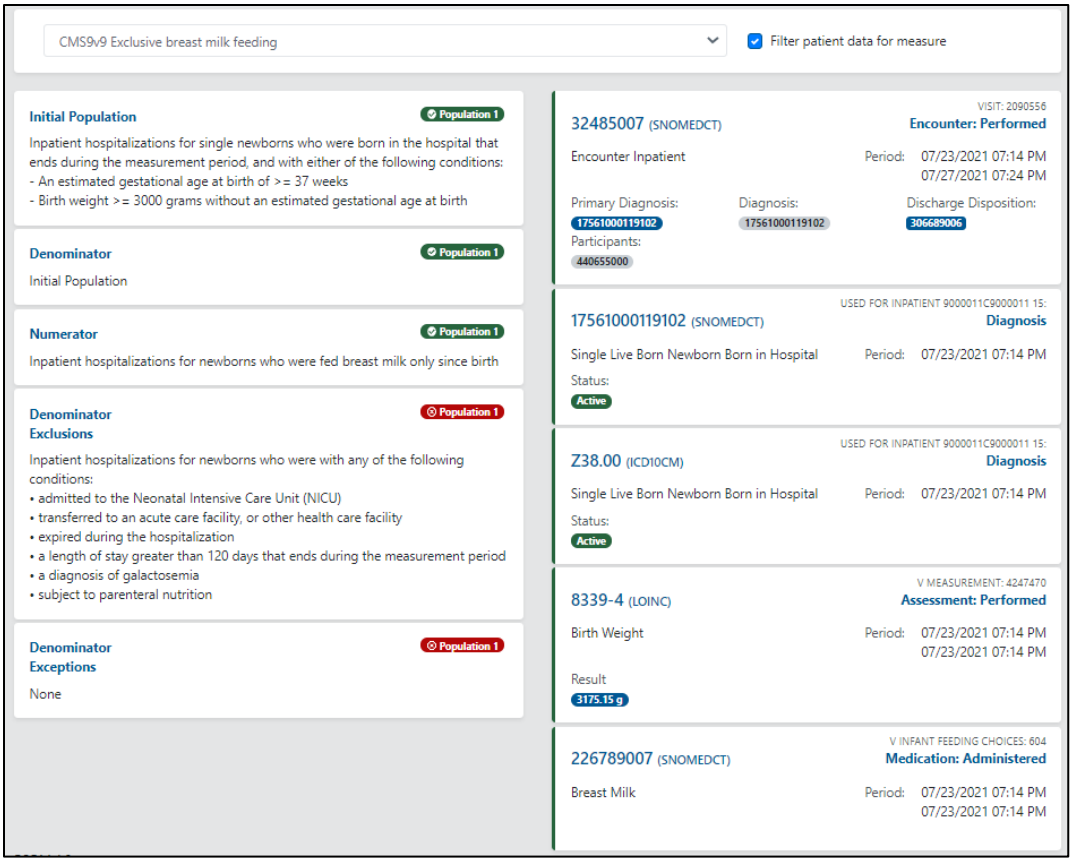


Figure 2-15: Patient-specific Measure Detail

Note: The general eCQM information for each population criterion is on the left. The green indicator (Population 1) means that the patient met that population criteria, and the red.
(Population 1) means that the patient did not meet that population criteria. On the right are all patient data that was captured. A green on the left side of the data box means that the data meets one of the values set for the selected measure. Red means the data is not associated with the measure selected.

9. Select the **Filter patient data for measure** (Filter patient data for measure) check box to show only the data used for the selected measure.

10. Click the **Dashboard** tab to display back the main dashboard.

2.3.2 Imports

Use the **Imports** tab to upload the QRDA I zip files. The **Imports** screen also displays historical imports if available.

The **Import Patients** screen displays the scheduled date/time of when the files are uploaded, the job ID, the file name, and the status.

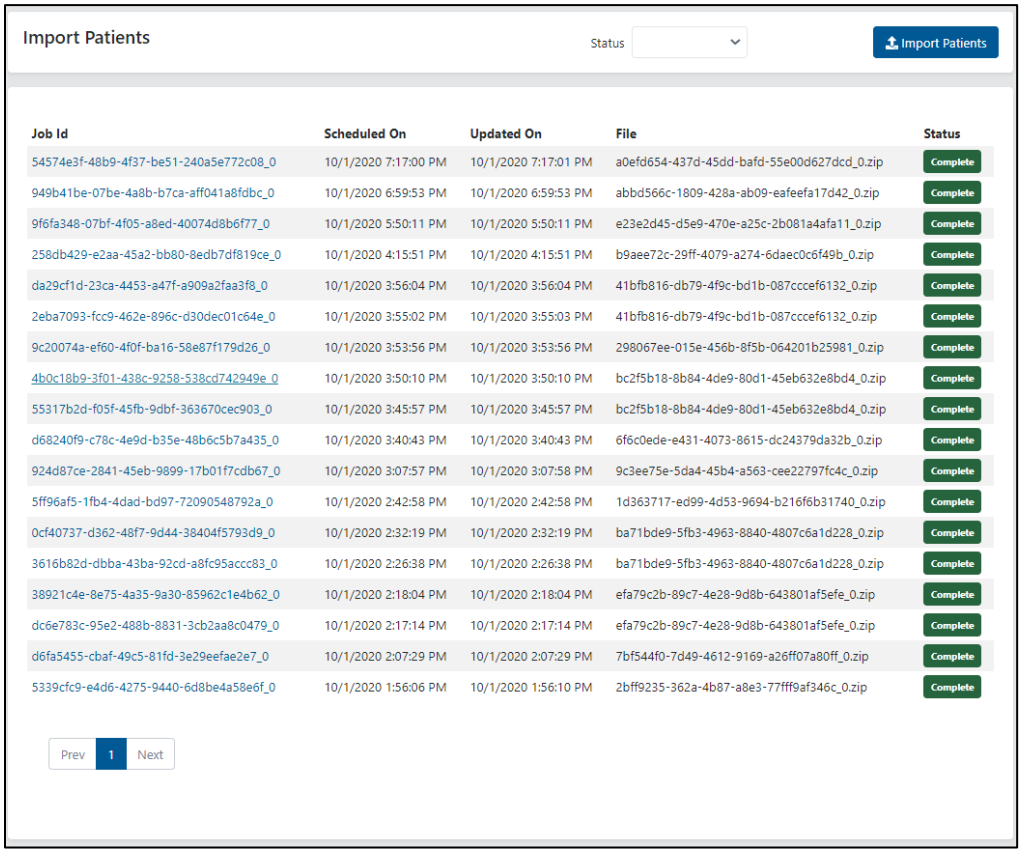


Figure 2-16: Imports Screen

1. Click the **Import Patients** button to upload QRDA I zip files. Users can upload multiple files.

2. Navigate to where the zip files are located, then drag and drop the zip file to the **Import Patients** window. Alternatively, click inside the **Import Patients** window and navigate to the QRDA I zip file location. Then select a file and click **Open**.

