# Table of Contents

1.0 **Introduction** ......................................................................................................... 1  
  1.1 eCQM Overview .................................................................................................. 1  
  1.2 More Information .............................................................................................. 2  

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 ..................................................................................................... 10  
  2.3 Site Admin Menu Options ............................................................................... 13  
    2.3.1 Dashboard .............................................................................................. 13  
    2.3.2 Sites ..................................................................................................... 14  
    2.3.3 Imports ................................................................................................ 18  
    2.3.4 Export .................................................................................................. 19  
    2.3.5 Providers ............................................................................................. 21  
    2.3.6 Settings ............................................................................................... 21  
  2.4 Super Auditor Menu Options .......................................................................... 22  
  2.5 Site Auditor Menu Options ............................................................................. 25  

Appendix A: **Rules of Behavior** .............................................................................. 27  
  A.1 All RPMS Users ......................................................................................... 27  
    A.1.1 Access ................................................................................................. 27  
    A.1.2 Information Accessibility ....................................................................... 28  
    A.1.3 Accountability ..................................................................................... 28  
    A.1.4 Confidentiality .................................................................................. 29  
    A.1.5 Integrity ............................................................................................. 29  
    A.1.6 System Logon ..................................................................................... 30  
    A.1.7 Passwords ......................................................................................... 30  
    A.1.8 Backups ............................................................................................... 31  
    A.1.9 Reporting .......................................................................................... 31  
    A.1.10 Session Timeouts ............................................................................ 31  
    A.1.11 Hardware ......................................................................................... 31  
    A.1.12 Awareness ...................................................................................... 32  
    A.1.13 Remote Access ............................................................................... 32  
  A.2 RPMS Developers ........................................................................................ 33  
  A.3 Privileged Users............................................................................................ 33  

**Glossary** ....................................................................................................................... 36  

**Acronym List** ............................................................................................................... 37  

**Contact Information** .................................................................................................... 38
Preface

Electronic Clinical Quality Measures (eCQMs) are standardized metrics that measure and track the quality of health care services that eligible professionals (EPs), eligible hospitals (EHs), and critical access hospitals (CAHs) provide. The results of the measures are used to calculate a quality score. This process helps to ensure that our health care 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 & 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 (ECQM) application.

1.1 eCQM Overview

eCQMs are a component of the 2015 Edition Health Information Technology (Health IT) 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 12 EP eCQMs were selected and are listed in Table 1-1 and Table 1-2.

Table 1-1: IHS – Selected EH/CAH eCQM

<table>
<thead>
<tr>
<th>CMS ID</th>
<th>MEASURE TYPE</th>
<th>MEASURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMS9v6</td>
<td>Newborn</td>
<td>Exclusive Breast Milk Feeding</td>
</tr>
<tr>
<td>CMS31v6</td>
<td>Newborn</td>
<td>Hearing Screening Prior to Hospital Discharge</td>
</tr>
<tr>
<td>CMS26v5</td>
<td>Assessment</td>
<td>Home Management Plan of Care (HMPC) Document Given to Patient/Caregiver</td>
</tr>
<tr>
<td>CMS102v6</td>
<td>Assessment</td>
<td>Assessed for Rehabilitation</td>
</tr>
<tr>
<td>CMS32v7</td>
<td>Emergency Department</td>
<td>Median Time from ED Arrival to ED Departure for Discharged ED Patients</td>
</tr>
<tr>
<td>CMS53v6</td>
<td>Emergency Department</td>
<td>Primary PCI Received within 90 Minutes of Hospital Arrival</td>
</tr>
<tr>
<td>CMS55v6</td>
<td>Emergency Department</td>
<td>Median Time from ED Arrival to ED Departure for Admitted ED Patients</td>
</tr>
<tr>
<td>CMS111v6</td>
<td>Emergency Department</td>
<td>Median Admit Decision Time to ED Departure Time for Admitted Patients</td>
</tr>
<tr>
<td>CMS113v6</td>
<td>Delivery</td>
<td>Elective Delivery</td>
</tr>
<tr>
<td>CMS71v7</td>
<td>Stroke Prevention</td>
<td>Anticoagulation Therapy for Atrial Fibrillation/Flutter</td>
</tr>
<tr>
<td>CMS72v6</td>
<td>Stroke Prevention</td>
<td>Antithrombotic Therapy By End of Hospital Day 2</td>
</tr>
<tr>
<td>CMS104v6</td>
<td>Stroke Prevention</td>
<td>Stroke-2 Ischemic stroke – Discharged on Anti-thrombotic Therapy</td>
</tr>
<tr>
<td>CMS105v6</td>
<td>Stroke Prevention</td>
<td>Discharged on Statin Medication</td>
</tr>
</tbody>
</table>
### Electronic Clinical Quality Measures (eCQM) Engine (ECQM) Version 1.0

