RESOURCE AND PATIENT MANAGEMENT SYSTEM

Electronic Clinical Quality Measures Export Tool

(BQRE)

User Manual

Version 7.0
January 2025

Office of Information Technology
Division of Information Technology

Table of Contents

Preface

Electronic Clinical Quality Measures (eCQMs) are tools that help measure and track the quality of healthcare services that eligible clinicians (EC), eligible hospitals (EH), and critical access hospitals (CAH) provide. Measuring and reporting eCQMs helps to ensure that our healthcare 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 Office of the National Coordinator for Health Information Technology (ONC) Certification Criteria for Health IT necessary for participating in various Centers for Medicare and 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 13 EH/CAH eCQMs, 2 EH/CAH Hybrid, and 24 EC eCQMs were selected, and are listed, in Table 1-1, Table 1-2, and Table 1-3.

Table 1-1: IHS Selected EH/CAH eCQMs

CMS ID	Measure Type	Measure
CMS009v11 (retired)	Process	Exclusive Breast Milk Feeding
CMS071v13	Process	Anticoagulation Therapy for Atrial Fibrillation/Flutter
CMS072v12	Process	Antithrombotic Therapy By End of Hospital Day 2
CMS104v12	Process	Discharged on Antithrombotic Therapy
CMS108v12	Process	Venous Thromboembolism Prophylaxis
CMS190v12	Process	Intensive Care Unit Venous Thromboembolism Prophylaxis
CMS334v5	Outcome	Cesarean Birth
CMS506v6	Process	Safe Use of Opioids–Concurrent Prescribing
CMS816v3	Outcome	Hospital Harm–Severe Hypoglycemia
CMS819v2	Outcome	Hospital Harm-Opioid-Related Adverse Events
CMS871v3	Outcome	Hospital Harm–Severe Hyperglycemia
CMS986v2	Intermediate Clinical Outcome	Global Malnutrition Composite Score
CMS1028v2	Outcome	Severe Obstetric Complications

Table 1-2: IHS Selected EH/CAH Hybrid

CMS ID	Measure Type	Measure
CMS844v4	Hybrid-Cohort Administrative	Core Clinical Data Elements for the Hybrid Hospital-Wide (All-Condition, All-Procedure) Risk-Standardized Mortality Measure (HWM)
CMS529v4	Hybrid-Cohort Administrative	Core Clinical Data Elements for the Hybrid Hospital-Wide Readmission (HWR) Measure with Claims and Electronic Health Record Data

Table 1-3: IHS Selected EC eCQMs

CMS ID	Measure Type	Measure
CMS002v13	Process	Preventative Care and Screening: Screening for Depression and Follow-Up Plan
CSM022v12	Process	Preventative Care and Screening: Screening for High Blood Pressure and Follow-up Documented
CMS050v12	Process	Closing Referral Loop: Receipt of Specialist Report
CMS069v12	Process	Preventative Care and Screening: Body Mass Index (BMI) Screening and Follow-Up Plan
CMS117v12	Process	Childhood Immunization Status
CMS122v12	Intermediate Clinical Outcome	Diabetes: Hemoglobin A1c (HbA1c) Poor Control (> 9%)
CMS124v12	Process	Cervical Cancer Screening
CMS125v12	Process	Breast Cancer Screening
CMS130v12	Process	Colorectal Cancer Screening
CMS131v12	Process	Diabetes: Eye Exam
CMS137v12	Process	Initiation and Engagement of Alcohol and Other Drug Dependence Treatment
CMS138v12	Process	Preventive Care and Screening: Tobacco Use: Screening and Cessation Intervention
CMS139v12	Process	Falls: Screening for Future Fall Risk
CMS144v12	Process	Heart Failure: Beta-Blocker Therapy for Left Ventricular Systolic Dysfunction
CMS145 v12	Process	Coronary Artery Disease (CAD): Beta-Blocker Therapy-Prior Myocardial Infarction (MI) or Left Ventricular Systolic Dysfunction (LVEF) less than or equal to 40%
CMS154v12	Process	Appropriate Treatment for Upper Respiratory Infection (URI)
CMS155v12	Process	Weight Assessment and Counseling for Nutrition and Physical Activity for Children and Adolescents
CMS156v12	Process	Use of High-Risk Medications in Older Adults

CMS ID	Measure Type	Measure
CMS159v12	Outcome	Depression Remission at Twelve Months
CMS160v7 (retired)	Process	Depression Utilization of the PHQ-9 Tool
CMS165v12	Intermediate Clinical Outcome	Controlling High Blood Pressure
CMS177v12	Process	Child and Adolescent Major Depressive Disorder: Suicide Risk Assessment
CMS347v7	Process	Statin Therapy for the Prevention and Treatment of Cardiovascular Disease
CMS349v6	Process	HIV Screening

Note: The measures not updated for 2024 and are not eligible to submit to CMS.

CMS009v11 uses logic from 2023.

CMS160v7 uses logic from 2019.

1.2 More Information

The following websites provide additional eCQM 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 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 Category I (QRDA I). The sites will be able to extract for the 41 measures (13 eligible hospitals and 28 eligible clinicians) that were developed for the 2023 reporting year. Users access the BQRE by logging in to an HTTP 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 security keys 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.

Users can access the QRDA I file(s) from a shared, secure location on the local application server and then import it to the eCQM Engine (Figure 2-1) for computations and to generate the QRDA Category III (QRDA III) file(s).