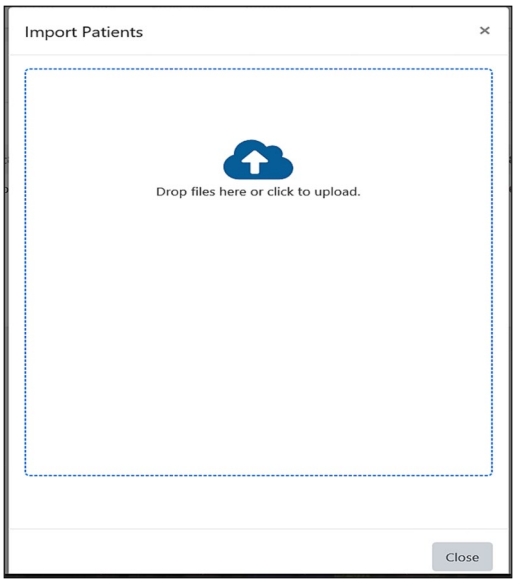


Figure 2-17: Import Patient's window

3. Once a file is uploaded, a green indicator will appear.

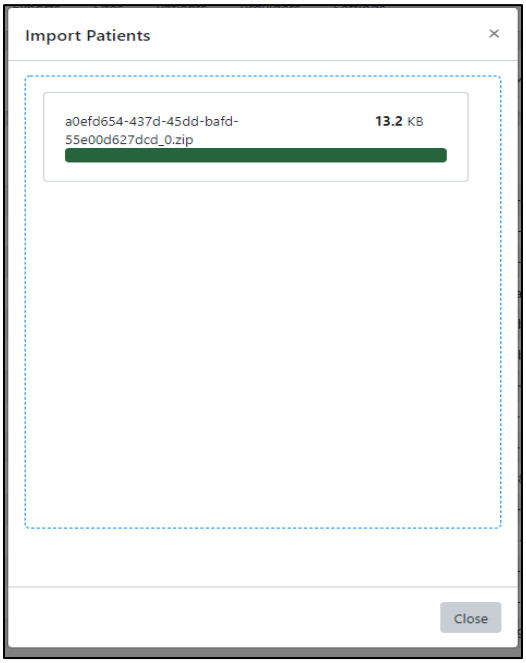


Figure 2-18: Import is complete

4. Click **Close**.

> **Note**: All files must be completed before closing the **Import Patient** window.

5. The uploaded files are displayed in the **Imports** window.

6. The status will display **Complete** once the upload is done.
7. To view the results and calculations, click the **Dashboard** menu option and select the appropriate Team and Year/Quarter.
8. Use the Status box to view a specific status. For example, select **Error** to view only imports with an **Error** status. Select the blank option in the list to view all imports again.

2.3.3 Submissions

Use the **Submissions** tab to export QRDA I and QRDA III files. The **Submissions** screen displays the scheduled date/time of when the export started, the job ID, and the status.

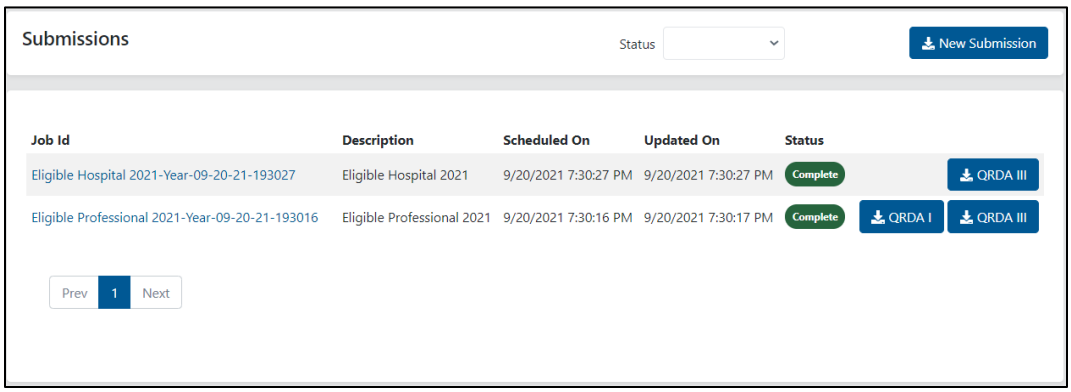


Figure 2-19: Submissions Tab

1. Click the **New Submission** button to start a new export.
2. Select the **Team** and **Submission Quarter** from the drop-down menu on the New Submission (QRDA I/III) window (Figure 2-20).
3. The current Performance Year is defaulted.
4. Select the **Include Patient QRDA I** checkbox if QRDA I files also need to be generated. This is optional.

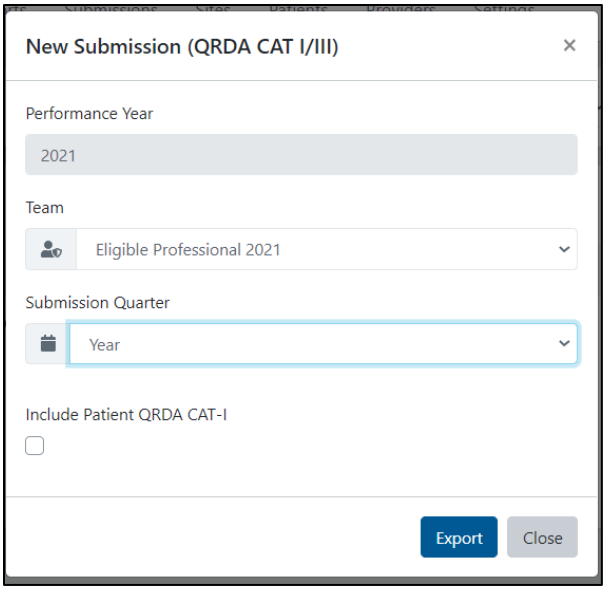


Figure 2-20: New Submissions Export Screen

5. Click the **Export** button to start the process.

> **Note**: If the selected Team or year has no calculations available, the message in Figure 2-21 displays to the user.

