



RESOURCE AND PATIENT MANAGEMENT SYSTEM

Electronic Clinical Quality Measures Engine

(ECQM)

User Manual

Version 3.0
December 2020

Office of Information Technology
Division of Information Technology

Table of Contents

1.0	Introduction.....	1
1.1	eCQM Overview	1
1.2	More Information.....	3
2.0	ECQM Engine.....	4
2.1	Log In/Log Out.....	5
2.2	Super Admin Menu Options.....	5
2.2.1	Sites	6
2.2.2	Users	8
2.2.3	Diagnostic.....	11
2.3	Site Admin Menu Options	12
2.3.1	Dashboard.....	12
2.3.2	Imports	16
2.3.3	Export	19
2.3.4	Sites	20
2.3.5	Patients	24
2.3.6	Providers	25
2.3.7	Settings	26
2.4	Super Auditor Menu Options	27
2.5	Site Auditor Menu Options.....	29
Appendix A	Rules of Behavior	31
	Glossary.....	40
	Acronym List	41
	Contact Information	42

Preface

Electronic Clinical Quality Measures (eCQMs) are standardized metrics that measure and track the quality of healthcare services that eligible professionals (EP), eligible hospitals (EH), and critical access hospitals (CAH) provide. The results of the measures are used to calculate a quality score. This process helps to ensure that our healthcare system is delivering effective, safe, efficient, patient-centered, equitable, and timely care. While the eCQMs are not practice guidelines, they are indicative through measuring positive or negative outcomes of clinical good practices.

eCQM performance rates are used by various governing bodies to evaluate programs and in the case of Centers for Medicare and 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 (IHS RPMS-CEHR) generates patient-based files containing the data needed to create CQM reports in standardized format. These are called Quality Reporting Data Architecture (QRDA) Category I (CAT-I) files.

The ECQM Engine is a browser-enabled graphical user interface for the Indian Health Service (IHS) which extracts the data from multiple CAT-I files and generates QRDA Category III (CAT-III) aggregated report files, which may be submitted to CMS. The ECQM Engine also outputs human-readable reports that can be used in quality improvement activities at individual sites.

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 2015 Edition Health Information Technology certification criteria 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 16 EH/CAH eCQMs and 24 EP eCQMs were selected and are listed in Table 1-1 and Table 1-2.

Table 1-1: IHS – Selected EH/CAH eCQM

CMS ID	Measure Type	Measure
CMS009v8	Newborn	Exclusive Breast Milk Feeding
CMS031v7*	Newborn	Hearing Screening Prior to Hospital Discharge
CMS026v6*	Assessment	Home Management Plan of Care (HMPC) Document Given to Patient/Caregiver
CMS102v7*	Assessment	Assessed for Rehabilitation
CMS032v8*	Emergency Department	Median Time from ED Arrival to ED Departure for Discharged ED Patients
CMS053v7*	Emergency Department	Primary PCI Received within 90 Minutes of Hospital Arrival
CMS055v7*	Emergency Department	Median Time from ED Arrival to ED Departure for Admitted ED Patients
CMS111v8	Emergency Department	Median Admit Decision Time to ED Departure Time for Admitted Patients
CMS113v7*	Delivery	Elective Delivery
CMS071v9	Stroke Prevention	Anticoagulation Therapy for Atrial Fibrillation/Flutter
CMS072v8	Stroke Prevention	Antithrombotic Therapy By End of Hospital Day 2
CMS104v8	Stroke Prevention	Discharged on Antithrombotic Therapy
CMS105v8	Stroke Prevention	Discharged on Statin Medication
CMS107v7*	Stroke Prevention	Stroke-8 Ischemic or hemorrhagic stroke – Stroke education

CMS ID	Measure Type	Measure
CMS108v8	Stroke Prevention	Venous Thromboembolism Prophylaxis
CMS190v8	Stroke Prevention	Intensive Care Unit Venous Thromboembolism Prophylaxis

* Measure was not updated for 2020 and is not eligible to submit to CMS and uses the logic from 2019

Table 1-2: IHS – Selected EP eQMs

CMS ID	Measure Type	Measure
CMS117v8	Pediatric	Childhood Immunization Status
CMS155v8	Pediatric	Weight Assessment and Counseling for Nutrition and Physical Activity for Children and Adolescents
CMS122v8	Diabetes	Diabetes: Hemoglobin A1c (HbA1c) Poor Control (>9%)
CMS131v8	Diabetes	Diabetes: Eye Exam
CMS134v8	Diabetes	Diabetes: Medical Attention for Nephropathy
CMS165v8	Diabetes	Controlling High Blood Pressure
CMS002v9	Other Adult	Screening for Depression and Follow-Up Plan
CMS069v8	Other Adult	Body Mass Index (BMI) Screening and Follow-Up Plan
CMS127v8	Other Adult	Pneumococcal Vaccination Status for Older Adults
CMS138v8	Other Adult	Tobacco Use: Screening and Cessation Intervention
CMS139v8	Other Adult	Falls: Screening for Future Fall Risk
CMS156v8	Other Adult	Use of High-Risk Medications in the Elderly
CMS050v8	Transfer of Health Information and Interoperability	Closing Referral Loop
CMS124v8	Preventive Care	Cervical Cancer Screening
CMS125v8	Preventive Care	Breast Cancer Screening
CMS130v8	Preventive Care	Colorectal Cancer Screening
CMS349v2	Preventive Care	HIV Screening
CMS137v8	Prevention and Treatment of Opioid and Substance Use Disorders	Initiation and Engagement of Alcohol and Other Drug Dependence Treatment
CMS144v8	Management of Chronic Conditions	Heart Failure: Beta-Blocker Therapy for Left Ventricular Systolic Dysfunction
CMS347v3	Management of Chronic Conditions	Statin Therapy for the Prevention and Treatment of Cardiovascular Disease
CMS159v8	Prevention, Treatment, and Management of Mental Health	Depression Remission at Twelve Months
CMS160v7*	Prevention, Treatment, and Management of Mental Health	Depression Utilization of the PHQ-9 Tool

CMS ID	Measure Type	Measure
CMS161v8	Prevention, Treatment, and Management of Mental Health	Adult Major Depressive Disorder: Suicide Risk Assessment
CMS177v8	Prevention, Treatment, and Management of Mental Health	Child and Adolescent Major Depressive Disorder: Suicide Risk Assessment

* Measure was not updated for 2020 and is not eligible to submit to CMS and uses the 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 is used to receive QRDA CAT-I and generate QRDA CAT-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 own directory server (LDAP).

Central install eliminates the need for initial site install and future patching. There will be no need to monitor 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/resources bandwidth constraint during the peak reporting times. Sites will have control of their system's availability, thus avoiding system outages and they are in charge of their own timetable.