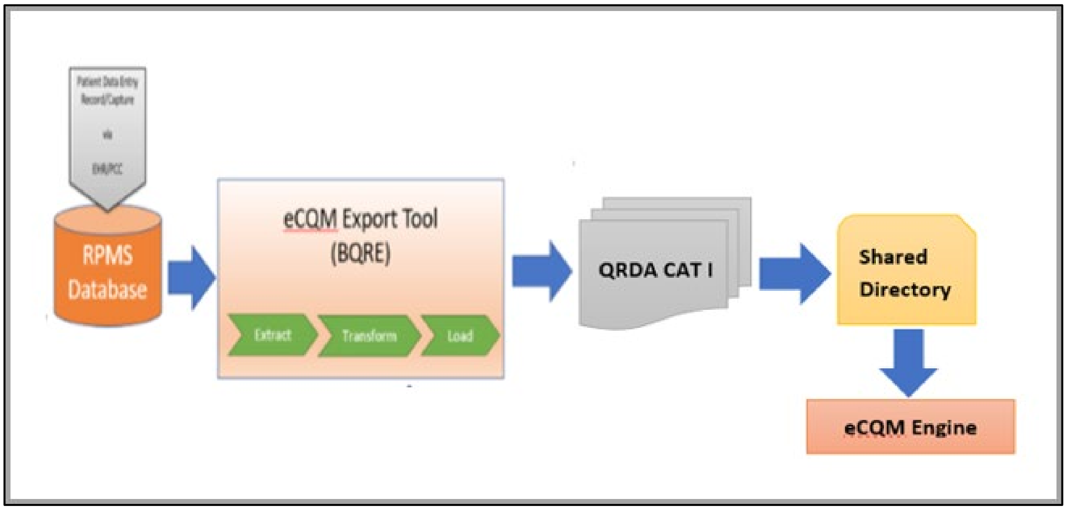
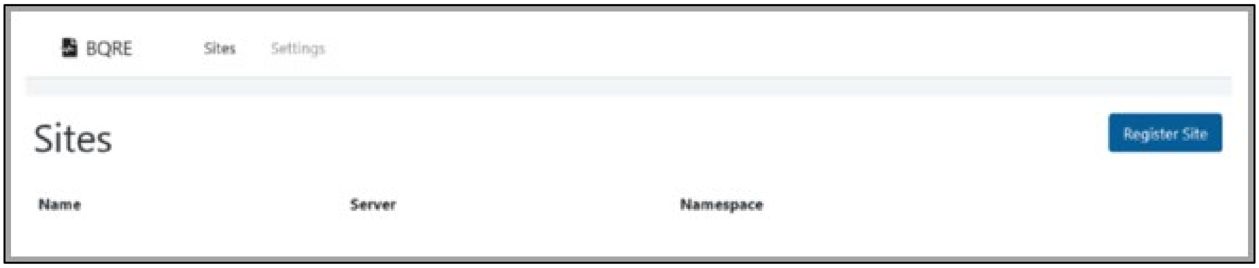


Figure 2-1: eCQM Export Tool

2.1 Log in and Register a New Site

To log in to the BQRE application, open an internet browser (Google Chrome version 80+ [highly recommended], Firefox, and Microsoft Edge are all supported) and enter the IP address and the port of the application server where BQRE has been installed (for example, https://IPaddressOFbqreApplicationServer:Port).

Once the user can access the application, the **Sites** window (Figure 2-2) displays for the user. It will be empty upon initial access.



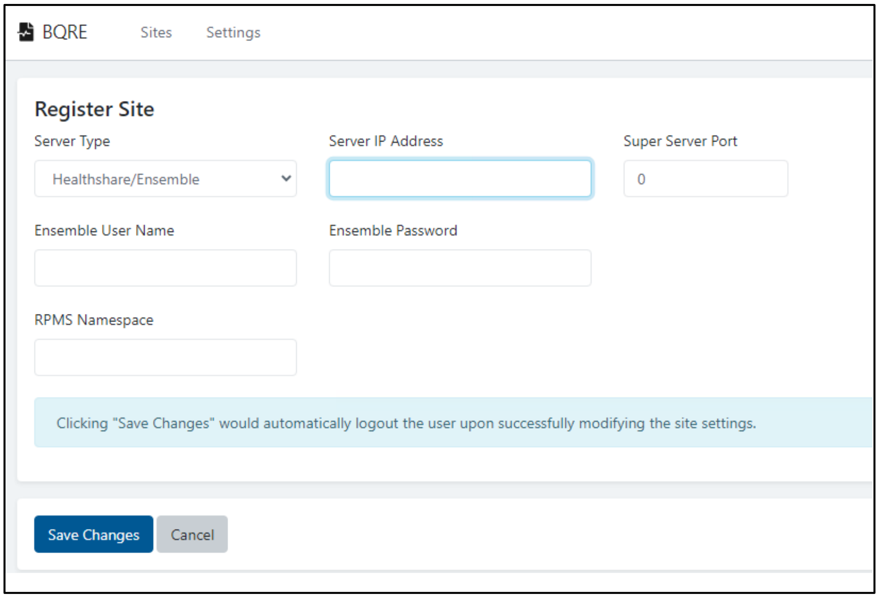
Sites

Name Server Namespace

Figure 2-2: Sites window

2.1.1 Register a Site

1. Click the **Register Site** button to create a new site (the Site Admin performs this task). The **Register Site** window (Figure 2-3) displays.



Register Site

Server Type: Healthshare/Ensemble

Server IP Address:

Super Server Port: 0

Ensemble User Name:

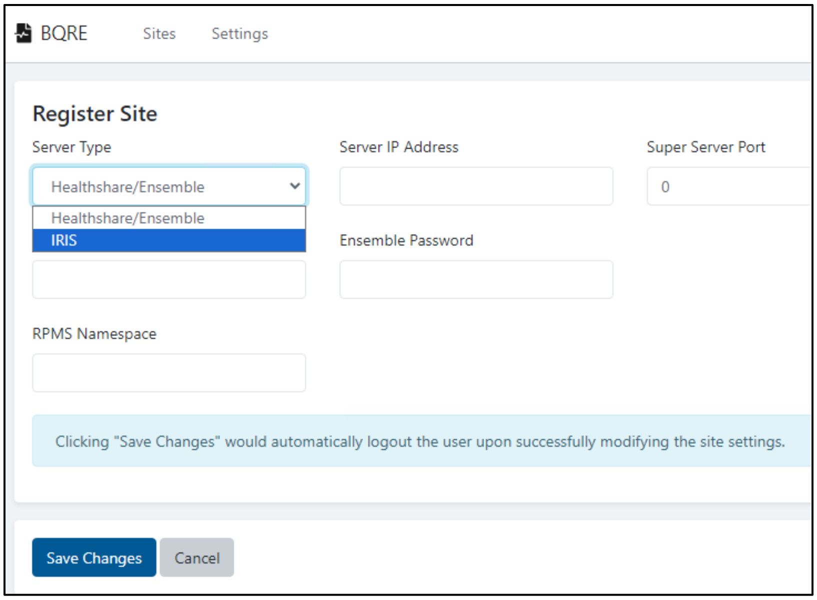
Ensemble Password:

RPMS Namespace:

Clicking "Save Changes" would automatically logout the user upon successfully modifying the site settings.

Figure 2-3: Register Site window

2. Select the “Server Type” depending on your RPMS System Configuration (HealthShare/Ensemble or IRIS).



Register Site

Server Type: Healthshare/Ensemble

- Healthshare/Ensemble
- IRIS

Server IP Address

Super Server Port: 0

Ensemble Password

RPMS Namespace

Clicking "Save Changes" would automatically logout the user upon successfully modifying the site settings.