Figure 2-21: Error message

6. The **Status** column will display **Running**, and once done, the **Status** column will display **Complete**.

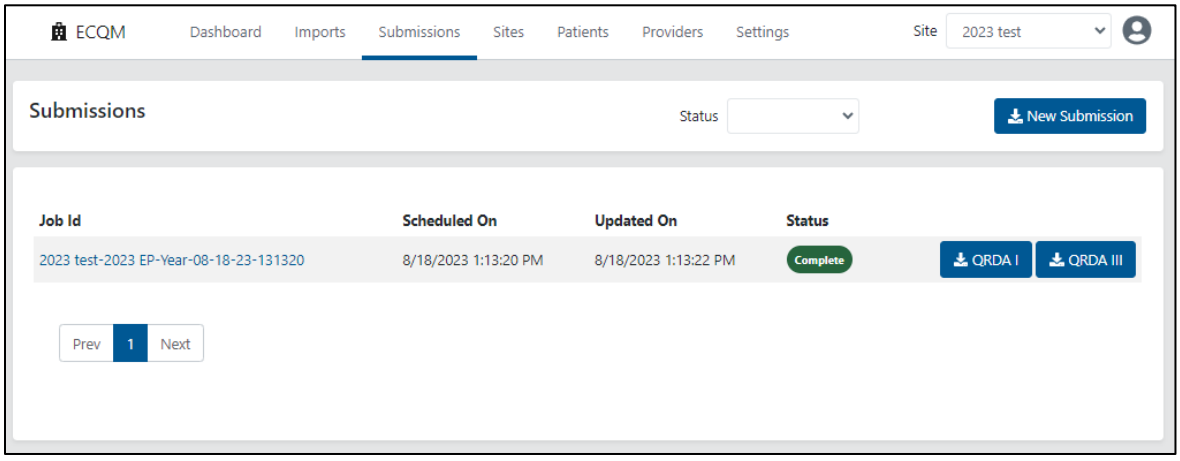


Figure 2-22: ECQM, QRDA I, and QRDA III Buttons

7. Click the **QRDA I** button to download files.
8. Click the **QRDA III** button to download files.
9. Use the **Status** box to view specific status. For example, select **Error** to view only exports with an **Error** status. Select the blank option in the list to view all exports again.

2.3.4 Sites

Use the **Sites** tab to modify the site's information and create/update teams. The site Admin can only be linked to one site and has access to that site only.

2.3.4.1 Create Teams

Teams are units of eCQM computation identified by a name. They contain a selection of measures and, optionally, a list of providers. eCQMs are computed for all the active teams configured for the site. Three types of teams can be created: EC, EH, and HYBRID.

The EC Team selects the 26 EP measures (not including two retired measures), and the EH Team provides a selection of 13 EH measures. The HYBRID team provides a selection of 2 EH/CAH measures. When a new site is created, the teams are automatically created but marked as INACTIVE. The Engine Site Admin must activate the teams for the ECQM to perform calculations. The predefined Teams (EH, EC, and HYBRID) are created for the current Computation/Performance Year. Sites can modify these teams or create new ones for the new performance year.

To create a new team:

1. Click the **Team** icon.
2. Click **Register Team** to create a new team.
3. Select either **EP**, **EH**, or **HYBRID** from the menu.
4. Enter the Team **Name** (maximum of 30 characters).
5. Current **Computation/Performance Year** is defaulted.
6. Select the **Active** check box.
7. Select the **QRDA I CMS Program** from the list. The options include the following:
   - HQR_PI
   - HQR_IQR
   - HQR__PI_IQR

- HQR_IQR_VOL

8. Select the **QRDA III CMS Program** from the list. The options include the following:

   - MIPS_INDIV
   - MIPS_GROUP
   - CPCPLUS
   - MIPS_VIRTUALGROUP

   Note: The Quality Coordinator/Manager should know which options to select for the QRDA I and QRDA III CMS Program based on the site goals and site quality program. The selected option is used for QRDA I and QRDA III export.

9. If the user selects **EP** from the list of Register Teams, the **Providers** search box is available. Adding providers to the team is optional.

   a. Enter a partial name of the provider to be added.

   b. Select the correct provider from the returned list.

   Note: Adding a provider means that, for EC Measure calculation, the result will be limited to only that patient data for which the selected provider is designated as the service provider in the QRDA I export data. Users can only search providers in the Providers tab.