The ECQM Engine receives securely transmitted QRDA CAT-I files in XML format for clinical quality measure calculations.

The ECQM Engine authenticates users against a directory service with LDAP (Lightweight Directory Access Protocol). One example of such service is the Microsoft Active Directory. This authentication is necessary to support sites that are in a variety of locations including the Federal D1 network, the Tribal E1 network, and others outside of 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	Individual who performs the following ECQM functions: <ul style="list-style-type: none"> • Install 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	Individual who tracks and monitors all activities performed

ECQM Role	Definition
Site Admin	Individual who performs the following ECQM functions: <ul style="list-style-type: none"> • Upload QRDA CAT-I zip files • Setup compute/reporting groups • Download reports/results • Manage provider lists • Delete/Purge data
Site Auditor	Individual who tracks and monitors sites 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 (**http://IPaddressOFecqmApplicationServer**).
2. The **Login** screen displays.

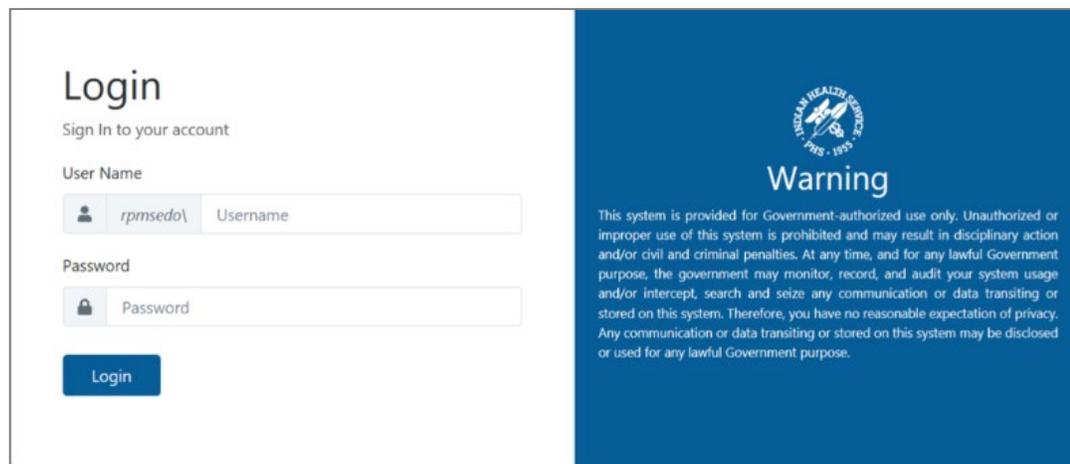


Figure 2-1: ECQM Engine Login Screen

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 to the system.

2.2.1 Sites

Use the **Sites** tab to define/modify site information. Only Super Admin users have access to create sites. Each site is created by the Super Admin with a distinct site profile based on the information included in the QRDA CAT-I files and identifying information used to create the QRDA CAT-III files.

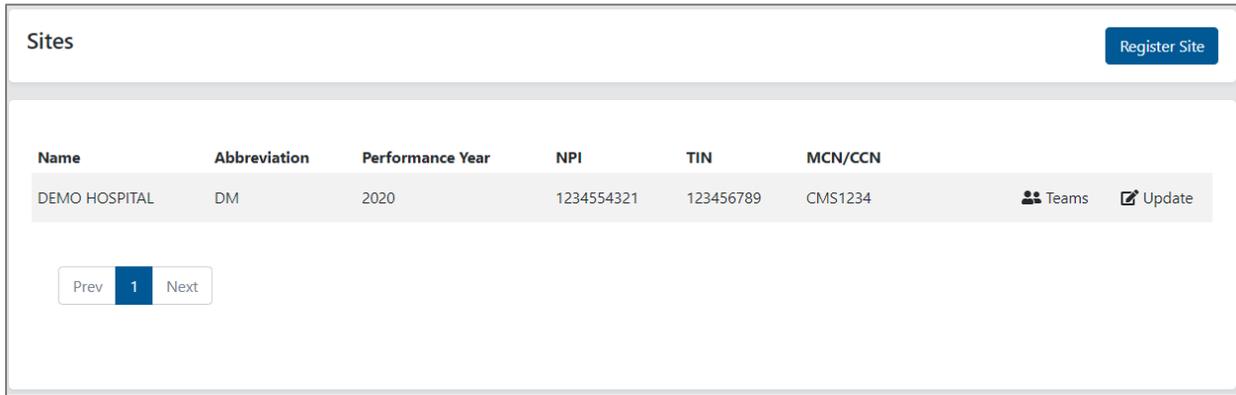


Figure 2-2: Sites screen

2.2.1.1 Create Site

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

Register

New Site

<p>Name</p> <input style="width: 95%;" type="text" value="IHS Test Site"/>	<p>Abbreviation</p> <input style="width: 95%;" type="text" value="ITS"/>
<p>TIN</p> <input style="width: 95%;" type="text" value="123123123"/> <p><small>Tax Identification Number</small></p>	<p>NPI</p> <input style="width: 95%;" type="text" value="1234567890"/> <p><small>National Provider Identifier</small></p>
<p>CCN</p> <input style="width: 95%;" type="text" value="HSZ8"/> <p><small>CMS Certification Number</small></p>	

Address

Street

City State Zip Code

Legal Authenticator

First Name Last Name

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 digit).
5. Under **Legal Authentication**:
 - a. Enter a **First Name**.
 - b. Enter a **Last Name**.

Note: The Legal Authenticator is the person who is associated with the QRDA submission. This could be the Quality Coordinator or the Health Records Management officer of the site. 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.

Update

DEMO HOSPITAL

<p>Name</p> <input style="width: 90%;" type="text" value="IHS TEST SITE"/>	<p>Abbreviation</p> <input style="width: 90%;" type="text" value="ITS"/>
<p>TIN</p> <input style="width: 90%;" type="text" value="123123123"/> <p><small>Tax Identification Number</small></p>	<p>NPI</p> <input style="width: 90%;" type="text" value="1234567890"/> <p><small>National Provider Identifier</small></p>
<p>CCN</p> <input style="width: 90%;" type="text" value="HSZ8"/> <p><small>CMS Certification Number</small></p>	

Address

Street

<p>City</p> <input style="width: 90%;" type="text" value="Albuquerque"/>	<p>State</p> <input style="width: 90%;" type="text" value="NM"/>	<p>Zip Code</p> <input style="width: 90%;" type="text" value="89701"/>
--	--	--

Legal Authenticator

<p>First Name</p> <input style="width: 90%;" type="text" value="AUTH"/>	<p>Last Name</p> <input style="width: 90%;" type="text" value="TEST"/>
---	--

Performance Year

Performance Year

Save Changes
Cancel

Figure 2-4: Update Site screen

2. On the **Update** screen, click the fields to update the site information, address information, and legal authenticator.
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 have access to 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.