#### User Manual Introduction

January 2019

**Table 1-2: IHS – Selected EP eCQMs**

<table>
<thead>
<tr>
<th>CMS ID</th>
<th>MEASURE TYPE</th>
<th>MEASURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMS107v6</td>
<td>Stroke Prevention</td>
<td>Stroke-8 Ischemic or hemorrhagic stroke – Stroke education</td>
</tr>
<tr>
<td>CMS108v6 *</td>
<td>Stroke Prevention</td>
<td>Venous Thromboembolism Prophylaxis</td>
</tr>
<tr>
<td>CMS190v6 *</td>
<td>Stroke Prevention</td>
<td>Intensive Care Unit Venous Thromboembolism Prophylaxis</td>
</tr>
</tbody>
</table>

* New measure added in 2018

---

**Table 1-2: IHS – Selected EP eCQMs**

<table>
<thead>
<tr>
<th>CMS ID</th>
<th>MEASURE TYPE</th>
<th>MEASURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMS117v6</td>
<td>Pediatric</td>
<td>Childhood Immunization Status</td>
</tr>
<tr>
<td>CMS155v6</td>
<td>Pediatric</td>
<td>Weight Assmnt/Counseling for Nutrition/Physical Activity Children/Adolescents</td>
</tr>
<tr>
<td>CMS122v6</td>
<td>Diabetes</td>
<td>Diabetes: Hemoglobin A1c (HbA1c) Poor Control (&gt;9%)</td>
</tr>
<tr>
<td>CMS131v6</td>
<td>Diabetes</td>
<td>Diabetes: Eye Exam</td>
</tr>
<tr>
<td>CMS134v6</td>
<td>Diabetes</td>
<td>Diabetes: Medical Attention for Nephropathy</td>
</tr>
<tr>
<td>CMS165v6</td>
<td>Diabetes</td>
<td>Controlling High Blood Pressure</td>
</tr>
<tr>
<td>CMS2v7</td>
<td>Other Adult</td>
<td>Preventive Care and Screening: Screening for Clinical Depression and Follow-up</td>
</tr>
<tr>
<td>CMS69v6</td>
<td>Other Adult</td>
<td>Preventive Care and Screening: Body Mass Index (BMI) Screening and Follow-up</td>
</tr>
<tr>
<td>CMS127v6 *</td>
<td>Other Adult</td>
<td>Pneumococcal Vaccination Status for Older Adults</td>
</tr>
<tr>
<td>CMS138v6</td>
<td>Other Adult</td>
<td>Preventive Care/Screening: Tobacco Use: Screening and Cessation Intervention</td>
</tr>
<tr>
<td>CMS139v6 *</td>
<td>Other Adult</td>
<td>Falls: Screening for Future Fall Risk</td>
</tr>
<tr>
<td>CMS156v6 *</td>
<td>Other Adult</td>
<td>Use of High-Risk Medications in the Elderly</td>
</tr>
</tbody>
</table>

* New measure added in 2018

---

**1.2 More Information**

The following websites provide additional CQM information:

- eCQI Resource Center: [https://ecqi.healthit.gov/](https://ecqi.healthit.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 file(s) in both XML and JSON format for clinical quality measure calculations. JSON file(s) generated using the BQRE Extraction Tool are automatically transmitted to the ECQM Engine over an HTTPS (SSL) connection using an application API Token to ensure secure communication.

