# Table of Contents

## 1.0 Introduction
- 1.1 eCQM Overview ......................................................................................................... 1
- 1.2 More Information ......................................................................................................... 2

## 2.0 eCQM Export Tool
- 2.1 Log in and Register a New Site ....................................................................................... 4
  - 2.1.1 Register a Site ........................................................................................................ 4
- 2.2 Sites Menu ...................................................................................................................... 5
  - 2.2.1 Profile ..................................................................................................................... 5
  - 2.2.2 Connection ............................................................................................................. 9
  - 2.2.3 Delete ..................................................................................................................... 9
  - 2.2.4 QRDA III ............................................................................................................... 10
  - 2.2.5 Exports .................................................................................................................. 10
  - 2.2.6 Audit ...................................................................................................................... 14
- 2.3 Settings Menu ........................................................................................................... 15

## Appendix A: Rules of Behavior
- A.1 All RPMS Users ........................................................................................................ 17
  - A.1.1 Access .................................................................................................................. 17
  - A.1.2 Information Accessibility ....................................................................................... 18
  - A.1.3 Accountability ...................................................................................................... 18
  - A.1.4 Confidentiality ..................................................................................................... 19
  - A.1.5 Integrity ................................................................................................................ 19
  - A.1.6 System Logon ......................................................................................................... 19
  - A.1.7 Passwords ............................................................................................................. 20
  - A.1.8 Backups ................................................................................................................ 21
  - A.1.9 Reporting ............................................................................................................. 21
  - A.1.10 Session Timeouts ............................................................................................... 21
  - A.1.11 Hardware ............................................................................................................. 21
  - A.1.12 Awareness ......................................................................................................... 22
  - A.1.13 Remote Access ................................................................................................. 22
- A.2 RPMS Developers .................................................................................................... 23
- A.3 Privileged Users ...................................................................................................... 23

## Glossary
- ........................................................................................................................................... 26

## Acronym List
- ........................................................................................................................................... 27

## Contact Information
- ........................................................................................................................................... 28
Preface

Electronic Clinical Quality Measures (eCQM) are tools that help measure and track the quality of health care services that eligible professionals (EP), eligible hospitals (EH), and critical access hospitals (CAH) provide. Measuring and reporting eCQMs helps to ensure that our health care system is delivering effective, safe, efficient, patient-centered, equitable, and timely care. The 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
1.0 Introduction

This User Manual provides information on how to use the Electronic Clinical Quality Measure Export Tool (BQRE) 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 Centers for Medicare & Medicaid Services (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 (2 pediatric and 10 adult) were selected and are listed in Table 1-1 and Table 1-2.

Table 1-1: IHS – Selected EH/CAH eCQMs

<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>
### 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

1.2 More Information

The following websites provide additional eCQM information:

- eCQI Resource Center: [https://ecqi.healthit.gov/](https://ecqi.healthit.gov/)
- Agency for Healthcare Research and Quality: [https://ushik.ahrq.gov](https://ushik.ahrq.gov)
2.0 eCQM Export Tool

The eCQM Export Tool (BQRE) is a local, site-installed application designed to extract reportable data from the RPMS database and format it into a standard Quality Reporting Document Architecture (QRDA) CAT-I file. The sites will be able to extract for the 28 measures (16 Eligible Hospital and 12 Eligible Provider) which were developed using the 2017 published version. Users access the BQRE by logging in to an HTTPS web application using the IP address of the server where the BQRE is installed along with the port number (the default port is 37019). Users must have RPMS credentials to authenticate for each site where the tool is installed.

Provisioning of user accounts is performed by the BQRE Package Manager. Users can be assigned a BQRE Quality Coordinator or BQRE Quality Auditor role. These roles are driven by a security key in RPMS, APCLZMENU, and BUSAZRPT respectively. The user cannot have both keys assigned; it must be one or the other. The tool provides the ability to configure sites, set default data, define the extract format, specify the shared directory location, and set up an extraction time schedule.

The BQRE securely transmits the PII-containing QRDA CAT-I file(s) to the eCQM Engine for processing over an HTTPS (SSL) connection using an application API Token for JSON extract format. Users can also access the QRDA CAT-I file(s) from a shared, secure location on the local application server. Once computations have been performed in the eCQM Engine, QRDA CAT-III files can then be pulled in BQRE and users are able to access the file from the defined Shared Directory location.

Figure 2-1: eCQM Export Tool
2.1 Log in and Register a New Site

To log in to the BQRE application, open an internet browser (Internet Explorer® 11 [highly recommended] or higher or Google Chrome® Version 68 or higher) and enter the IP address and the port of the application server where BQRE has been installed. The default port for BQRE is 37019 (http://IPaddressOfbqreApplicationServer:37019).

Once the user can access the application, the user is taken to the Sites screen (Figure 2-2). The Sites screen will be empty upon initial access.

![Sites screen](image)

Figure 2-2: Sites screen

2.1.1 Register a Site

1. Click the Register Site button to create a new site (this task is performed by the Site Admin). The Register Site screen (Figure 2-3) displays.