10. Select the **All Measures** check box to add or select individual measures to include the measures.

11. Click **Save Changes**.

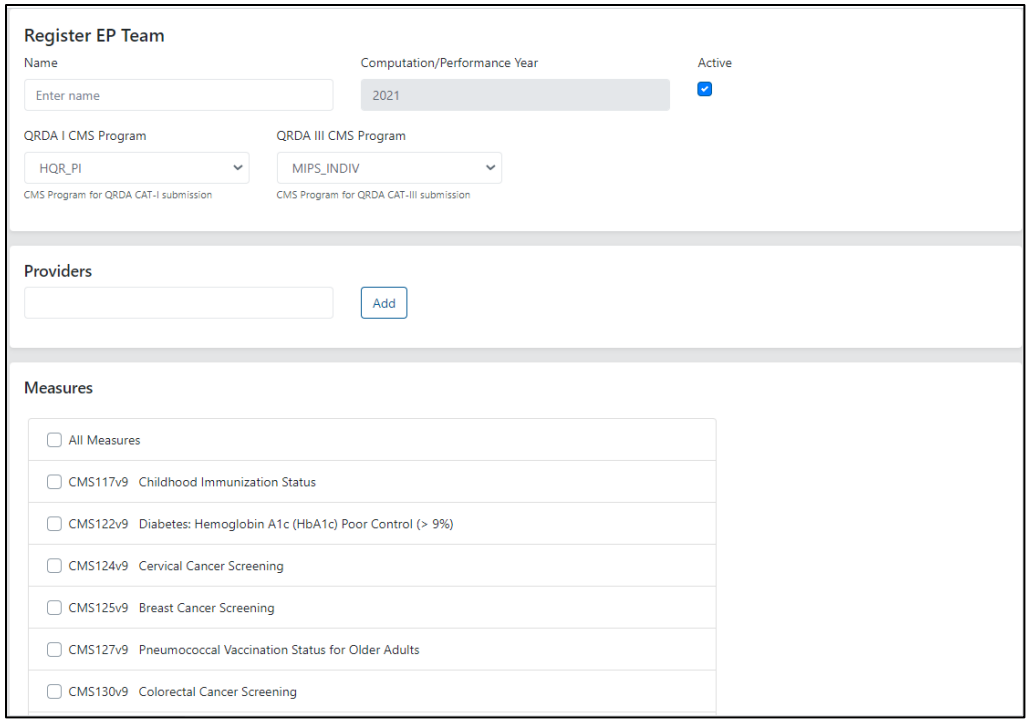


Figure 2-23: Register EP Team screen

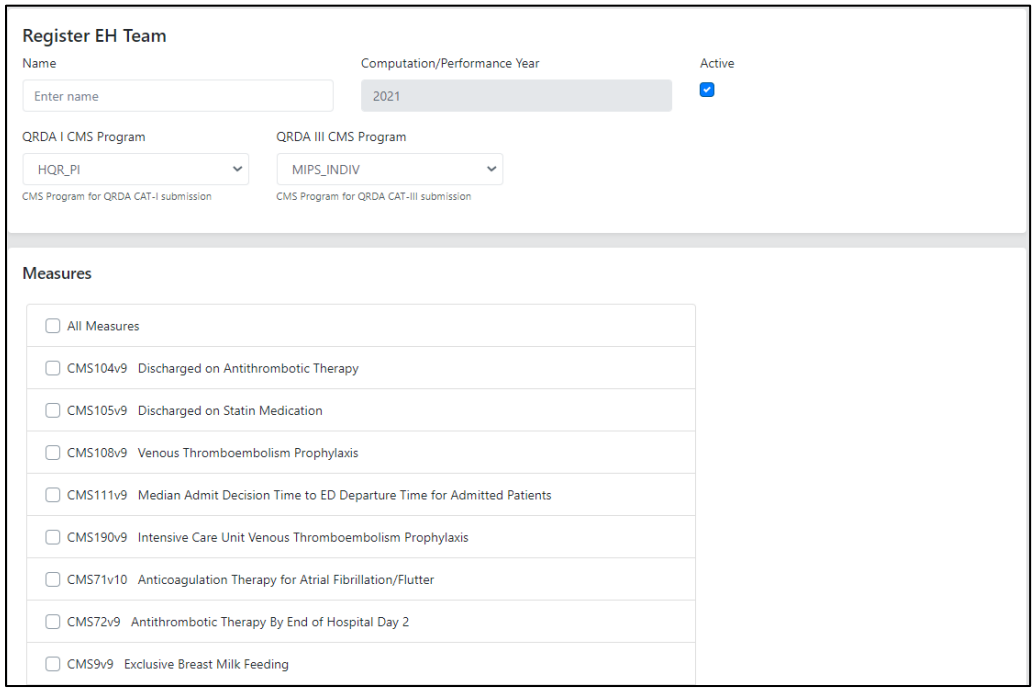


Figure 2-24: Register EH Team screen

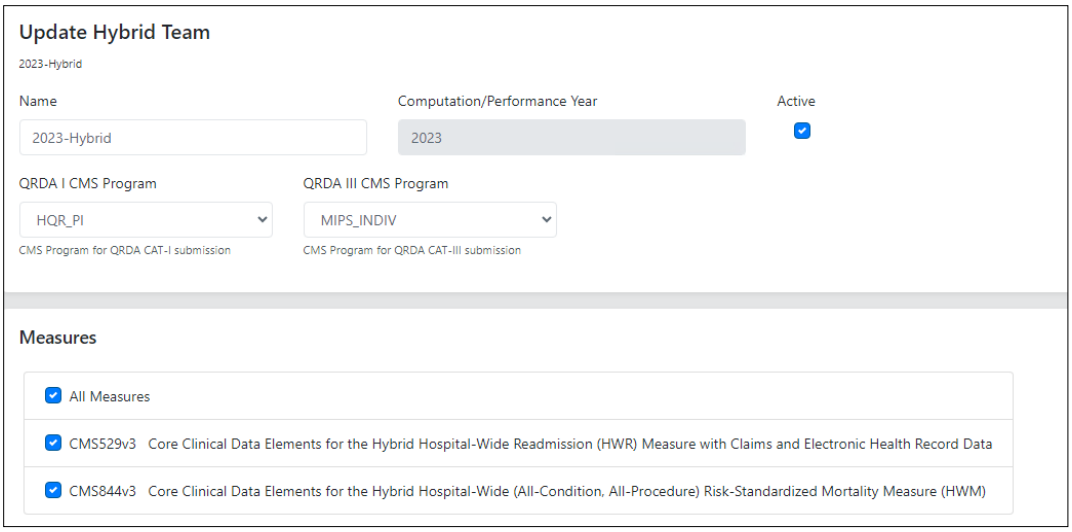


Figure 2- 25: Register Hybrid Team screen

2.3.4.2 Modify Teams

1. Click the **Team** icon.
2. Click the **Update** button next to a team to modify a team.
3. Modify the **Name** as appropriate.
4. Modify the **QRDA I and QRDA III CMS Program** as appropriate.
5. Select or clear **Measures**, as needed.
6. Click **Save Changes**.

2.3.4.3 Activate/Inactivate Teams

1. Click the **Team** icon.
2. Click the **Deactivate** (

) icon next to an active team to inactivate. The page refreshes, and the Team displays as **Inactive**.

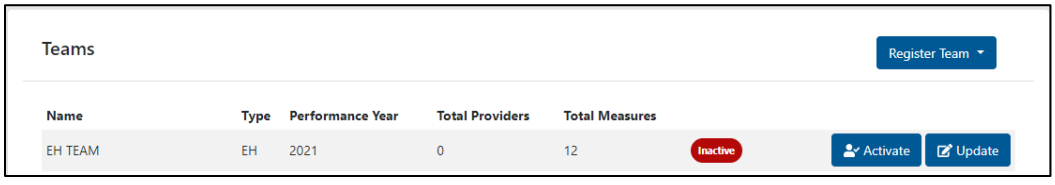


Figure 2-26: Team screen–Inactive Team

Note: The user can also inactivate a team by clicking the Update icon, clearing the **Active** check box, and clicking **Save Changes**.

3. Click the **Activate** (Activate) icon next to the inactive team to reactivate the team. The page refreshes, and the Team will display as **Active**.

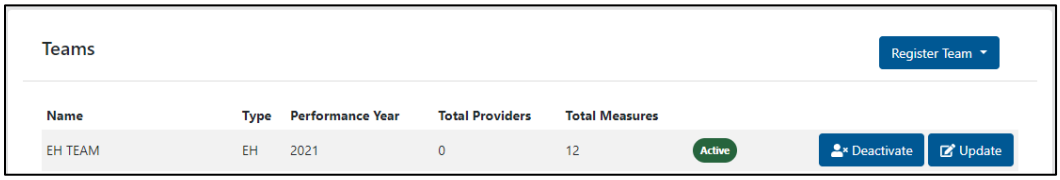


Figure 2-27: Team screen–Active Team

> **Note:** A user can also reactivate a team by clicking the Update icon, clearing the **Active** check box, and then selecting **Save Changes**.

2.3.4.4 Update Sites

Refer to Section 2.2.1.2 On how to modify site information.

2.3.5 Patients

Use the **Patients** tab to view the list of patients loaded in ECQM. The list includes Name, ID (IEN), DOB, Gender, Race, and Ethnicity. From the Patients tab, users can check if a patient qualifies for a particular measure.

1. Select a patient from the list or enter a **patient name** or **IEN** in the search box.
2. Select a measure from the list.
3. Click the **Filter patient data** for the measure check box to show only data used for the selected measure.