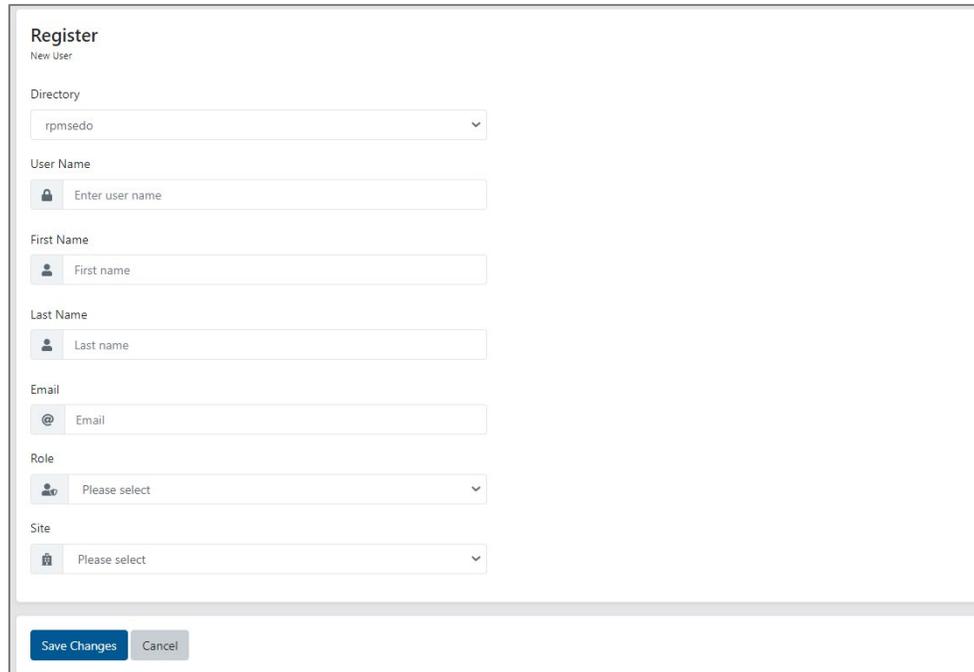
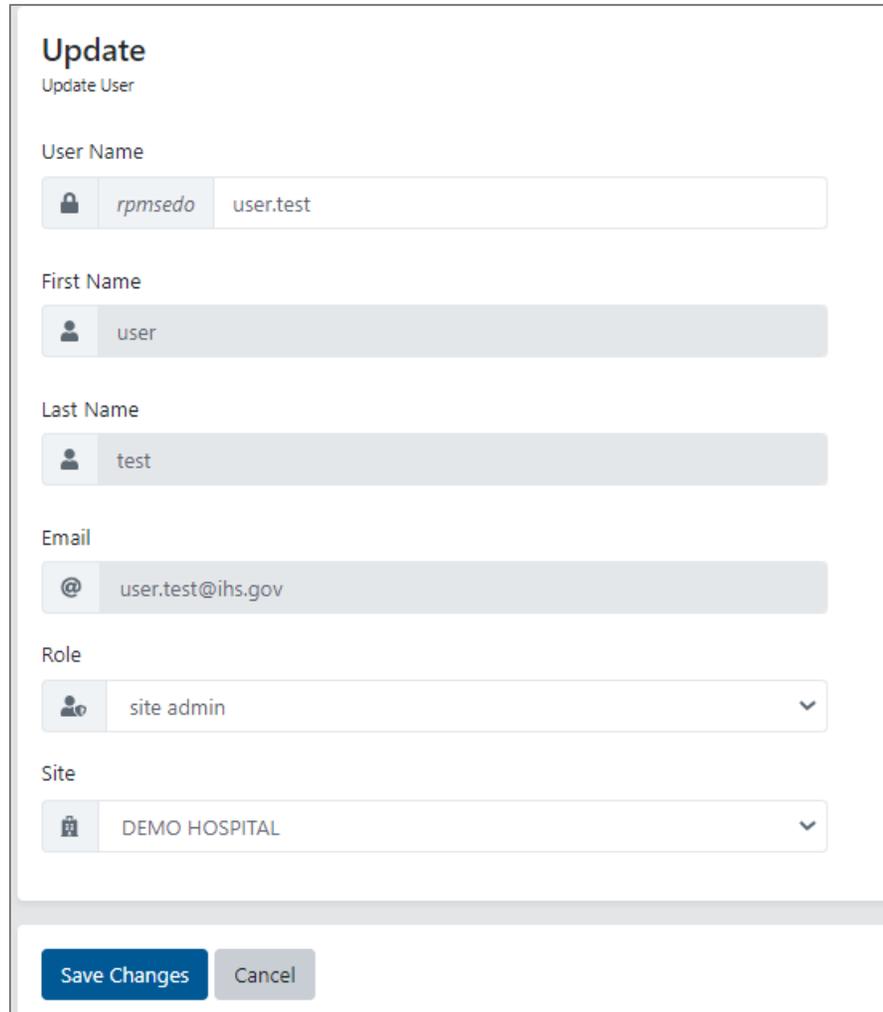


Figure 2-5: Register User screen

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.



Update
Update User

User Name
rpmseedo user.test

First Name
user

Last Name
test

Email
@ user.test@ihs.gov

Role
site admin

Site
DEMO HOSPITAL

Save Changes Cancel

Figure 2-6: Update User screen

2. Only **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 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 Site from the list to view users for the selected site only.
3. Select Role from the list to view users with the selected role.
4. Use combination of the three filters to further narrow down the list.

2.2.3 Diagnostic

Only users in the Super Admin role will be able to view the **Diagnostic** tab. It was originally created for the package development team to troubleshoot issues reported by the site users but may deliver useful insights for Super Admins.