![Register Site screen](image)

Figure 2-3: Register Site screen

a. Enter your Ensemble Server IP address.

b. Enter the Super Server Port number (usually 1972).
c. Enter your site’s Ensemble credentials (**Ensemble User Name** and **Ensemble Password**).

d. Enter the **RPMS Namespace**.

e. Click the **Save Changes** button. The application will verify the Ensemble credentials. If the connection cannot be established you will not be able to proceed.

f. The **Sites** screen displays the new sites added (Figure 2-4)

![Figure 2-4: New Site Added](image)

### 2.2 Sites Menu

The **Sites** screen lists the sites that have been defined for extraction. Sites can be added/modified as needed through this menu option. The BQRE Quality Coordinator can access the **Exports**, **QRDA III**, **Profile**, **Connection**, and **Delete** buttons.

The BQRE Quality Auditor will have access to the **Audit** button only.

#### 2.2.1 Profile

Use the **Profile** button to modify existing site profiles.

1. Click the **Profile** button.

2. The application will prompt for BQRE Quality Coordinator’s **RPMS Access** and **Verify** codes if not logged on already.

3. Enter the **Access** and **Verify** codes and click **Login**.

4. The **Profile** screen (Figure 2-5) displays.
5. Define/Update the Site information:

**Note:** The Profile screen will display default information from RPMS if available. Please note that any data added in this screen is not saved back to RPMS. This data is only for the purpose of eCQM export.

The following fields should have information loaded from RPMS – fill any empty fields as needed. All the following fields are required.

a. **Name:** Enter a user-friendly name for the site server.

b. **Street:** Enter the street address.

c. **City, State, Zip:** Enter the city, state and ZIP code.

d. **Phone, Fax:** Enter the phone and fax number.

e. **TIN:** Enter the site’s Tax ID number (no dash required).

f. **NPI:** Enter the site’s National Provider Identifier.

g. **CCN:** Enter the site’s CMS Certification Number.

h. **CMS Program:** Select the site CMS Program from the menu. The Quality Coordinator/Manager should know which option to select based on the Site goals and Site quality program.

6. Add Providers:
Note: Adding providers is usually performed by the Quality Program Coordinator and is optional. If providers are added, the BQRE will add the appropriate providers as service performers in the patient export data.

a. Enter the provider name (LastName, FirstName) in the Providers field to initiate a provider search in RPMS. As you type the provider name, the field auto populates with provider names on your RPMS system. Providers must have a valid NPI defined. The NPI displays next to the provider’s name. See Figure 2-6.

![Figure 2-6: Providers Search](image)

b. Select the provider from the search result to add to your site server configuration.

![Figure 2-7: Providers List](image)

c. Click Remove to delete the provider from the list.

7. Define the Legal Authenticator. 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. These are required fields.

a. Enter First Name.

b. Enter Last Name.
8. Define the **Default Settings**. Use the Default Settings to define the ethnicity, race, server time zone, extract format, and shared directory location:

   ![Default Settings](image)

   **Figure 2-9: Default Settings**

   a. Select the default patient ethnicity from the **Ethnicity** menu.
   b. Select the default patient race from the **Race** menu.
   c. Select the **Server Time Zone** from the menu.
   d. Select the default **Extract Format** from the menu.
   e. Enter the **Qrda Storage Path**.

   **Note:** The defaults for the Ethnicity and Race are used for extraction when no data is defined for these fields in RPMS. Your Meaningful Use coordinator can later review the profile page to confirm all values are correct and modify as required. The **Qrda Storage Path** is the location of the Shared Directory path where QRDA CAT-I and QRDA CAT-III file is stored. This is a folder on the local drive of the application server.

9. Define the Upload Settings. The Client Site ID and Upload API key needs to be defined if sites want to transmit the QRDA CAT-I file(s) to the ECQM Engine application. The Extract Format must be set to **ECQM Optimized JSON**. The BQRE will automatically transmit to the ECQM Engine over an HTTPS (SSL) connection using an application API Token to ensure secure communication.
a. **Client Site ID**: copy and paste the Site ID from the ECQM Engine application’s Site Profile definition.
b. **Upload API Key**: copy and paste the generated API Key from the ECQM Engine application’s Site Profile definition.

10. Click **Save Changes**.

11. Click **Cancel** to discard any changes.

### 2.2.2 Connection

Use the **Connection** button to update or modify the Ensemble connection information such as IP, port, password, and namespace.

1. Click the **Connection** button.

2. Update fields as appropriate on the **Update Site** screen.

3. Enter the **Ensemble Password**.

4. Click **Save Changes**.

5. Click **Cancel** to disregard changes.

![Update Site screen](image)

**Figure 2-10: Update Site screen**

### 2.2.3 Delete

Use the **Delete** button to delete a site that is no longer needed.

1. Click the **Delete** button next to the site that needs to be deleted.
2. Enter the Ensemble **Username** and **Password**.