Figure 2-4: Server Type Window

3. Enter your **Ensemble Server** IP address.

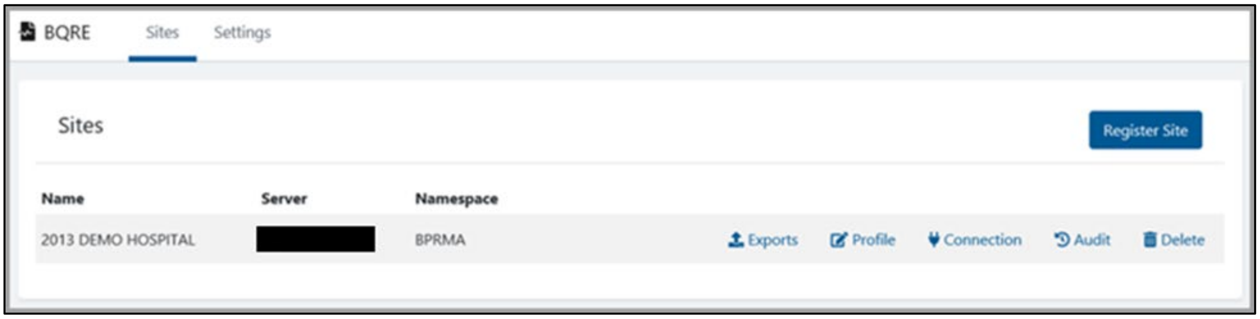
4. Enter the **Super Server Port** number.

5. Enter your site's **Ensemble credentials** (Ensemble User Name and Ensemble Password).

6. Enter the **RPMS Namespace**.

7. 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.

The **Sites** window (Figure 2-5) displays the new sites added.



Sites

Name	Server	Namespace					
2013 DEMO HOSPITAL	[redacted]	BPRMA	Exports	Profile	Connection	Audit	Delete

Figure 2-5: New Site Added window

2.2 Sites Menu

The **Sites** window 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**, **Profile**, **Connection**, and **Delete** buttons (Figure 2-5).

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

2.2.1 Profile

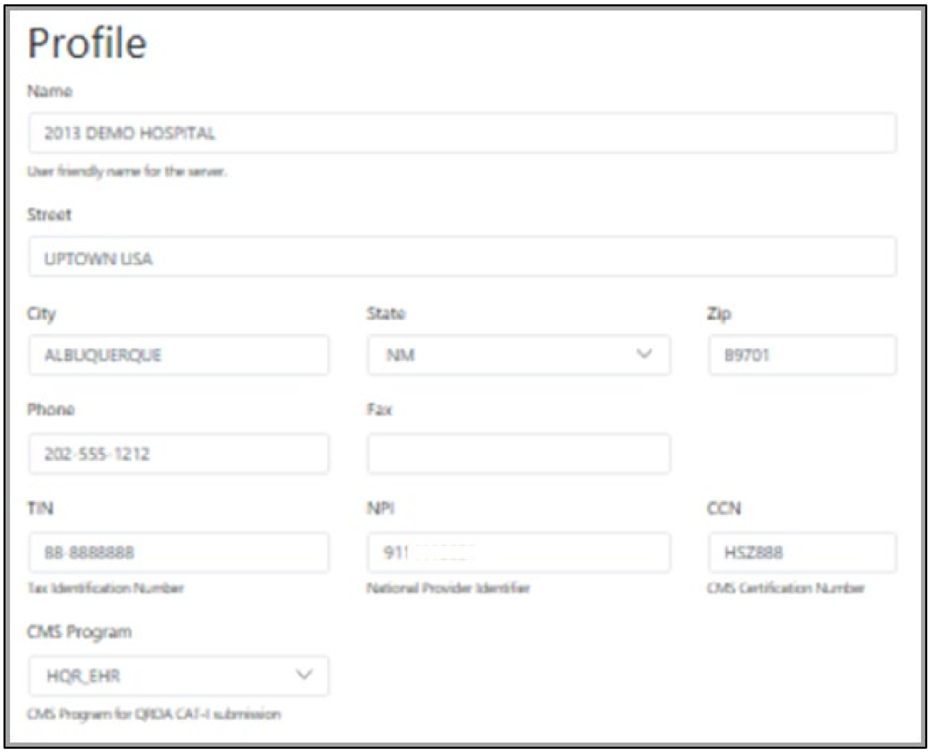
Use the **Profile** button to modify existing site profiles.

1. Click the **Profile** button.

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

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

   The **Profile** window (Figure 2-6) displays.



Profile

Name: 2013 DEMO HOSPITAL

User friendly name for the server.

Street: UPTOWN USA

City: ALBUQUERQUE

State: NM

Zip: 89701

Phone: 202-555-1212

Fax:

TIN: 88-8888888

Tax Identification Number

NPI: 91[redacted]

National Provider Identifier

CCN: HSZ888

CMS Certification Number

CMS Program: HQR_EHR

CMS Program for QRDA CAT-I submission

Figure 2-6: Profile window

3. Define/update the site information:

> **Note:** The **Profile** window will display default information from RPMS if available. Note that any data added in this window 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. Complete any empty fields as needed. All the following fields are required:

- **Name:** Enter a user-friendly name for the site server.
- **Street:** Enter the street address.
- **City, State, Zip:** Enter the city, state, and ZIP code.
- **Phone, Fax:** Enter the phone and fax number.
- **TIN:** Enter the site's tax ID number (no dash required).
- **NPI:** Enter the site's National Provider Identifier.
- **CCN:** Enter the site's CMS certification number.
- **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. Options include the following:
  - **HQR_PI**
  - **HQR_IQR**
  - **HQR_PI_IQR**
  - **HQR_IQR_VOL**

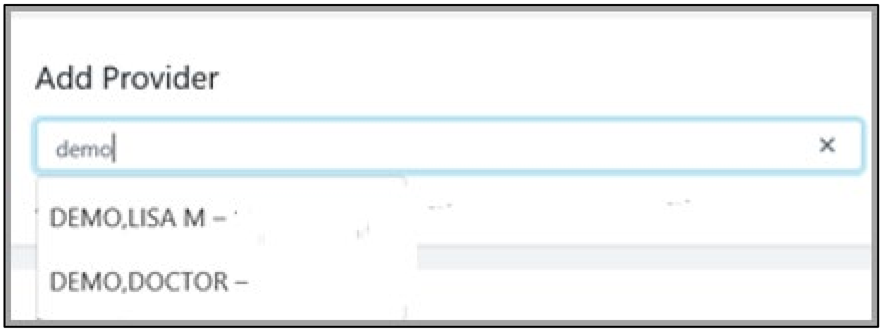
4. Add/view providers.

> **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. Click **View All** to add/view providers.

   b. To add a provider, enter the provider name (LastName, FirstName) (Figure 2-7) or the NPI (Figure 2-8) in the search field to initiate a provider search in RPMS.