Job Id	Created On	Site	Type	Status
ae911ec3-b810-4c19-adee-b20fda11d79f	10/15/2020 5:35:37 PM	DEMO HOSPITAL	ComputeJob	Complete
070a712c-2d87-4c22-9abf-cdd82f35b179	10/15/2020 5:35:37 PM	DEMO HOSPITAL	ComputeJob	Complete
839b32a0-03c6-4f63-8a00-d4f9e43395ee_0	10/15/2020 5:35:31 PM	DEMO HOSPITAL	PatientImportJob	Complete
ada5128b-edb2-4f3f-997e-77a6709fadb	10/14/2020 9:52:52 PM	DEMO HOSPITAL	ComputeJob	Complete
019e5e87-b4aa-47ae-9f68-b5731b7fc768	10/14/2020 9:52:52 PM	DEMO HOSPITAL	ComputeJob	Complete
a451a1f1-7f27-47d5-952e-a999882a9d6a_0	10/14/2020 9:52:51 PM	DEMO HOSPITAL	PatientImportJob	Complete
d2e8c9e5-55c1-4c45-b271-212a72b274bd	10/14/2020 8:34:01 PM	DEMO HOSPITAL	ComputeJob	Complete
ec13e2e8-3010-4f05-8076-83cb1e23dc95	10/14/2020 8:34:01 PM	DEMO HOSPITAL	ComputeJob	Complete
49c8fcc9-fc6c-48c7-8e95-ac5b2cb68d07_0	10/14/2020 8:33:59 PM	DEMO HOSPITAL	PatientImportJob	Complete
bf31ef85-83ed-4c38-8d81-aae7c976d285	10/13/2020 10:45:26 PM	DEMO HOSPITAL	ComputeJob	Complete
633749e5-ba64-46b1-b5be-57722e127348	10/13/2020 10:45:26 PM	DEMO HOSPITAL	ComputeJob	Complete
e76784a1-d2f4-4990-b0cb-5cb7ab5e83a3_0	10/13/2020 10:45:25 PM	DEMO HOSPITAL	PatientImportJob	Complete
375afe90-5da8-44b9-b97f-c697e35ae109	10/13/2020 10:35:58 PM	DEMO HOSPITAL	ComputeJob	Complete
5c0b87ef-08ee-4333-8e30-5a3ba24d3dd0	10/13/2020 10:31:09 PM	DEMO HOSPITAL	ComputeJob	Complete

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, CAT 3 Export, and computation. The list can be filtered using the filter options.

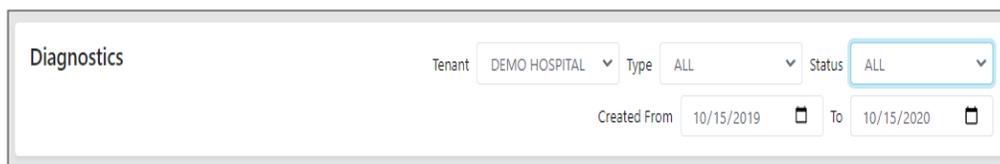


Figure 2-8: Diagnostics tab – Filter Options

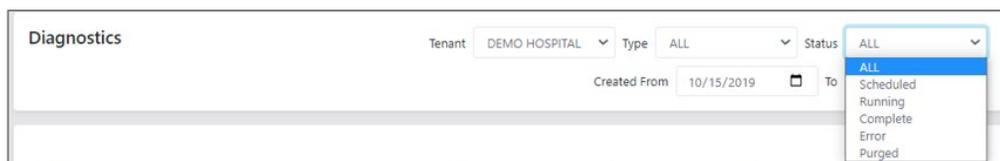


Figure 2-9: Diagnostics tab – Job Status

The **Diagnostics** tab also allows filtering by the job types.

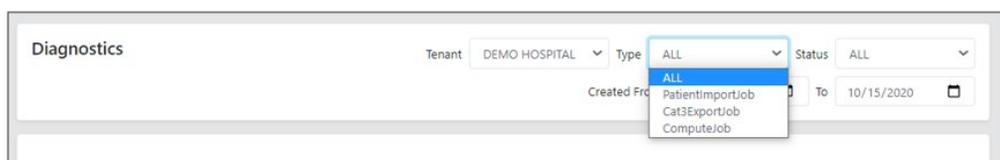


Figure 2-10: Diagnostic tab – Job Type

2.3 Site Admin Menu Options

Site Admins upload QRDA CAT-1 zip files, download reports and results, define the reporting groups (Teams), and update their own site information as needed. 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 individual measures and calculations within the Team selected. 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 is met for each patient. Users will also have an 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 or if there is a new Team or changes 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 display in the list. Any inactive team will display **(Inactive)** next to the team name. Calculations will only be performed on active teams.

3. Select a **year** (current year is defaulted).
4. The dashboard displays the measures and its calculations.

Measure	PERCENTAGE	NUMERATOR	DENOMINATOR
CMS102v7 Clinical Process Effectiveness Assessed for Rehabilitation	% <i>Higher is Better</i>	U	EXCLUSION EXCEPTION
Assessed for Rehabilitation	8.33 %	1	18 6 0
CMS104v8 Clinical Process Effectiveness Discharged on Antithrombotic Therapy	% <i>Higher is Better</i>	U	EXCLUSION EXCEPTION
Discharged on Antithrombotic Therapy	50.00 %	3	11 5 0