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 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

<table>
<thead>
<tr>
<th>ECQM Role</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super Admin</td>
<td>Individual who performs the following ECQM functions:</td>
</tr>
<tr>
<td></td>
<td>• Install Engine for the first time using D1/E1 credentials</td>
</tr>
<tr>
<td></td>
<td>• Specify Super Auditor (other than self)</td>
</tr>
<tr>
<td></td>
<td>• Create Site accounts</td>
</tr>
<tr>
<td></td>
<td>• Specify Site Admin User</td>
</tr>
<tr>
<td></td>
<td>• Specify Site Auditor (other than Site Admin User)</td>
</tr>
<tr>
<td>ECQM Role</td>
<td>Definition</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Super Auditor</td>
<td>Individual who tracks and monitors all activities performed</td>
</tr>
<tr>
<td>Site Admin</td>
<td>Individual who performs the following ECQM functions:</td>
</tr>
<tr>
<td></td>
<td>• Upload QRDA CAT-I zip files</td>
</tr>
<tr>
<td></td>
<td>• Setup compute/reporting groups</td>
</tr>
<tr>
<td></td>
<td>• Download reports/results</td>
</tr>
<tr>
<td></td>
<td>• Manage provider lists</td>
</tr>
<tr>
<td></td>
<td>• Delete/Purge data</td>
</tr>
<tr>
<td>Site Auditor</td>
<td>Individual who tracks and monitors sites activities</td>
</tr>
</tbody>
</table>

### 2.1 Log In/Log Out

1. Open your Internet Explorer browser and type in the IP address of the server where the ECQM application has been installed (http://IPaddressO FECQMApplicationServer).

2. The Login screen displays.

![Login Screen](image)

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.

![Sites screen]

Figure 2-2: Sites screen

2.2.1.1 Create Site

1. Click the Register Site button to register a new site.
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)
   f. Select **CMS Program**
      Options are:
      - **MIPS_INDIV**
      - **MIPS_GROUP**
4. Under **Address**:
   a. Enter a **Street**
   b. Enter a **City**
   c. Enter a **State**
   d. Enter a **Zip Code** (5 digit or 9 digit)

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

<table>
<thead>
<tr>
<th>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.</th>
</tr>
</thead>
</table>

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.
2. On the **Update** screen, click on the field(s) that needed to be updated.

3. Enter the correct information.

4. Under **API Key** an API Token can be generated to be used when auto transmitting QRDA CAT-I file in JSON format from the eCQM Export Tool (BQRE). The **API Key** and **Site ID** must be copied to the BQRE’s Site Profile. Click the **Generate Key** button to generate an API key or leave blank if auto transmission will not be used.

5. Click **Save Changes**.

6. Click **Cancel** to discard any changes.
2.2.2 Users

Use the Users tab to create/modify/deactivate user(s). Only Super Admin users have access to create users 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/deactivate a user.

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

![Figure 2-5: Register User screen](image)

2. On the Register screen:
   a. Select Directory from the drop-down 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/update.

![Update User screen](image)

Figure 2-6: Update User screen.

2. Only Role and Site can be edited.
3. Click Save Changes.
4. Click Cancel to discard all changes.

2.2.2.3 Deactivate a User
Click the Deactivate button next to a user that needs to be deactivated.

2.2.2.4 Reactivate a User
1. Click the Activate button next to user to reactivate a user.
2. Click the Update button to review information and make changes as needed.
3. Click **Save Changes** to save the changes.

4. Click **Cancel** to discard all changes.

### 2.2.2.5 Viewing the Diagnostic Tab

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.

![Diagnostics tab](image)

Figure 2-7: **Diagnostics** tab

It displays information about ECQM jobs that are currently running, have completed running, are scheduled to run, or have errored out.