3. Click **Delete**.

### 2.2.4 QRDA III

This option is used to pull QRDA CAT-III files from the ECQM Engine for JSON extract format auto-transmission (see Section 3.3.1 of the *BQRE Installation Guide and Release Notes*) and saves the file in the shared directory defined in the Qrda Storage Path in the Site Profile.

1. Click the **QRDA III** button to display the **QRDA III** screen.

2. The application will prompt for the BQRE Quality Coordinator’s **RPMS Access** and **Verify** codes if not logged on already.

3. Enter the **RPMS Access** and **Verify Code** and click **Login**.

4. The **QRDA III** screen displays (Figure 2-11).

![QRDA III screen](image)

Figure 2-11: **QRDA III** screen

5. Click the **Pull QRDA III** button.

6. The **QRDA III** screen updates the **Team**, **Last Report Run On** and **Last Updated On** and generates a QRDA CAT-III zip file in the shared directory.

### 2.2.5 Exports

Use the **Exports** button to start the process of exporting QRDA CAT-I file or to check on the status of existing export.

1. Click the **Exports** button to view the status of an existing export.

2. The application will prompt for the BQRE Quality Coordinator’s **RPMS Access** and **Verify** codes if not logged on already.

3. The **Exports** screen displays (Figure 2-12).
Figure 2-12: Exports screen

4. Click the **Detail** button to view the export detail information. The **Detail** screen includes the Batch Job Detail information, the Export Schedule information, and the number of patients processed.

   Select **Transmitted** from the **Status** list to view the patients that were processed (Figure 2-13).
5. Click the **Back to Exports** button to go back to the **Exports** screen.

6. Click the **Schedule Export** button on the **Exports** screen to start a new export. The **Schedule an export** screen displays (Figure 2-14).

7. Enter the **Start Date** and **End Date**.
Note: The Start Date defaults to the beginning of the current calendar year. The End Date defaults to the end of the current calendar year. The End Date must be a date later than the Start Date.

8. Click the Schedule button.

9. Click the Refresh button to refresh the Export screen. Once the export is complete, the job displays under Completed.

10. To view the failed export details, click the Detail button on an export under the Failed section of the Export screen (Figure 2-15).

![Figure 2-15: Failed Export](image)

11. Select Extraction Failed from the Status option.

12. Click the Failure Reason link to see the detailed error encountered during the export (Figure 2-16). Users can copy the information on the screen and send it to their Quality Coordinator for review.

![Figure 2-16: Failed Reason Detail](image)
13. Click the **Back to Batch** button to return to the **Export** screen.

**2.2.6 Audit**

Use the **Audit** button to view the audit trail of all the activities performed in BQRE. This option is only accessible if the user has the BQRE Quality Auditor security key.

![Audit screen](image)

*Figure 2-17: Audit screen*

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

1. Enter the **User Name** (Last Name, First Name).

2. Select a **Category** from the list. Options include the following:
   - **Authentication**
   - **PatientData**
   - **Configuration**

3. Select **Type**. Options include the following:
   - **Login**
   - **Logout**
   - **Delete**
   - **Create**
   - **Update**
   - **Activate**
   - **Deactivate**
• Query
• Upload
• Download
• Schedule

4. Enter Event. Examples of events include the following:

• Login
• Logout
• Update Site
• Profile Update
• Schedule
• Pull

5. Enter the From Date and To Date (format MM/DD/YYYY 00:00:00 AM/PM).

6. Select Sort By:

• Time Descending
• Time Ascending
• Category
• Type
• Event

7. Click the Filter button.

### 2.3 Settings Menu

Use the Settings menu option to schedule an export process background job. The system will start processing patient data daily at the defined start time.

1. Click the Settings menu option.
2. Enter/Select **Start Time** and click the **Check** button. The default value is 12:01 AM. Enter Start Time in 00:00:00 format.

3. Define duration in hours (0–23). The default duration is 23 hours.

4. Click the **Update** button to save.
Appendix A: Rules of Behavior

The Resource and Patient Management (RPMS) system 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/](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 RoBs 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.
- Always protect all RPMS terminals from public viewing.
- 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 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 \textit{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 nonrecovery 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**
Tools that help measure and track the quality of health care services provided by eligible professionals, eligible hospitals, and critical access hospitals.

**Promoting Interoperability (Formerly called Meaningful use)**
The use of 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>BMI</td>
<td>Body Mass Index</td>
</tr>
<tr>
<td>CEHRT</td>
<td>Certified Electronic Health Record Technology</td>
</tr>
<tr>
<td>CAH</td>
<td>Critical Access Hospitals</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>EP</td>
<td>Eligible Professional</td>
</tr>
<tr>
<td>Health IT</td>
<td>Health Information Technology</td>
</tr>
<tr>
<td>HMPC</td>
<td>Home Management Plan of Care</td>
</tr>
<tr>
<td>IHS</td>
<td>Indian Health Service</td>
</tr>
<tr>
<td>PI</td>
<td>Promoting Interoperability</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>
</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/](http://www.ihs.gov/helpdesk/)
**Email:** support@ihs.gov