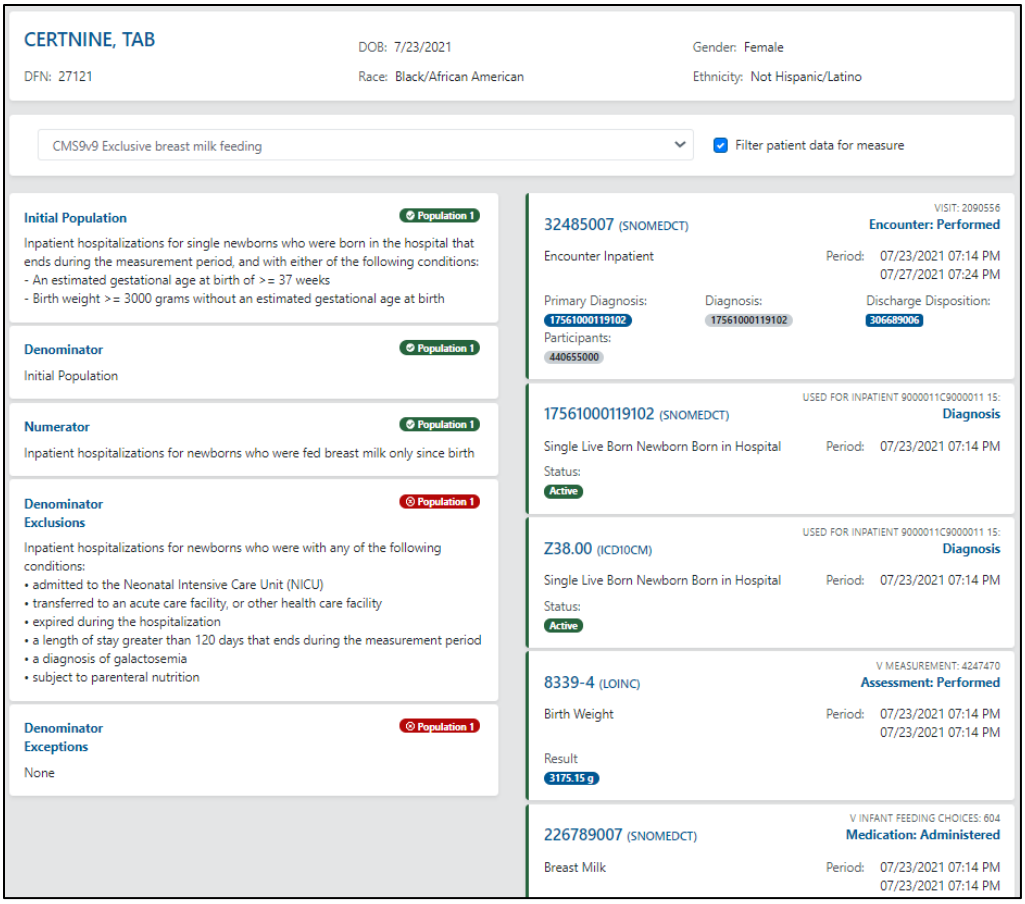


Figure 2-28: Sample Measure Detail from the Patients tab

2.3.6 Providers

Providers included as service providers in the automatic transmission of the QRDA I zip files from the eCQM Extraction Tool (BQRE) will be added automatically in the **Providers** tab. Providers can also be added manually, although it is not recommended. When manually adding a provider, the NPI must be entered correctly. Any providers added through this menu will be available for selection when creating a Team for EC.

1. Click the **Add Provider** button to add a new provider.
2. On the **Add Provider** screen:
   a. Enter the provider's **First Name**.
   b. Enter the provider's **Last Name**.
   c. Enter the provider's **NPI** (10 digits).

Note: The provider must have a valid NPI.

3. Click **Add**.
4. Click **Close** to cancel.
5. Use the Search Lookup to find a provider.
   a. Enter the provider's name (LastName, FirstName format) or the NPI number.
   b. Click the **Search** ( ) icon or press Enter.
6. The list of matching providers will be displayed.
7. To view the list of all providers again, click the **Providers** tab or clear out the search and press Enter.

2.3.7 Settings

Use the **Settings** tab to delete or purge imported patient data. This action will permanently delete imported patient data, exports, and providers. Teams will not be deleted, and providers who were added to Teams will not be deleted. The user will have to delete them manually under Teams.

Warning: This process cannot be undone.

1. Click the **Delete** button to start the deletion process.
2. A warning message displayed (Figure 2-28). Click the **Delete Patient Data** button to continue.

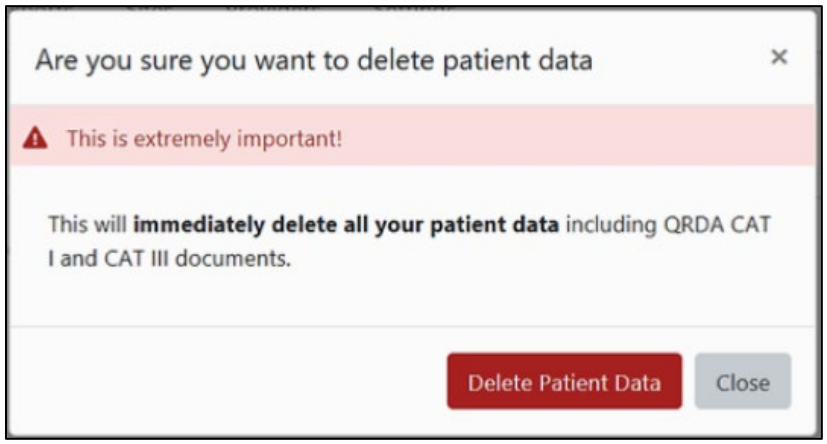


Figure 2-29: Delete Warning Message

3. Click the **Import** menu options. Any import jobs have been cleared.
4. Click the **Export** menu options. Any export jobs have been cleared.
5. Click the **Dashboard** menu options. The dashboard has been cleared.

2.4 Super Auditor Menu Options

The Super Auditor monitors the actions taken by all users in ECQM, such as creating sites, defining users and teams, logging in, and logging out. The Super Auditor can search or filter by user, event type, and date range. The Super Auditor role is created by the Super Admin.