![Diagnostics tab - Job Status](image)

Figure 2-8: **Diagnostics** tab – **Job Status**

The **Diagnostics** tab also allows filtering by the type of jobs.
2.3 Site Admin Menu Options

Site Admins upload QRDA CAT-I zip files, downloads reports/results, defines 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 Team selected and reporting period, the Dashboard displays the individual measures and its calculations within the Team selected. Calculations will include percentage or average time, numerator counts, denominator counts, and stratifications for each measure. The I ( ) icon next to the measure displays a brief description of the measures by hovering the mouse over the icon. 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 are performed.

1. Click the Teams drop-down 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 drop-down list. Any inactive team will display (Inactive) next to the team name. Calculations will only be performed on active teams.

3. Select a Year.

4. The Dashboard displays the measures and its calculations.
2.3.2 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.

2.3.2.1 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: Eligible Professional (EP) and Eligible Hospital (EH). The EP Team provides a selection of the 12 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 are marked as INACTIVE. The Engine Site Admin must activate the teams in order for the ECQM to perform calculations. The pre-defined Teams (EH and EP) are created for the 2018 Computation/Performance Year. Sites can either modify these teams to reflect the current performance year or create new teams for the new performance year.

To create a new team, follow the steps below:

1. Click the Team icon.
2. Click Register Team to create a new team.
3. Select either EP or EH from the drop-down menu.
4. Enter the Name of the Team (maximum of 30 characters).
5. Select the appropriate Computation/Performance Year from the drop-down list.
6. Click the **Active** checkbox.

7. If **EP** is selected from drop down list, the **Include Provider** checkbox is available for selection. This field is optional.
   
a. Enter a partial name of the provider to be added.

b. Select the correct provider from the returned list.

c. Click **Add**.

   **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.

8. Click the **Measures** checkbox to include the measures.

9. Click **Save Changes**.
Figure 2-11: **Register EP Team** screen
2.3.2.2 Modify Teams

1. Click the Team icon.

2. Click the Update button next to a team to modify a team.

3. Modify the Name and Computation/Performance Year as appropriate.

4. Check/uncheck Measures as needed.

5. If Teams need to be inactivated uncheck the Active check box.

6. Click Save Changes.

Figure 2-12: Register EH Team screen
2.3.2.3 Update Sites

See Section 2.2.1.2 on how to Modify Site information.

2.3.3 Imports

Use the Imports tab to upload the QRDA CAT-I zip file(s). The Imports screen also displays historical imports if available. QRDA CAT-I file(s) in JSON format from BQRE Extraction Tool is automatically imported in the eCQM Engine over an HTTPS (SSL) connection using an application API Token. The Imports screen displays the Scheduled Date/Time of when the files are uploaded, the Job ID, the file name, and the Status. If the QRDA CAT-I is from auto-transmission, AUTO PUSH FROM BQRE displays in the File column.

Figure 2-13: Imports Screen

1. Click the Import Patients button to upload QRDA CAT-I zip files. Multiple files can be uploaded.

2. Navigate to where the zip files are located, then drag and drop the zip file to the Import Patients window or click inside the Import Patients window. Navigate to the QRDA CAT-I zip file location, then select and click Open.
3. Click **Close**.

   **Note:** Allow all file(s) to complete before closing the **Import Patient** window.

4. The uploaded files display in the **Imports** window.

5. Status will display **Complete** once the upload is done.

6. To view the results and calculations, click on the **Dashboard** menu option and select the appropriate Team and Year.

### 2.3.4 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.
1. Click on the **Export Results** button to start a new export.

2. On the **Export Measure Results (QRDA CAT-III)** window, select the Team from the drop-down menu.

3. Select the Year.

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 following message is displayed to the user.

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

7. Click on the **QRDA-I** button to download CAT-I files.

8. Click on the **QRDA-III** button to download CAT-III files.
2.3.5 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 Provider tab. Provider(s) 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 Providers button to add a new provider.