Figure 2-11: Dashboard example

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

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

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

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

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

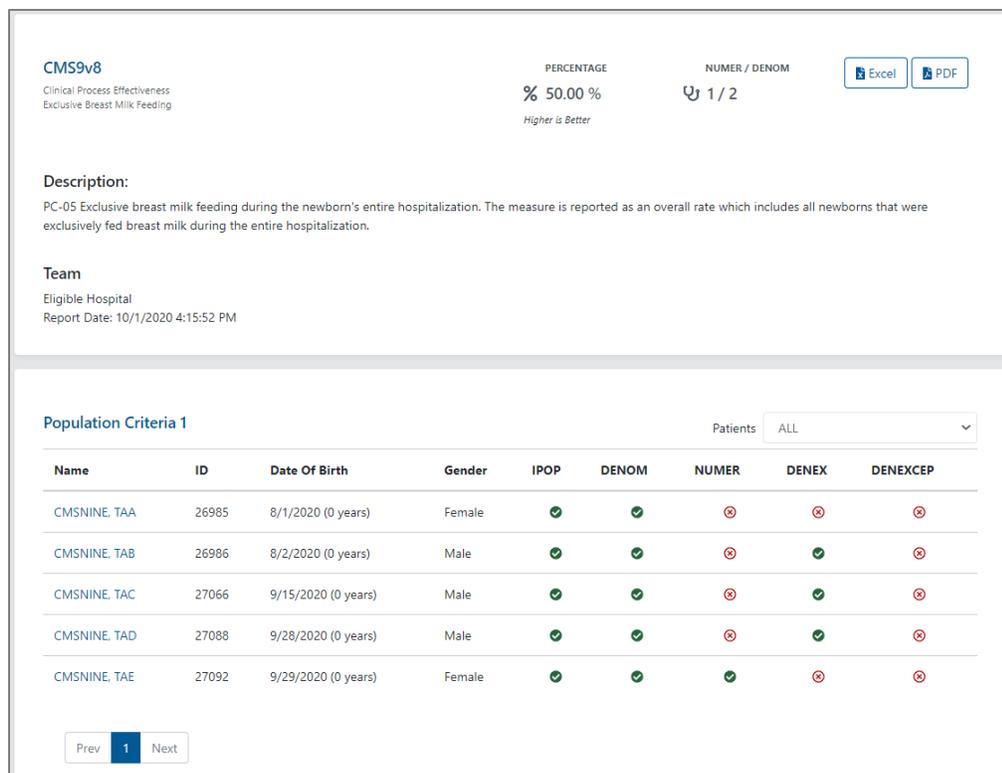


Figure 2-12: Measure Detail Screen example

- To filter patient by measure criteria, select options from the Patients list. For example, selecting **IN DENEX** from the list displays patients that were included in Denominator Exclusion only.
- 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-CMS9v8.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	CMSNINE, TAB	26986	8/2/2020	M	1002-5	2186-5	True	True	False	False
3	CMSNINE, TAC	27066	9/15/2020	M	1002-5	2186-5	True	True	False	False
4	CMSNINE, TAD	27088	9/28/2020	M	2106-3	2186-5	True	True	False	False
5	CMSNINE, TAA	26985	8/1/2020	F	1002-5	2186-5	True	False	False	False
6	CMSNINE, TAE	27092	9/29/2020	F	1002-5	2186-5	True	False	True	False
7										

Figure 2-13: Sample Excel content

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

Click the **PDF** () button to generate a PDF format of the summary report. The PDF document is named automatically. The name format is the Team name, followed by the measure number and version, for example: **Eligible Hospital-CMS9v8.xlsx**.

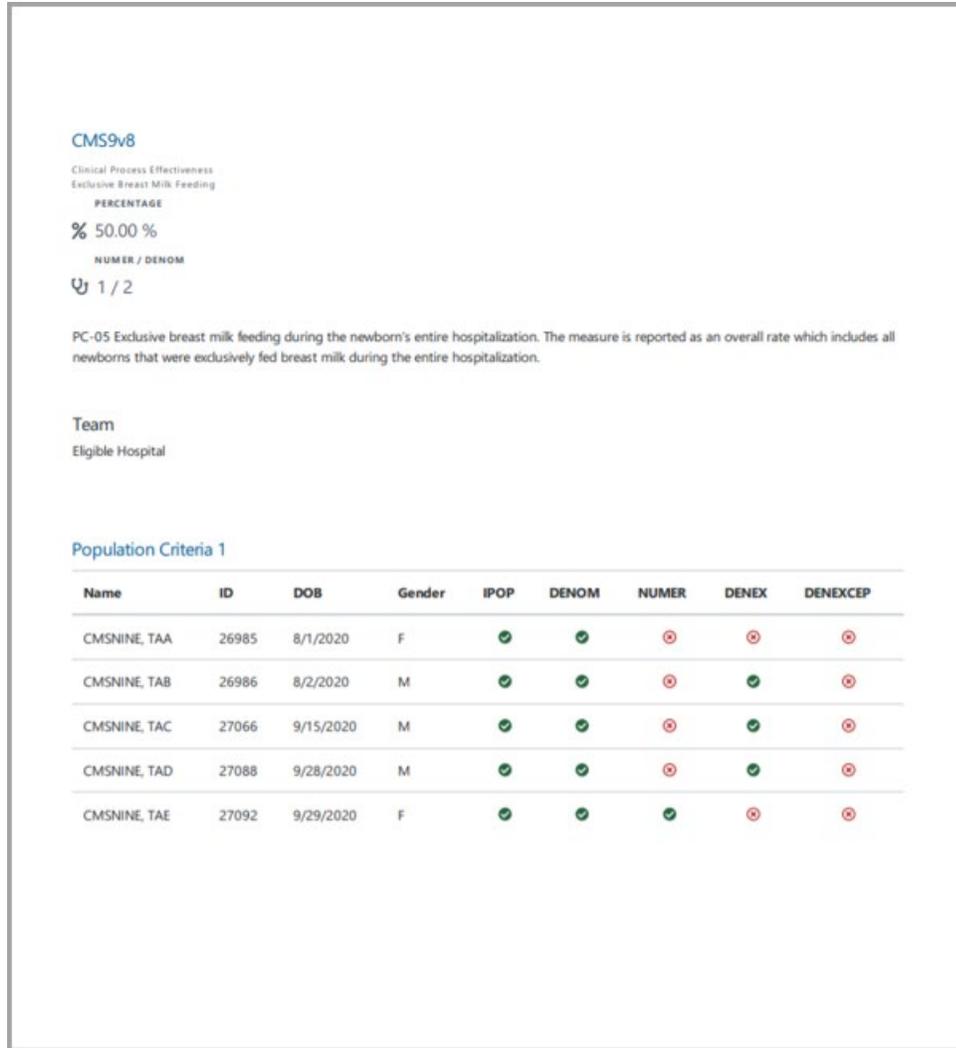


Figure 2-14: Sample PDF

- Click the patient name to view the patient-specific measure detail and the general eCQM information.

Figure 2-15: Patient specific Measure Detail

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

9. Select the **Filter patient data for measure** (Filter patient data for measure) check box to only show the data that is 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 CAT-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.

Import Patients Status [Import Patients](#)