   > **Note:** If entering a provider name or NPI number, as you type the name or the NPI of the provider, the search auto-populates with possible matches from your RPMS system.



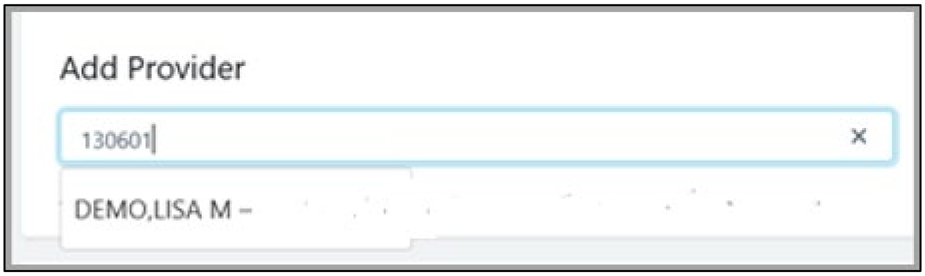
Add Provider

demo

DEMO,LISA M –

DEMO,DOCTOR –

Figure 2-7: Provider Search using Provider Name dialog



Add Provider

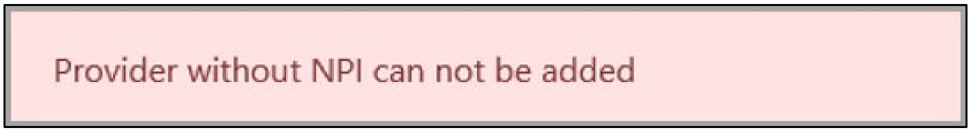
130601

DEMO,LISA M –

Figure 2-8: Provider Search Using NPI dialog

Providers must have a valid NPI defined. The NPI displays next to the provider’s name.

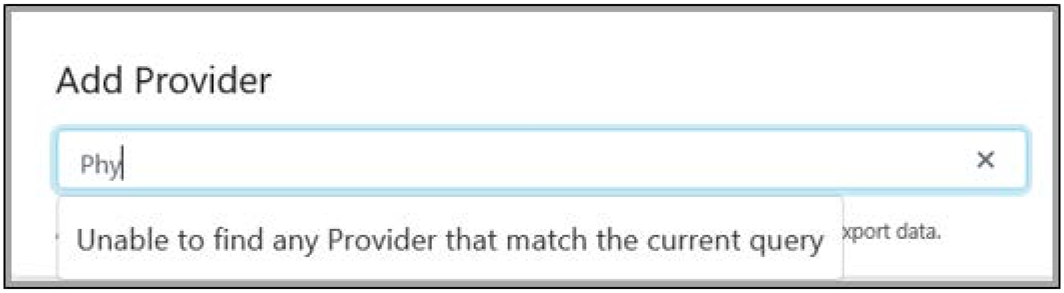
If a provider with no NPI is selected an error message displays (see Figure 2-9).



Provider without NPI can not be added

Figure 2-9: Provider with No or Invalid NPI message

If no match can be found, the following message displays (Figure 2-10).



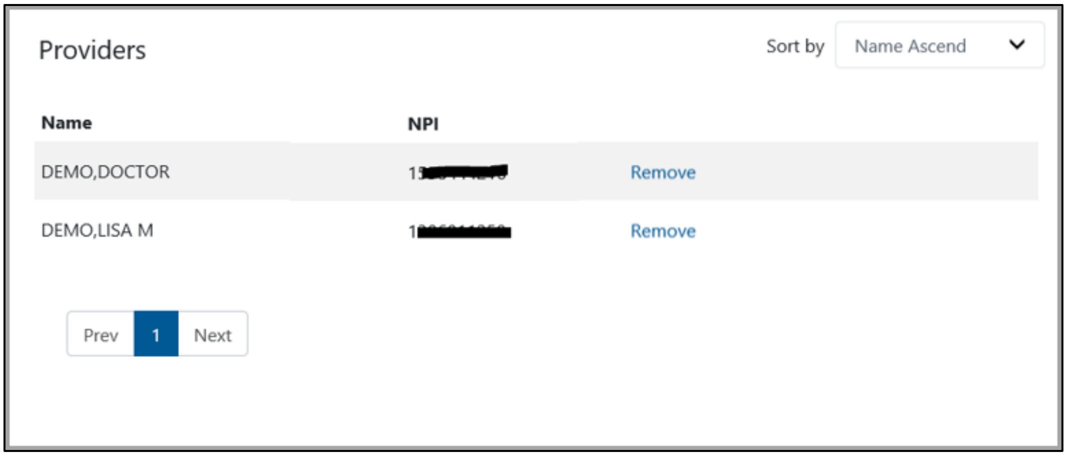
Add Provider

Phy

Unable to find any Provider that match the current query

Figure 2-10: No Match Found message

c. Select the provider from the search result to add to your site server configuration (Figure 2-11).



Providers

Sort by Name Ascend

Name	NPI	
DEMO,DOCTOR	[redacted]	Remove
DEMO,LISA M	[redacted]	Remove

Figure 2-11: Providers list

d. Click **Sort By** to sort the list by **Name Ascend**, **Name Descend**, and by **NPI**.

e. Click **Remove** to delete the provider from the list.

There is no need to save as the list is saved automatically.

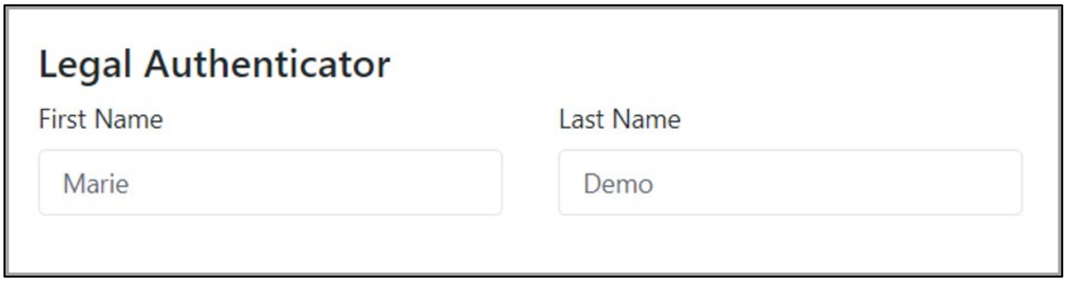
f. Click **Back to Profile** to go back to the main **Profile** page.

5. 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 (Figure 2-12).

a. Enter the **First Name**.

b. Enter the **Last Name**.