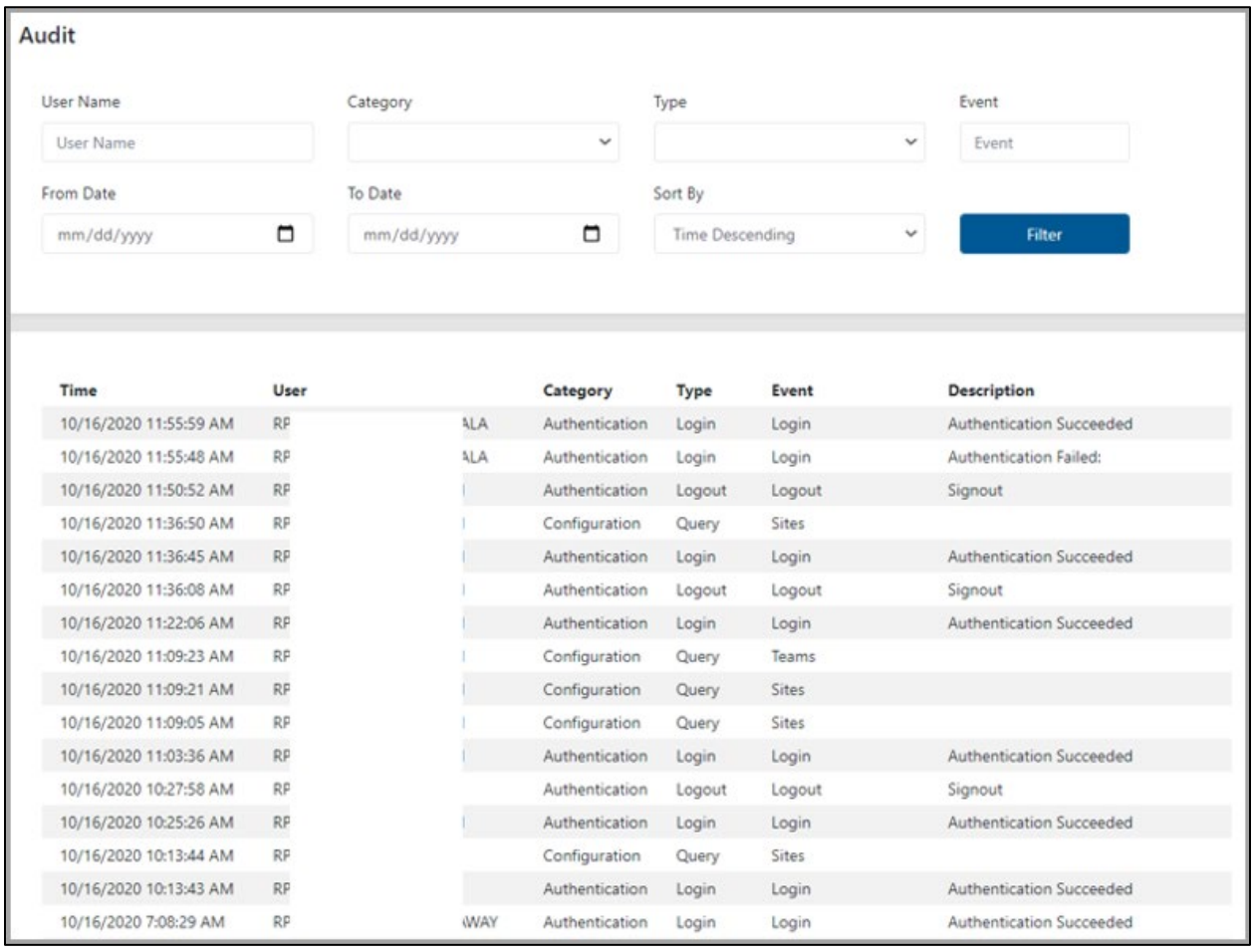


Figure 2-30: Super Auditor screen

To filter actions in the **Audit** screen:

1. Enter the User Name. (The format is **domain\username**)
2. Select a **Category** from the list. The options include the following:
   - Authentication
   - PatientData
   - Configuration
3. Select the **Type**. The options include the following:

- Login
- Logout
- Delete
- Create
- Update
- Activate
- Deactivate
- Query
- Upload
- Download
- Schedule

4. Enter the **Event**. Examples of events are as follows:
    - Login
    - Logout
    - Sites
    - Teams
    - QRDA
    - QRDA I
    - QRDA III
    - Patient Data Upload
    - Delete
5. Enter the **From Date** and **To Date**.
6. Select **Sort By**:
    - Time Descending
    - Time Ascending
    - Category
    - Type
    - Event
7. Click the **Filter** button.

2.5 Site Auditor Menu Options

The Site Auditor monitors site-related actions such as site log-in/log-out, site update, team update, download of QRDA I and QRDA III, and patient data upload. The Site Auditor can search or filter by user, event type, and date range. Super Admins create the Site Auditor role.

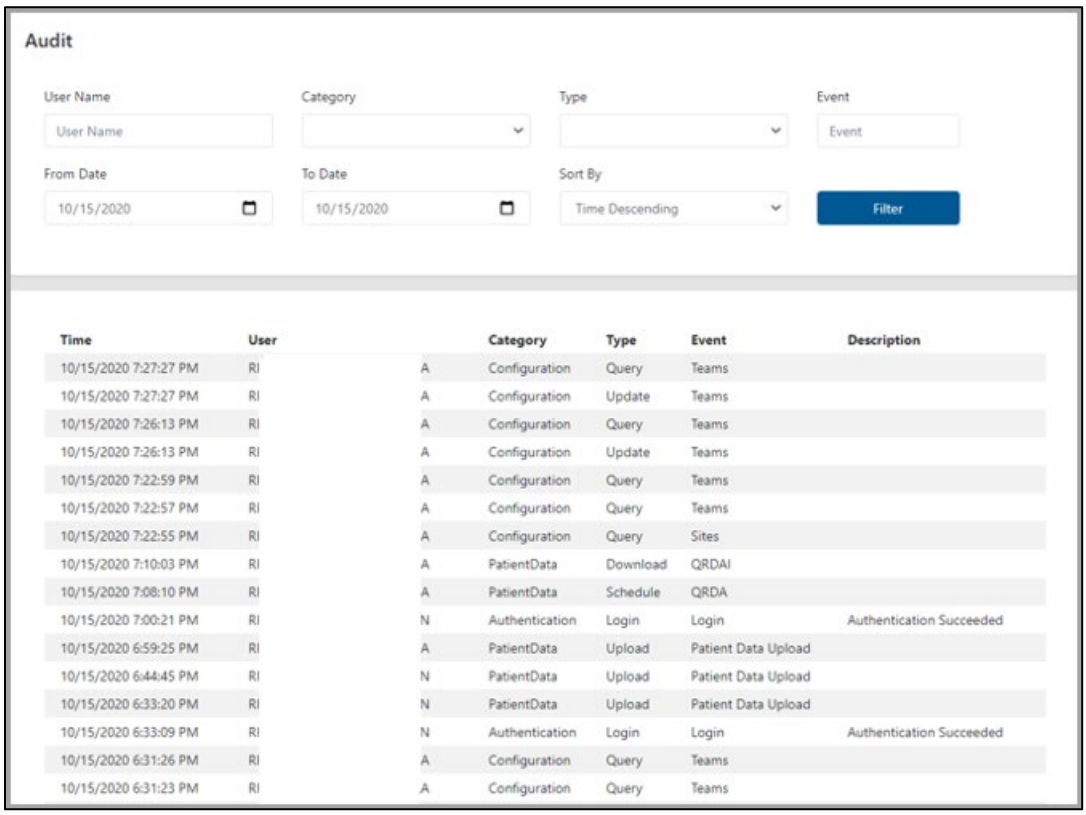


Figure 2-31: Site Auditor screen

To filter actions in the **Audit** screen:

1. Enter the **User Name** (format is domain\username).
2. Select a **Category** from the list. The options include the following:
   - Authentication
   - PatientData
   - Configuration
3. Select the **Type**. The options include the following:
   - Login
   - Logout
   - Delete

- Create
- Update
- Activate
- Deactivate
- Query
- Upload
- Download
- Schedule

4. Enter the **Event**. Examples of events are as follows:
    - Login
    - Logout
    - Sites
    - Teams
    - QRDA
    - QRDA-I
    - QRDA-III
    - Patient Data Upload
    - Delete
5. Enter the **From Date** and **To Date**.
6. Select **Sort By**:
    - Time Descending
    - Time Ascending
    - Category
    - Type
    - Event
7. Click the **Filter** button.