Job Id	Scheduled On	Updated On	File	Status
54574e3f-48b9-4f37-be51-240a5e772c08_0	10/1/2020 7:17:00 PM	10/1/2020 7:17:01 PM	a0efd654-437d-45dd-bafd-55e00d627dcd_0.zip	Complete
949b41be-07be-4a8b-b7ca-aff041a8fdbbc_0	10/1/2020 6:59:53 PM	10/1/2020 6:59:53 PM	abbd566c-1809-428a-ab09-eafeefa17d42_0.zip	Complete
9f6fa348-07bf-4f05-a8ed-40074d8b6f77_0	10/1/2020 5:50:11 PM	10/1/2020 5:50:11 PM	e23e2d45-d5e9-470e-a25c-2b081a4afa11_0.zip	Complete
258db429-e2aa-45a2-bb80-8edb7df819ce_0	10/1/2020 4:15:51 PM	10/1/2020 4:15:51 PM	b9aee72c-29ff-4079-a274-6daec0c6f49b_0.zip	Complete
da29cf1d-23ca-4453-a47f-a909a2faa3f8_0	10/1/2020 3:56:04 PM	10/1/2020 3:56:04 PM	41bfb816-db79-4f9c-bd1b-087cccef6132_0.zip	Complete
2eba7093-fcc9-462e-896c-d30dec01c64e_0	10/1/2020 3:55:02 PM	10/1/2020 3:55:03 PM	41bfb816-db79-4f9c-bd1b-087cccef6132_0.zip	Complete
9c20074a-ef60-4f0f-ba16-58e87f179d26_0	10/1/2020 3:53:56 PM	10/1/2020 3:53:56 PM	298067ee-015e-456b-8f5b-064201b25981_0.zip	Complete
4b0c18b9-3f01-438c-9258-538cd742949e_0	10/1/2020 3:50:10 PM	10/1/2020 3:50:10 PM	bc2f5b18-8b84-4de9-80d1-45eb632e8bd4_0.zip	Complete
55317b2d-f05f-45fb-9dbf-363670cec903_0	10/1/2020 3:45:57 PM	10/1/2020 3:45:57 PM	bc2f5b18-8b84-4de9-80d1-45eb632e8bd4_0.zip	Complete
d68240f9-c78c-4e9d-b35e-48b6c5b7a435_0	10/1/2020 3:40:43 PM	10/1/2020 3:40:43 PM	6f6c0ede-e431-4073-8615-dc24379da32b_0.zip	Complete
924d87ce-2841-45eb-9899-17b01f7cdb67_0	10/1/2020 3:07:57 PM	10/1/2020 3:07:58 PM	9c3ee75e-5da4-45b4-a563-cee22797fc4c_0.zip	Complete
5ff96af5-1fb4-4dad-bd97-72090548792a_0	10/1/2020 2:42:58 PM	10/1/2020 2:42:58 PM	1d363717-ed99-4d53-9694-b216f6b31740_0.zip	Complete
0c40737f-d362-48f7-9d44-38404f5793d9_0	10/1/2020 2:32:19 PM	10/1/2020 2:32:19 PM	ba71bde9-5fb3-4963-8840-4807c6a1d228_0.zip	Complete
3616b82d-dbba-43ba-92cd-a8fc95acc83_0	10/1/2020 2:26:38 PM	10/1/2020 2:26:38 PM	ba71bde9-5fb3-4963-8840-4807c6a1d228_0.zip	Complete
38921c4e-8e75-4a35-9a30-85962c1e4b62_0	10/1/2020 2:18:04 PM	10/1/2020 2:18:04 PM	efa79c2b-89c7-4e28-9d8b-643801af5efe_0.zip	Complete
dc6e783c-95e2-488b-8831-3cb2aa8c0479_0	10/1/2020 2:17:14 PM	10/1/2020 2:17:14 PM	efa79c2b-89c7-4e28-9d8b-643801af5efe_0.zip	Complete
d6fa5455-cbaf-49c5-81fd-3e29eefae2e7_0	10/1/2020 2:07:29 PM	10/1/2020 2:07:29 PM	7bf544f0-7d49-4612-9169-a26ff07a80ff_0.zip	Complete
5339cfc9-e4d6-4275-9440-6d8be4a58e6f_0	10/1/2020 1:56:06 PM	10/1/2020 1:56:10 PM	2bff9235-362a-4b87-a8e3-77ff9af346c_0.zip	Complete

Prev 1 Next

Figure 2-16: Imports Screen

1. Click the **Import Patients** button to upload QRDA CAT-1 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 CAT-I zip file location. Then select a file and click **Open**.



Figure 2-17: Import Patients window

3. Once a file is done uploading, a green indicator displays.

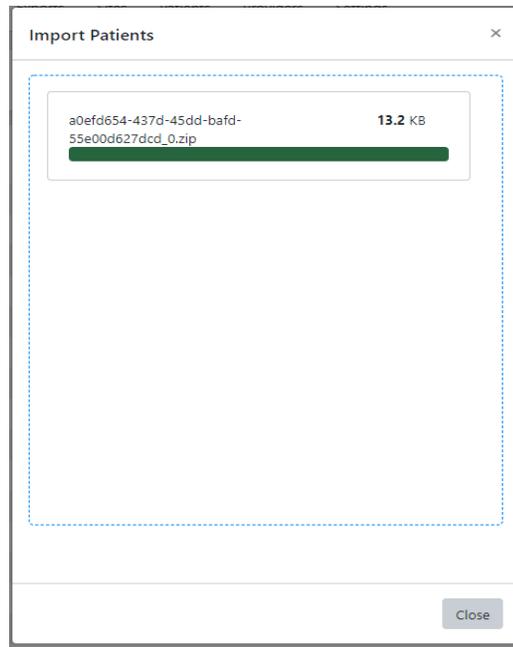


Figure 2-18: Import is complete

4. Click **Close**.

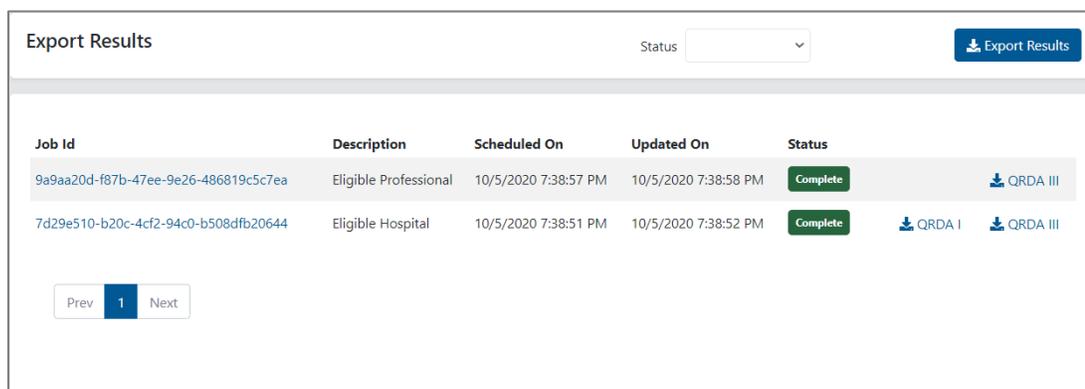
Note: Allow all files to complete before closing the **Import Patient** window.

5. The uploaded files display 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.
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 Export

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



The screenshot shows the 'Export Results' interface. At the top right, there is a 'Status' dropdown menu and a blue 'Export Results' button. Below this is a table with the following columns: Job Id, Description, Scheduled On, Updated On, and Status. Two rows of data are visible, both with a 'Complete' status. The first row is for 'Eligible Professional' and the second for 'Eligible Hospital'. Below the table is a pagination control with 'Prev', '1', and 'Next' buttons.

Job Id	Description	Scheduled On	Updated On	Status
9a9aa20d-f87b-47ee-9e26-486819c5c7ea	Eligible Professional	10/5/2020 7:38:57 PM	10/5/2020 7:38:58 PM	Complete
7d29e510-b20c-4cf2-94c0-b508dfb20644	Eligible Hospital	10/5/2020 7:38:51 PM	10/5/2020 7:38:52 PM	Complete

Figure 2-19: Exports screen

1. Click the **Export Results** button to start a new export.
2. On the **Export Measure Results (QRDA CAT-III)** window, select the Team from the menu.
3. The current **Performance Year** is defaulted.
4. Toggle the **Export Patient Data (QRDA CAT-I)** if QRDA CAT-1 files need to be generated as well. This is optional.
5. Click the **Export** button to start the process.