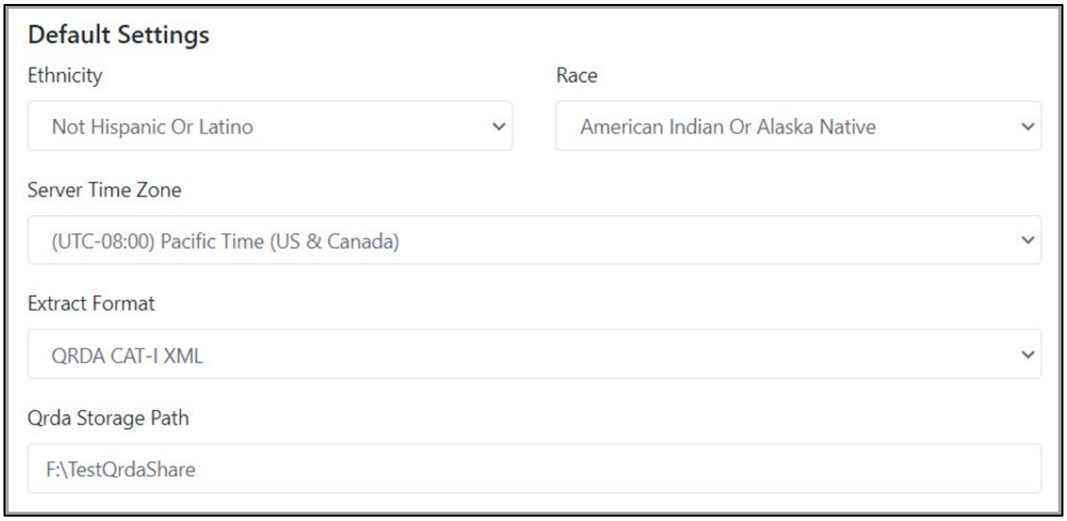
Legal Authenticator

First Name: Marie

Last Name: Demo

Figure 2-12: Legal Authenticator dialog

6. Define the **Default Settings**. Use these settings to define the ethnicity, race, server time zone, extract format, and shared directory location (Figure 2-13).



Default Settings

Ethnicity: Not Hispanic Or Latino

Race: American Indian Or Alaska Native

Server Time Zone: (UTC-08:00) Pacific Time (US & Canada)

Extract Format: QRDA CAT-I XML

Qrda Storage Path: F:\TestQrdaShare

Figure 2-13: Default Settings dialog

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**.

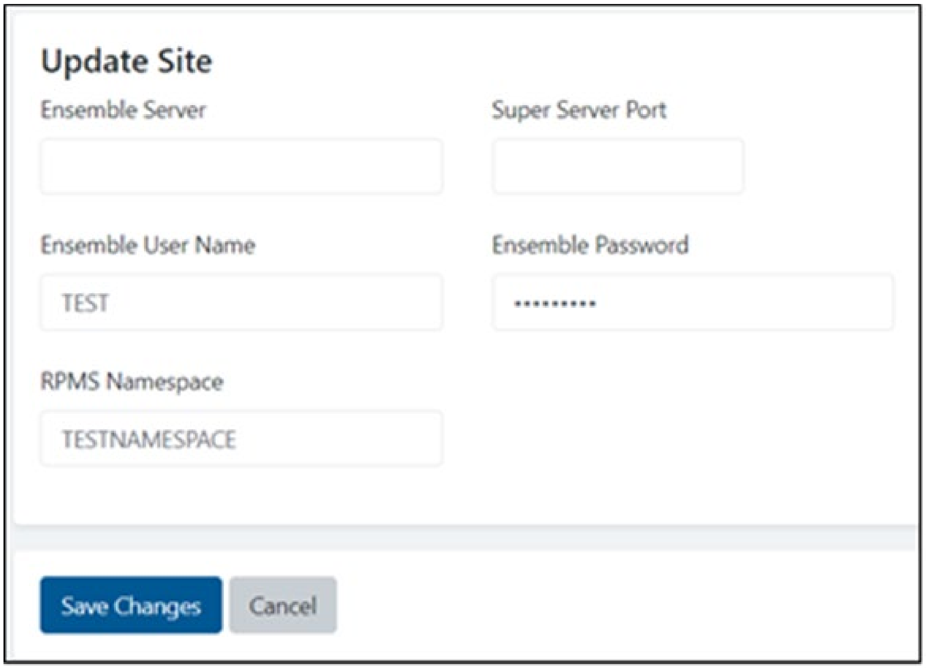
> **Note:** The defaults for the Ethnicity and Race are used for extraction when no data is defined for these fields in RPMS. Your Meaningful Use coordinator can later review the profile page to confirm all values are correct and modify as required. The Qrda Storage Path is the location of the Shared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

7. Click **Save Changes** or 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** window (Figure 2-14).
3. Enter the **Ensemble Password**.
4. Click **Save Changes** or click **Cancel** to disregard changes.



Update Site

Ensemble Server

Super Server Port

Ensemble User Name

TEST

Ensemble Password

•••••••••

RPMS Namespace

TESTNAMESPACE

Figure 2-14: Update Site window

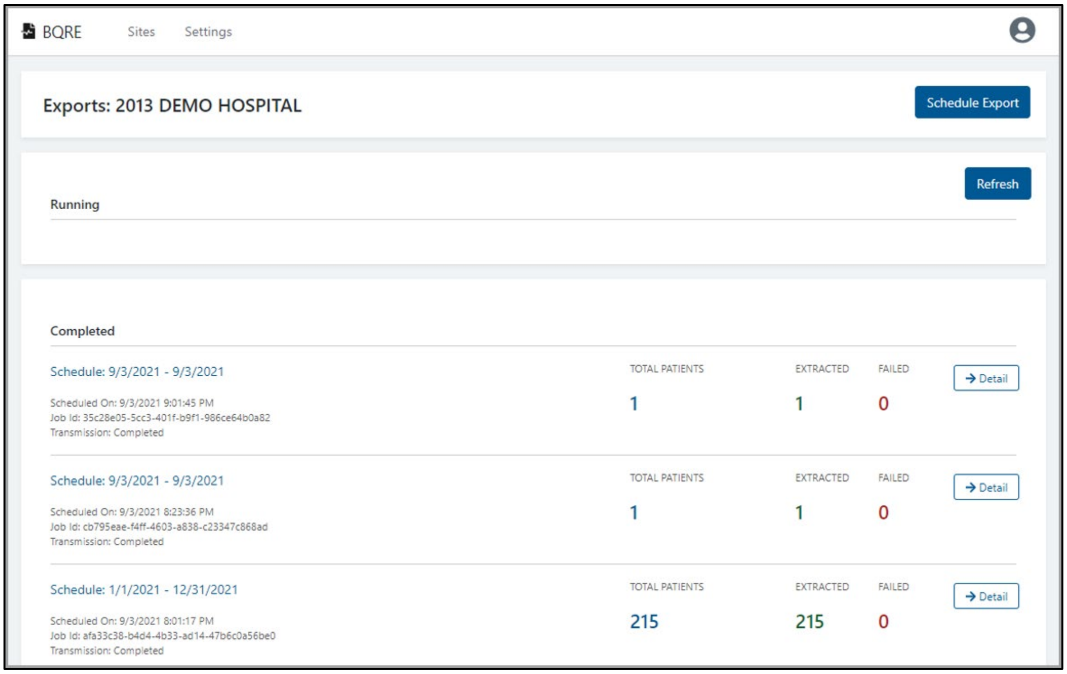
2.2.3 Exports

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

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

   The application prompts for the BQRE Quality Coordinator's **RPMS Access** and **Verify** codes if not logged on already.