Appendix A Rules of Behavior

The Resource and Patient Management System (RPMS) is a United States Department of Health and Human Services, Indian Health Service (IHS) information system for *OFFICIAL USE ONLY*. The RPMS system is subject to monitoring; therefore, no expectation of privacy shall be assumed. Individuals found performing unauthorized activities are subject to disciplinary action, including criminal prosecution.

Per IHS policy, all RPMS users (Contractors and IHS Employees) will be provided a copy of the Rules of Behavior (ROB) and must acknowledge that they have received and read them before being granted access to an RPMS system.

- For a listing of general ROB for all users, see the most recent edition of the *IHS General User Security Handbook* (SOP 06-11a).
- For a listing of system administrators/managers' rules, see the most recent edition of the *IHS Technical and Managerial Handbook* (SOP 06-11b).

Both documents are available at this IHS website:
https://home.ihs.gov/security/index.cfm

> **Note**: Users must be logged on to the IHS D1 Intranet to access these documents.

The ROB listed in the following sections are specific to RPMS.

A.1 All RPMS Users

In addition to these rules, each application may include additional ROB that may be defined within that application's documentation (e.g., Dental, Pharmacy).

A.1.1 Access

RPMS users shall:

- Only use data for which you have been granted authorization.
- Only give information to personnel who have access authority and have a need to know.
- Always verify a caller’s identification and job purpose with your supervisor or the entity provided as an employer before providing any information system access, sensitive or nonpublic agency information.
- Be aware that personal use of information resources is authorized on a limited basis within the provisions of *Indian Health Manual* Part 8, “Information Resources Management,” Chapter 6, “Limited Personal Use of Information Technology Resources.”

RPMS users shall not:

- Retrieve information for someone who does not have the authority to access the information.
- Access, research, or change any user account, file, directory, table, or record not required to perform their *official* duties.
- Store sensitive files on a PC hard drive, portable devices, or media if access to the PC or files cannot be physically or technically limited.
- Exceed their authorized access limits in RPMS by changing information or searching databases beyond the responsibilities of their jobs or by divulging information to anyone not authorized to know that information.

A.1.2 Information Accessibility

RPMS shall restrict access to information based on the type and identity of the user. However, regardless of the type of user, access shall be restricted to the minimum level necessary to perform the job.

RPMS users shall:

- Access only those documents they created and those other documents to which they have a valid need-to-know and to which they have expressly granted access through an RPMS application based on their menus (job roles), keys, and FileMan access codes. Some users may be afforded additional privileges based on their functions, such as system administrator or application administrator.
- Acquire written preauthorization by IHS policies and procedures before interconnecting or transferring data from RPMS.

A.1.3 Accountability

RPMS users shall:

- Behave ethically, technically proficient, informed, and trustworthy.
- Log out of the system whenever they leave the vicinity of their personal computers (PC).
- Be alert to threats and vulnerabilities in the security of the system.
- Report all security incidents to their local Information System Security Officer (ISSO).
- Differentiate tasks and functions to ensure that no person has sole access to or control of essential resources.
- Protect all sensitive data entrusted to them as part of their government employment.

- Abide by all Department and Agency policies, procedures, and guidelines related to ethics, conduct, behavior, and information technology (IT) information processes.

A.1.4 Confidentiality

RPMS users shall:

- Be aware of the sensitivity of electronic and hard copy information and protect it accordingly.
- Store hard copy reports/storage media containing confidential information in a locked room or cabinet.
- Erase sensitive data on storage media before reusing or disposing of the media.
- Protect all RPMS terminals from public viewing at all times.
- Abide by all Health Insurance Portability and Accountability Act (HIPAA) regulations to ensure patient confidentiality.

RPMS users shall not:

- Allow confidential information to remain on the PC screen when someone who is not authorized to access that data is nearby.
- Store sensitive files on a portable device or media without encrypting.

A.1.5 Integrity

RPMS users shall:

- Protect their systems against viruses and similar malicious programs.
- Observe all software license agreements.
- Follow industry standard procedures for maintaining and managing RPMS hardware, operating system software, application software, database software, and database tables.
- Comply with all copyright regulations and license agreements associated with RPMS software.

RPMS users shall not:

- Violate federal copyright laws.
- Install or use unauthorized software within the system libraries or folders.
- Users may not use freeware, shareware, or public domain software on/with the system without their manager's written permission and without first scanning it for viruses.

A.1.6 System Logon

RPMS users shall:

- Have a unique User Identification/Account name and password.
- Be granted access based on authenticating the account name and password entered.
- Be locked out of an account after five successive failed login attempts within a specified period (e.g., one hour).

A.1.7 Passwords

RPMS users shall:

- Change passwords a minimum of every 90 days.
- Create passwords with a minimum of eight characters.
- If the system allows, use a combination of alpha-numeric characters for passwords, with at least one uppercase letter, one lowercase letter, and one number. If possible, it is recommended that a unique character be used in the password.
- Change vendor-supplied passwords immediately.
- Protect passwords by committing them to memory or storing them safely (do not store passwords in login scripts or batch files).
- Change passwords immediately if the password has been seen, guessed, or otherwise compromised, and report the compromise or suspected compromise to their Information System Security Officer (ISSO).
- Keep user identifications (IDs) and passwords confidential.

RPMS users shall not:

- Use common words found in any dictionary as a password.
- Use obvious readable passwords or passwords that incorporate personal data elements (e.g., user's name, date of birth, address, telephone number, or social security number; names of children or spouses; favorite band, sports team, or automobile; or other personal attributes).
- Share passwords/IDs with anyone or accept using another's password/ID, even if offered.
- Reuse passwords. A new password must contain no more than five characters per eight characters from the previous password.
- Post passwords.
- Keep a password list in a prominent place, such as under keyboards, in desk drawers, or in any other location where it might be disclosed.

- Give a password out over the phone.

A.1.8 Backups

RPMS users shall:

- Plan for contingencies such as physical disasters, loss of processing, and disclosure of information by preparing alternate work strategies and system recovery mechanisms.
- Make backups of systems and files on a regular, defined basis.
- If possible, store backups away from the system in a secure environment.

A.1.9 Reporting

RPMS users shall:

- Contact and inform their ISSO that they have identified an IT security incident and begin the reporting process by providing an IT Incident Reporting Form regarding this incident.
- Report security incidents as detailed in the *IHS Incident Handling Guide* (SOP 05-03).

RPMS users shall not:

- Assume that someone else has already reported an incident. The risk of an incident going unreported far outweighs the possibility that an incident gets reported more than once.