Note: If the selected Team or year has no calculations available, the message in Figure 2-20 displays to the user.

Export Measure Results Not Found for selected Team/Year

Figure 2-20: Error message

6. The **Status** column will display **Running**, and once done, the **Status** column will display **Complete**.
7. Click the **QRDA-I** button to download CAT-I files.
8. Click the **QRDA-III** button to download CAT-III 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 will only have access to the site that they are linked to. A Site Admin can only be linked to one site.

2.3.4.1 Create Teams

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

The EP Team provides a selection of the 14 EP measures and the EH Team provides a selection of 16 EH measures. When a new site is created the EH and EP 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 and EP) are created for the current Computation/Performance Year. Sites can either modify these teams or create new teams 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** or **EH** 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 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 QRDA I and QRDA II CMS Program based on the site goals and site quality program. 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 EP 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 CAT-I export data. User can only search providers that are in the **Providers** tab.

10. Select the **All Measures** check box to add all or select individual measures to include the measures.
11. Click **Save Changes**.

Register EP Team

Name Computation/Performance Year Active

QRDA I CMS Program QRDA III CMS Program

CMS Program for QRDA CAT-I submission CMS Program for QRDA CAT-III submission

Providers

Measures

<input type="checkbox"/> All Measures
<input type="checkbox"/> CMS117v8 Childhood Immunization Status
<input type="checkbox"/> CMS122v8 Diabetes: Hemoglobin A1c (HbA1c) Poor Control (> 9%)
<input type="checkbox"/> CMS124v8 Cervical Cancer Screening
<input type="checkbox"/> CMS125v8 Breast Cancer Screening
<input type="checkbox"/> CMS127v8 Pneumococcal Vaccination Status for Older Adults
<input type="checkbox"/> CMS130v8 Colorectal Cancer Screening
<input type="checkbox"/> CMS131v8 Diabetes: Eye Exam

Figure 2-21: Register EP Team screen

Register EH Team

Name

Computation/Performance Year

Active

QRDA I CMS Program

CMS Program for QRDA CAT-I submission

QRDA III CMS Program

CMS Program for QRDA CAT-III submission

Measures

<input type="checkbox"/> All Measures
<input type="checkbox"/> CMS104v8 Discharged on Antithrombotic Therapy
<input type="checkbox"/> CMS105v8 Discharged on Statin Medication
<input type="checkbox"/> CMS108v8 Venous Thromboembolism Prophylaxis
<input type="checkbox"/> CMS111v8 Median Admit Decision Time to ED Departure Time for Admitted Patients
<input type="checkbox"/> CMS190v8 Intensive Care Unit Venous Thromboembolism Prophylaxis
<input type="checkbox"/> CMS71v9 Anticoagulation Therapy for Atrial Fibrillation/Flutter
<input type="checkbox"/> CMS72v8 Antithrombotic Therapy By End of Hospital Day 2
<input type="checkbox"/> CMS9v8 Exclusive Breast Milk Feeding
<input type="checkbox"/> CMS26v6 Home Management Plan of Care (HMPC) Document Given to Patient/Caregiver (Not Reportable)
<input type="checkbox"/> CMS102v7 Assessed for Rehabilitation (Not Reportable)

Figure 2-22: Register EH 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 **CMS Program** as appropriate.
5. Select or clear **Measures**, as needed.
6. Click **Save Changes**.

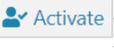
2.3.4.3 Activate/Inactivate Teams

1. Click the **Team** icon.
2. Click the **Deactivate** ( Deactivate) icon next to inactivate an active team.
3. The page refreshes and the Team displays as **Inactive**.

Teams						Register Team
Name	Type	Performance Year	Total Providers	Total Measures		
Eligible Hospital	EH	2020	0	16	Inactive	Activate Update

Figure 2-23: 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**.

- Click the **Activate** () icon next to the inactive team to reactivate the team.
- The page refreshes and the Team displays as **Active**.

Teams						Register Team
Name	Type	Performance Year	Total Providers	Total Measures		
Eligible Hospital	EH	2020	0	16	Active	Deactivate Update

Figure 2-24: Team screen – Active Team

Note: A user can also reactivate a team by clicking the **Update** icon, clearing the **Active** check box, 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 that have been loaded in ECQM. The list includes Name, Id (IEN), DOB, Gender, Race, and Ethnicity. From the Patients tab, users will be able to check if the patient qualifies for a particular measure.

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

The screenshot displays the 'Sample Measure Detail from Patients tab' for patient CMSTWO, TAA. At the top, patient information is shown: DOB: 9/9/2004, Gender: Male, Race: White, Ethnicity: Not Hispanic/Latino, and DFN: 26970. Below this, a dropdown menu shows the selected measure: 'CMS2v9 Preventive Care and Screening: Screening for Depression and Follow Up Plan', with a checked box for 'Filter patient data for measure'. The main content is divided into two columns. The left column contains definitions for 'Initial Population', 'Denominator', 'Numerator', 'Denominator Exclusions', and 'Denominator Exceptions'. The right column lists several encounters with their respective codes (e.g., 308335008, 96110, 73831-0), encounter types (SNOMEDCT, CPT, LOINC), and dates. A 'Result' box at the bottom right shows the value '428171000124102'. The version 'ECQM 3.0' is noted at the bottom left of the interface.

Figure 2-25: Sample Measure Detail from Patients tab

2.3.6 Providers

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

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 display.
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 patient data that has been imported. Performing this action will permanently delete imported patient data, exports, and providers. The Teams will not be deleted. Providers who were added in Teams will not be deleted. The user will have to delete manually under Teams.

Warning: This process cannot be undone.

1. Click the **Delete** button to start the deletion process.
2. A warning message displays (Figure 2-26). Click the **Delete Patient Data** button to continue.



Figure 2-26: 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 creation of sites, defining users and teams, login, and logout. The Super Auditor can search or filter by user, event type, and date range. The Super Auditor role is created by Super Admin.