2. The **Exports** window displays (Figure 2-15).



Exports: 2013 DEMO HOSPITAL

Running

Completed

Schedule: 9/3/2021 - 9/3/2021
Scheduled On: 9/3/2021 9:01:45 PM
Job Id: 35c28e05-5cc3-401f-b9f1-986ce64b0a82
Transmission: Completed

TOTAL PATIENTS	EXTRACTED	FAILED
1	1	0

Schedule: 9/3/2021 - 9/3/2021
Scheduled On: 9/3/2021 8:23:36 PM
Job Id: cb795eae-f4ff-4603-a838-c23347c868ad
Transmission: Completed

TOTAL PATIENTS	EXTRACTED	FAILED
1	1	0

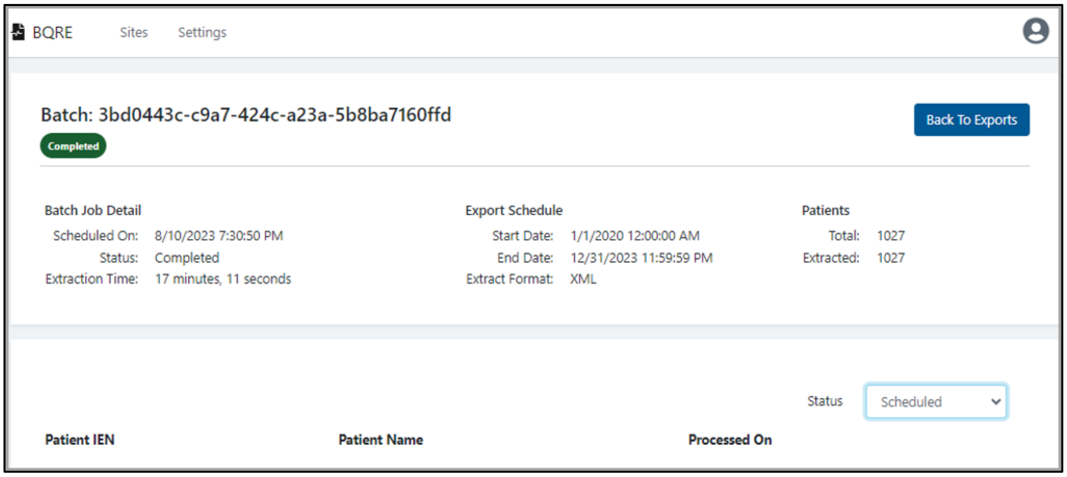
Schedule: 1/1/2021 - 12/31/2021
Scheduled On: 9/3/2021 8:01:17 PM
Job Id: afa33c38-b4d4-4b33-ad14-47b6c0a56be0
Transmission: Completed

TOTAL PATIENTS	EXTRACTED	FAILED
215	215	0

Figure 2-15: Exports window

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

4. Select the **Status: Scheduled**, **Extracted**, or **Extraction Failed** from the dropdown. Figure 2-16 displays.



Batch: 3bd0443c-c9a7-424c-a23a-5b8ba7160ffd
Completed

Batch Job Detail
Scheduled On: 8/10/2023 7:30:50 PM
Status: Completed
Extraction Time: 17 minutes, 11 seconds

Export Schedule
Start Date: 1/1/2020 12:00:00 AM
End Date: 12/31/2023 11:59:59 PM
Extract Format: XML

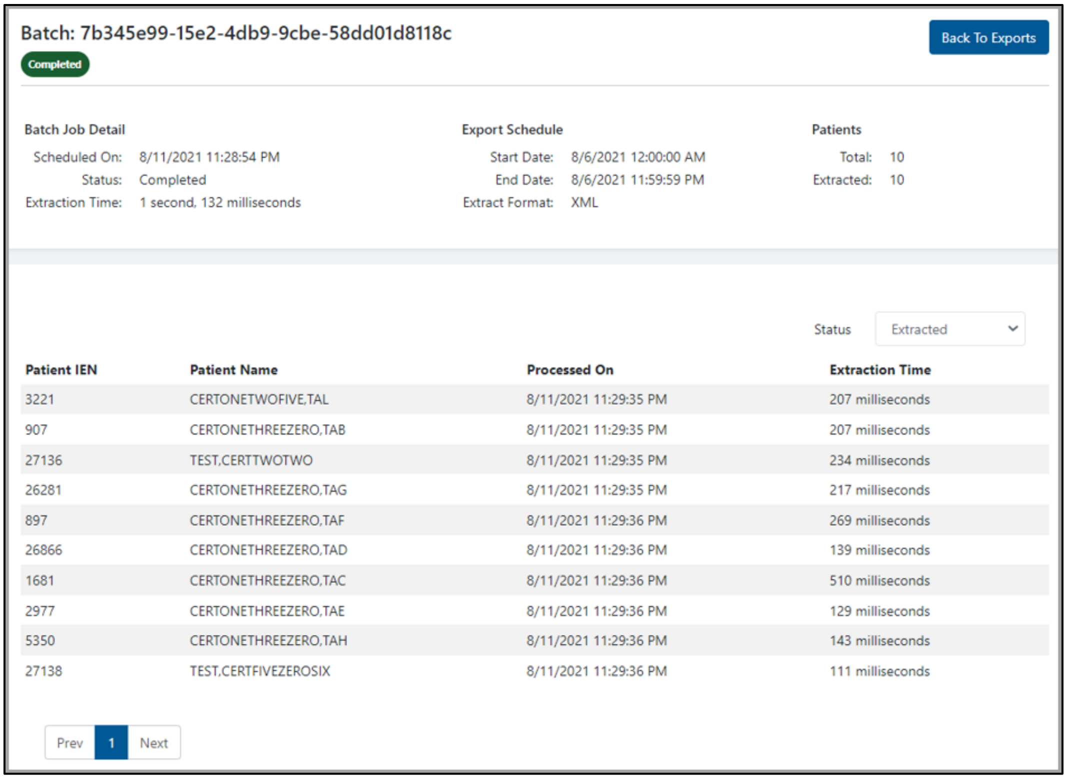
Patients
Total: 1027
Extracted: 1027

Status: Scheduled

Patient IEN	Patient Name	Processed On

Figure 2-16: Export Status Selection window

5. Select **Extracted** from the **Status** list to view the patients that were processed (Figure 2-17).



Batch: 7b345e99-15e2-4db9-9cbe-58dd01d8118c

Batch Job Detail

Scheduled On: 8/11/2021 11:28:54 PM
Status: Completed
Extraction Time: 1 second, 132 milliseconds