A.1.10 Session Timeouts

The RPMS system implements system-based timeouts, which allow users to exit a prompt after 5 minutes of inactivity.

RPMS users shall:

- Utilize a screen saver with password protection set to suspend operations at no greater than 10 minutes of inactivity. This will prevent inappropriate access and viewing of any material displayed on the screen after some period of inactivity.

A.1.11 Hardware

RPMS users shall:

- Avoid placing system equipment near obvious environmental hazards (e.g., water pipes).
- Keep an inventory of all system equipment.

- Keep records of maintenance/repairs performed on system equipment.

RPMS users shall not:

- Eat or drink near system equipment.

A.1.12 Awareness

RPMS users shall:

- Participate in organization-wide security training as required.
- Read and adhere to security information pertaining to system hardware and software.
- Take the annual information security awareness.
- Read all applicable RPMS manuals for the applications used in their jobs.

A.1.13 Remote Access

Each subscriber organization establishes its policies for determining which employees may work at home or in other remote workplace locations. Any remote work arrangement should include policies that:

- Are in writing.
- Provide remote user authentication through ID and password or other acceptable technical means.
- Outline the work requirements, security safeguards, and procedures the employee must follow.
- Ensure adequate storage of files, removal, and non-recovery of temporary files created in processing sensitive data, virus protection, and intrusion detection, and provide physical security for government equipment and sensitive data.
- Establish mechanisms to back up data created and stored at alternate work locations.

Remote RPMS users shall:

- Remotely access RPMS through a virtual private network (VPN) whenever possible. Direct dial-in access must be justified and approved in writing, and industry best practices or government procedures must secure its use.

Remote RPMS users shall not:

- Disable any encryption for network, internet, and Web browser communications.

A.2 RPMS Developers

RPMS developers shall:

- When writing or revising code, always be mindful of protecting the confidentiality, availability, and integrity of RPMS.
- Always follow the IHS RPMS Programming Standards and Conventions (SAC) when developing for RPMS.
- Only access information or code within the namespaces they have been assigned as part of their duties.
- Remember that all RPMS code is the property of the U.S. Government, not the developer.
- Not access live production systems without obtaining appropriate written access and shall only retain that access for the shortest period possible to accomplish the task that requires the access.
- Observe the separation of duties, policies, and procedures to the fullest extent possible.
- Document or comment on all changes to any RPMS software when the change or update is made. Documentation shall include the programmer's initials, change date, and reason for the change.
- Release their certified applications using checksums or other integrity mechanisms to assure the integrity of the routines within their RPMS applications.
- Follow industry best standards for systems assigned to develop, maintain, and abide by all Department and Agency policies and procedures.
- Document and implement security processes whenever available.

RPMS developers shall not:

- Write any code that adversely impacts RPMS, such as backdoor access, "Easter eggs," time bombs, or any other malicious code, or make inappropriate comments within the code, manuals, or help frames.
- Grant any user or system administrator access to RPMS unless proper documentation is provided.
- Release any sensitive agency or patient information.

A.3 Privileged Users

Personnel with significant access to processes and data in RPMS, such as system security administrators, systems administrators, and database administrators, have added responsibilities to ensure its secure operation.

Privileged RPMS users shall:

- Verify that any user requesting access to any RPMS system has completed the appropriate access request forms.
- Ensure that government and contractor personnel understand and comply with license requirements. End users, supervisors, and functional managers are ultimately responsible for this compliance.
- Advise the system owner on matters concerning information technology security.
- Assist the system owner in developing security plans, risk assessments, and supporting documentation for the certification and accreditation process.
- Ensure that any changes to RPMS that affect contingency and disaster recovery plans are conveyed to the person responsible for maintaining continuity of operations plans.
- Ensure that adequate physical and administrative safeguards are operational within their areas of responsibility and that access to information and data is restricted to authorized personnel on a need-to-know basis.
- Verify that users have received appropriate security training before allowing access to RPMS.
- Implement applicable security access procedures and mechanisms, incorporate appropriate levels of system auditing, and review audit logs.
- Document and investigate known or suspected security incidents or violations and report them to the ISSO, Chief Information Security Officer (CISO), and systems owner.
- Protect the supervisor, superuser, or system administrator passwords.
- Avoid instances where the same individual is responsible for several functions (e.g., transaction entry, and transaction approval).
- Watch for unscheduled, unusual, and unauthorized programs.
- Help train system users on the appropriate use and security of the system.
- Establish protective controls to ensure the system's accountability, integrity, confidentiality, and availability.
- Replace passwords when a compromise is suspected. Delete user accounts as quickly as possible when the user is no longer authorized in the system. Passwords forgotten by their owner should be replaced, not reissued.
- Terminate user accounts when a user transfers or has been terminated. If the user has the authority to grant authorizations to others, review these other authorizations. Retrieve any devices used to gain access to the system or equipment. Cancel login IDs and passwords and delete or reassign related active and backup files.

- If the system is left on and unattended, use a suspend program to prevent an unauthorized user from logging on with the current user's ID.
- Verify the user's identity when resetting passwords. This can be done in person or by having the user answer a question that can be compared to one in the administrator’s database.
- Shall follow industry best standards for systems they are assigned to and abide by all Department and Agency policies and procedures.

Privileged RPMS users shall not:

- Access any files, records, systems, etc., that are not explicitly needed to perform their duties
- Grant any user or system administrator access to RPMS unless proper documentation is provided.
- Release any sensitive agency or patient information.

Glossary

Admission Orderable Items

Site- or facility-defined items that indicate a patient's admission.

Clinical Quality Measures

Standardized metrics that measure and track the quality of health care services by ECs, EH, and CAH.

Meaningful Use

The use of Certified EHR Technology (CEHRT) to:

- Improve quality, safety, efficiency, and reduce health disparities
- Engage patients and family
- Improve care coordination and population and public health
- Maintain privacy and security of patient health information

Acronym List

Acronym	Meaning
CAH	Critical Access Hospital
CEHR	Certified Electronic Health Record
CEHRT	Certified Electronic Health Record Technology
CMS	Centers for Medicare & Medicaid Services
CQM	Clinical Quality Measures
eCQM	Electronic Clinical Quality Measures
EC	Eligible Clinician
ECQM	Electronic Clinical Quality Measure Engine
ED	Emergency Department
EH	Eligible Hospital
EHR	Electronic Health Records
IHS	Indian Health Service
ISSO	Information System Security Officer
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
ONC	Office of the National Coordinator for Health Information Technology
QRDA	Quality Reporting Document Architecture
QRDA I	QRDA Category I (Patient Data) File
QRDA III	QRDA Category III (Aggregated Data) File
RPMS	Resource and Patient Management System

Contact Information

If you have any questions or comments regarding this distribution, please contact the IHS IT Service Desk.

Phone: (888) 830-7280 (toll free)

Web: https://www.ihs.gov/itsupport/

Email: itsupport@ihs.gov