Audit

User Name: Category: Type: Event:

From Date: To Date: Sort By:

Time	User	Category	Type	Event	Description	
10/16/2020 11:55:59 AM	RP	\LA	Authentication	Login	Login	Authentication Succeeded
10/16/2020 11:55:48 AM	RP	\LA	Authentication	Login	Login	Authentication Failed:
10/16/2020 11:50:52 AM	RP		Authentication	Logout	Logout	Signout
10/16/2020 11:36:50 AM	RP		Configuration	Query	Sites	
10/16/2020 11:36:45 AM	RP		Authentication	Login	Login	Authentication Succeeded
10/16/2020 11:36:08 AM	RP		Authentication	Logout	Logout	Signout
10/16/2020 11:22:06 AM	RP		Authentication	Login	Login	Authentication Succeeded
10/16/2020 11:09:23 AM	RP		Configuration	Query	Teams	
10/16/2020 11:09:21 AM	RP		Configuration	Query	Sites	
10/16/2020 11:09:05 AM	RP		Configuration	Query	Sites	
10/16/2020 11:03:36 AM	RP		Authentication	Login	Login	Authentication Succeeded
10/16/2020 10:27:58 AM	RP		Authentication	Logout	Logout	Signout
10/16/2020 10:25:26 AM	RP		Authentication	Login	Login	Authentication Succeeded
10/16/2020 10:13:44 AM	RP		Configuration	Query	Sites	
10/16/2020 10:13:43 AM	RP		Authentication	Login	Login	Authentication Succeeded
10/16/2020 7:08:29 AM	RP	WAY	Authentication	Login	Login	Authentication Succeeded

Figure 2-27: 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. The Site Auditor role is created by Super Admins.

The screenshot shows the 'Audit' screen with a filter form and a table of audit events. The filter form includes fields for User Name, Category, Type, Event, From Date, To Date, and Sort By, along with a Filter button. The table below shows a list of audit events with columns for Time, User, Category, Type, Event, and Description.

Time	User	Category	Type	Event	Description
10/15/2020 7:27:27 PM	RI	A	Configuration	Query	Teams
10/15/2020 7:27:27 PM	RI	A	Configuration	Update	Teams
10/15/2020 7:26:13 PM	RI	A	Configuration	Query	Teams
10/15/2020 7:26:13 PM	RI	A	Configuration	Update	Teams
10/15/2020 7:22:59 PM	RI	A	Configuration	Query	Teams
10/15/2020 7:22:57 PM	RI	A	Configuration	Query	Teams
10/15/2020 7:22:55 PM	RI	A	Configuration	Query	Sites
10/15/2020 7:10:03 PM	RI	A	PatientData	Download	QRDAI
10/15/2020 7:08:10 PM	RI	A	PatientData	Schedule	QRDA
10/15/2020 7:00:21 PM	RI	N	Authentication	Login	Login Authentication Succeeded
10/15/2020 6:59:25 PM	RI	A	PatientData	Upload	Patient Data Upload
10/15/2020 6:44:45 PM	RI	N	PatientData	Upload	Patient Data Upload
10/15/2020 6:33:20 PM	RI	N	PatientData	Upload	Patient Data Upload
10/15/2020 6:33:09 PM	RI	N	Authentication	Login	Login Authentication Succeeded
10/15/2020 6:31:26 PM	RI	A	Configuration	Query	Teams
10/15/2020 6:31:23 PM	RI	A	Configuration	Query	Teams

Figure 2-28: 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 that is **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.

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

- For a listing of general ROB for all users, see the most recent edition of *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>

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

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 the documentation of that application (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 employer before providing any type of information system access, sensitive information, or nonpublic agency information.
- Be aware that personal use of information resources is authorized on a limited basis within the provisions *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 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, or 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 specifically 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 the functions they perform, such as system administrator or application administrator.
- Acquire a written preauthorization in accordance with IHS policies and procedures prior to interconnection to or transferring data from RPMS.

A.1.3 Accountability

RPMS users shall:

- Behave in an ethical, technically proficient, informed, and trustworthy manner.
- 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 one person has sole access to or control over important resources.
- Protect all sensitive data entrusted to them as part of their government employment.

- Abide by all Department and Agency policies and 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 prior to 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 that data is in the vicinity.
- 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, and/or 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.
- Use freeware, shareware, or public domain software on/with the system without their manager's written permission and without scanning it for viruses first.

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 time 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 lower case letter, and one number. It is recommended, if possible, that a special character also be used in the password.
- Change vendor-supplied passwords immediately.
- Protect passwords by committing them to memory or store them in a safe place (do not store passwords in login scripts or batch files).
- Change passwords immediately if 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 the use of 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 an obvious 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

RPMS system implements system-based timeouts that back users out of a prompt after no more than 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 own 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 authentication of the remote user through the use of ID and password or other acceptable technical means.
- Outline the work requirements and the security safeguards and procedures the employee is expected to 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/or stored at alternate work locations.

Remote RPMS users shall:

- Remotely access RPMS through a virtual private network (VPN) whenever possible. Use of direct dial in access must be justified and approved in writing and its use secured in accordance with industry best practices or government procedures.

Remote RPMS users shall not:

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

A.2 RPMS Developers

RPMS developers shall:

- Always be mindful of protecting the confidentiality, availability, and integrity of RPMS when writing or revising code.
- Always follow the IHS RPMS Programming Standards and Conventions (SAC) when developing for RPMS.
- Only access information or code within the namespaces for which 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 separation of duties, policies, and procedures to the fullest extent possible.
- Document or comment all changes to any RPMS software at the time the change or update is made. Documentation shall include the programmer's initials, date of change, and reason for the change.
- Use checksums or other integrity mechanism when releasing their certified applications to assure the integrity of the routines within their RPMS applications.
- Follow industry best standards for systems they are assigned to develop or 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 who have significant access to processes and data in RPMS, such as, system security administrators, systems administrators, and database administrators, have added responsibilities to ensure the secure operation of RPMS.

Privileged RPMS users shall:

- Verify that any user requesting access to any RPMS system has completed the appropriate access request forms.
- Ensure that government personnel 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 has responsibility for several functions (i.e., 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 accountability, integrity, confidentiality, and availability of the system.
- Replace passwords when a compromise is suspected. Delete user accounts as quickly as possible from the time that the user is no longer authorized 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 authority to grant authorizations to others, review these other authorizations. Retrieve any devices used to gain access to the system or equipment. Cancel logon IDs and passwords and delete or reassign related active and backup files.

- Use a suspend program to prevent an unauthorized user from logging on with the current user's ID if the system is left on and unattended.
- Verify the identity of the user when resetting passwords. This can be done either in person or 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 admission.

Clinical Quality Measures

Standardized metrics that measure and track the quality of health care services by EPs, 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
CAT-I	QRDA Category I (Patient Data) File
CAT-III	QRDA Category III (Aggregated Data) File
CEHR	Certified Electronic Health Record
CEHRT	Certified Electronic Health Record Technology
CMS	Centers for Medicare and Medicaid Services
CQM	Clinical Quality Measures
eCQM	Electronic Clinical Quality Measures
ECQM	Electronic Clinical Quality Measure Engine
ED	Emergency Department
EH	Eligible Hospital
EHR	Electronic Health Records
EP	Eligible Professional
IHS	Indian Health Service
ISSO	Information System Security Officer
IT	Information Technology
JSON	JavaScript Object Notation
OIT	Office of Information Technology
QRDA	Quality Reporting Document Architecture
RPMS	Resource and Patient Management System
XML	eXtensible Markup Language

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