Export Schedule

Start Date: 8/6/2021 12:00:00 AM
End Date: 8/6/2021 11:59:59 PM
Extract Format: XML

Patients

Total: 10
Extracted: 10

Status: Extracted

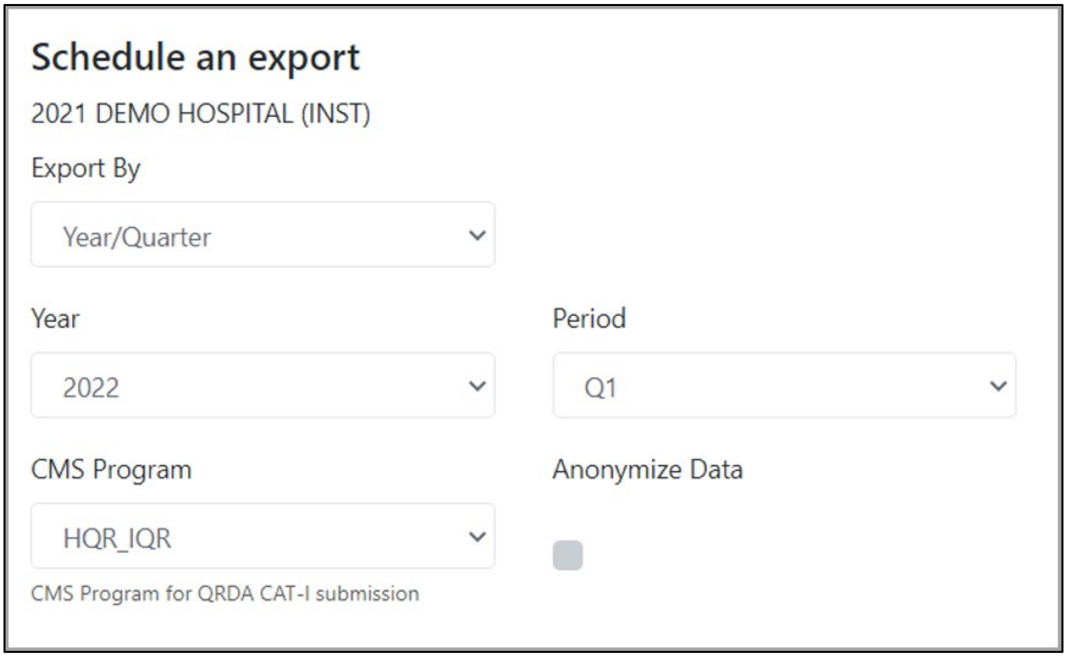
Patient IEN	Patient Name	Processed On	Extraction Time
3221	CERTONETWOFIVE,TAL	8/11/2021 11:29:35 PM	207 milliseconds
907	CERTONETHREEZERO,TAB	8/11/2021 11:29:35 PM	207 milliseconds
27136	TEST,CERTTWOTWO	8/11/2021 11:29:35 PM	234 milliseconds
26281	CERTONETHREEZERO,TAG	8/11/2021 11:29:35 PM	217 milliseconds
897	CERTONETHREEZERO,TAF	8/11/2021 11:29:36 PM	269 milliseconds
26866	CERTONETHREEZERO,TAD	8/11/2021 11:29:36 PM	139 milliseconds
1681	CERTONETHREEZERO,TAC	8/11/2021 11:29:36 PM	510 milliseconds
2977	CERTONETHREEZERO,TAE	8/11/2021 11:29:36 PM	129 milliseconds
5350	CERTONETHREEZERO,TAH	8/11/2021 11:29:36 PM	143 milliseconds
27138	TEST,CERTFIVEZEROSIX	8/11/2021 11:29:36 PM	111 milliseconds

Figure 2-17: Export Detail window

6. Click the **Back to Exports** button to go back to the **Exports** window.

7. Click the **Schedule Export** button on the **Exports** window to start a new export. The **Schedule an Export** window displays (Figure 2-18). If there are no providers associated with the site before scheduling an export, a message displays to the user.

   The user will be able to add by clicking the **Add Providers** link. Refer to Section 2.1.1, step 5 on how to add providers.



Schedule an export

2021 DEMO HOSPITAL (INST)

Export By: Year/Quarter

Year: 2022

Period: Q1

CMS Program: HQR_IQR

CMS Program for QRDA CAT-I submission

Anonymize Data: □

Figure 2-18: Schedule an Export window

8. Select the **Export By Year/Quarter or Custom Date Range**. Export By defaults to **Year/Quarter**, the current calendar year, and **Period Q1**. The user can change as needed for the export.

    a. Hybrid measures must be exported in two reporting years since the reporting period is **July 1, XXXX** thru **June 30, XXXX**. The previous reporting year must be selected then period **Q3**, then **Q4**; then the current year must be selected to export **Q1** then **Q2**.

> **Note:** If you select **Custom Date Range**, the 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**.

9. Change the **CMS Program** if needed.

> **Note:** The default value is based on what is defined in the Site Profile.