2. On the Add Provider screen:
   a. Enter Provider’s First Name
   b. Enter Provider’s Last Name
   c. Enter NPI (10 digits)

   **Note:** Provider must have a valid NPI.

3. Click Add.

4. Click Close to cancel.

2.3.6 Settings

Use the Settings tab to delete/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 that 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. Click the Delete Patient Data.
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 on 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/logout, and patient data downloads. Super Auditor can search or filter by user, event type, and date range. Super Auditor is created by Super Admin.
Figure 2-18: Super Auditor screen

Follow the steps below to filter actions in the **Audit** screen:

1. Enter **User Name** (format is `domain\username` and if it is a data upload auto transmission, it will say **AUTO PUSH FROM BQRE** for user name).

2. Select a **Category** from the drop-down list. Options are:
   - **Authentication**
   - **PatientData**
   - **Configuration**

3. Select **Type**. Options are:
   - **Login**
   - **Logout**
- Delete
- Create
- Update
- Activate
- Deactivate
- Query
- Upload
- Download
- Schedule

3. Enter Event. Examples of events are:
   - Login
   - Logout
   - Sites
   - Teams
   - QRDA
   - QRDA I
   - QRDA III
   - Patient Data Upload
   - Delete

4. Enter From Date and To Date.

5. Select Sort By:
   - Time Descending
   - Time Ascending
   - Category
   - Type
   - Event

6. 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. Site Auditor can search or filter by user, event type, and date range. Site Auditor is created by Super Admins.

![Site Auditor screen](image)

Follow the steps below to filter actions in the Audit screen:

1. Enter **User Name** (format is `domain\username`).
2. Select a **Category** from the drop-down list. Options are:
   - **Authentication**
   - **PatientData**
   - **Configuration**
3. Select **Type**. Options are:
   - Login
   - Logout
   - Delete
   - Create
   - Update
   - Activate
   - Deactivate
   - Query
   - Upload
   - Download
   - Schedule

4. Enter **Event**. Examples of events are:
   - Login
   - Logout
   - Sites
   - Teams
   - QRDA
   - QRDA-I
   - QRDA-III
   - Patient Data Upload
   - Delete

5. Enter **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 (HHS), 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 Web site: http://security.ihs.gov/.

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 (PCs).
- 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 eligible professionals, eligible hospitals, and critical access hospitals.

**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

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAT-I</td>
<td>QRDA Category I (Patient Data) File</td>
</tr>
<tr>
<td>CAT-III</td>
<td>QRDA Category III (Aggregated Data) File</td>
</tr>
<tr>
<td>CEHRT</td>
<td>Certified Electronic Health Record Technology</td>
</tr>
<tr>
<td>CMS</td>
<td>Centers for Medicare and Medicaid Services</td>
</tr>
<tr>
<td>CQM</td>
<td>Clinical Quality Measures</td>
</tr>
<tr>
<td>eCQM</td>
<td>Electronic Clinical Quality Measures</td>
</tr>
<tr>
<td>ED</td>
<td>Emergency Department</td>
</tr>
<tr>
<td>EH</td>
<td>Eligible Hospital</td>
</tr>
<tr>
<td>EHR</td>
<td>Electronic Health Records</td>
</tr>
<tr>
<td>EP</td>
<td>Eligible Professional</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>IHS</td>
<td>Indian Health Service</td>
</tr>
<tr>
<td>MU</td>
<td>Meaningful Use</td>
</tr>
<tr>
<td>NQF</td>
<td>National Quality Forum</td>
</tr>
<tr>
<td>OIT</td>
<td>Office of Information Technology</td>
</tr>
<tr>
<td>QRDA</td>
<td>Quality Reporting Document Architecture</td>
</tr>
<tr>
<td>RPMS</td>
<td>Resource and Patient Management System</td>
</tr>
<tr>
<td>XML</td>
<td>eXtensible Markup Language</td>
</tr>
</tbody>
</table>
Contact Information

If you have any questions or comments regarding this distribution, please contact the OIT Help Desk (IHS).

Phone:  (888) 830-7280 (toll free)
Web:    http://www.ihs.gov/helpdesk/
Email:  support@ihs.gov