10. Select the **Anonymize Data** check box to sanitize patient data in the export file.

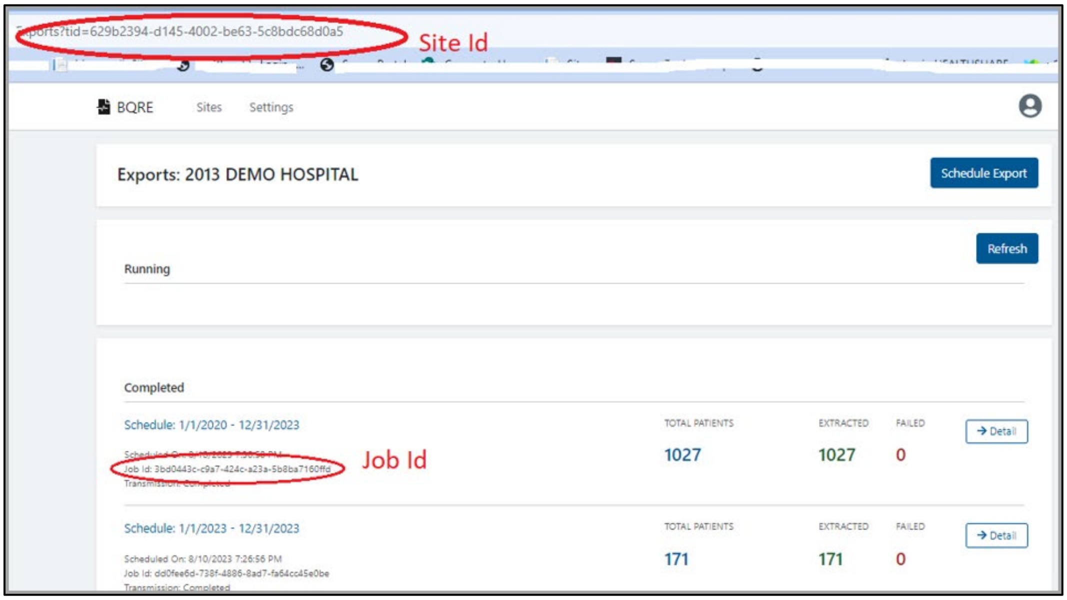
> **Note:** Anonymize data includes patients' first name, last name, street address, city, and state. Postal Code is partially anonymized by replacing the last three (3) digits of the zip code with 0.

11. Click the **Schedule** button.

12. Click the **Refresh** button to refresh the **Export** window. Once the export is complete, the job displays under **Completed**.

13. Once the job is **completed**, open the **Windows File Explorer** and navigate to the **QRDA Storage Path** directory.

    The path can be found in the **Site Profile** tab in BQRE. Open the folder that matches the **Site Id** (Figure 2-19). Within this folder, look for the subfolder that matches the Job Id. This subfolder will contain all the extracted QRDA files. For every 1000 files, the system will create a new folder with the Job Id followed by a number ending in 0, 1, or 2. Each of these folders will have a corresponding zip file that needs to be uploaded to ECQM or submitted to CMS for data submission.



Exports: 2013 DEMO HOSPITAL

Running

Completed

Schedule: 1/1/2020 - 12/31/2023
Scheduled On: 8/10/2023 7:30:50 PM
Job Id: 3bd0443c-c9a7-424c-a23a-5b8ba7160ffd
Transmission: Completed

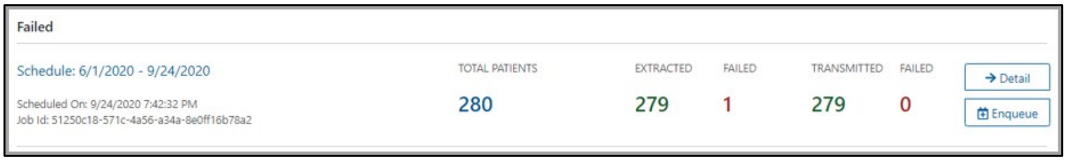
TOTAL PATIENTS	EXTRACTED	FAILED
1027	1027	0

Schedule: 1/1/2023 - 12/31/2023
Scheduled On: 8/10/2023 7:26:56 PM
Job Id: dd0fee6d-738f-4886-8ad7-fa64cc45e0be
Transmission: Completed

TOTAL PATIENTS	EXTRACTED	FAILED
171	171	0

Figure 2-19: Completed Export window

14. To view the failed export details, click the **Detail** button on an export under the **Failed** section of the **Export** window (Figure 2-20).



Failed

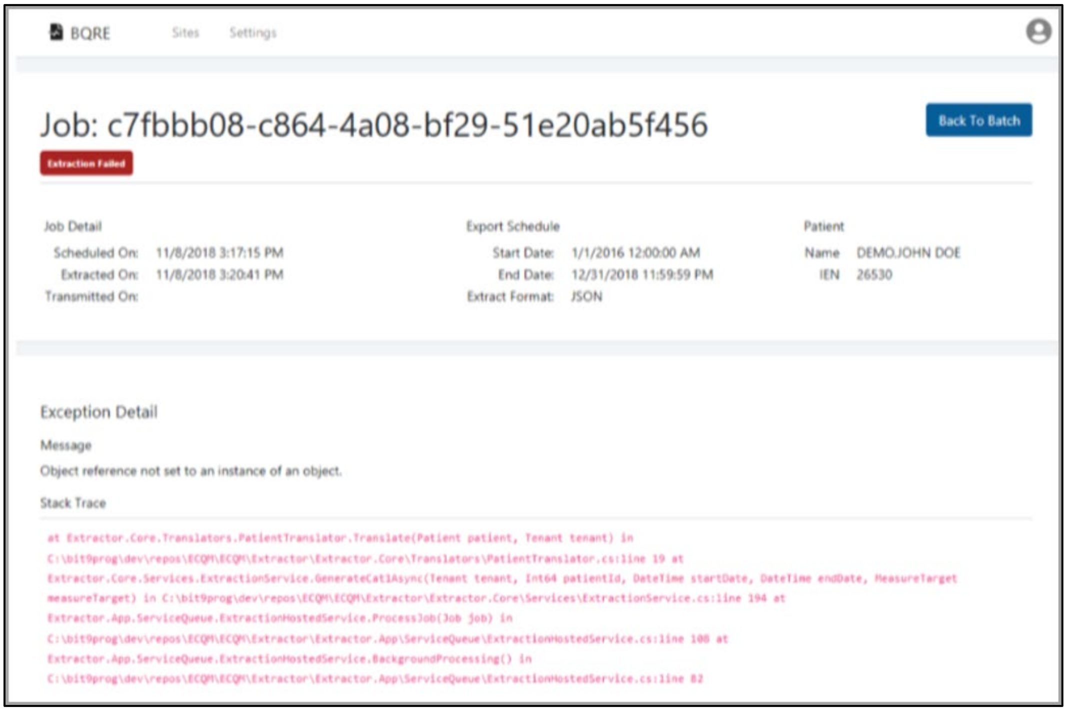
Schedule: 6/1/2020 - 9/24/2020
Scheduled On: 9/24/2020 7:42:32 PM
Job Id: 51250c18-571c-4a56-a34a-8e0ff16b78a2

TOTAL PATIENTS	EXTRACTED	FAILED	TRANSMITTED	FAILED
280	279	1	279	0

Figure 2-20: Failed Export window

15. Select **Extraction Failed** or **Transmission Failed** from the **Status** option.

16. Click the **Failure Reason** link to view the detailed error encountered during the export (Figure 2-21). Users can copy the information on the window and send it to their Quality Coordinator for review.



Job: c7fbbb08-c864-4a08-bf29-51e20ab5f456

Job Detail

Scheduled On: 11/8/2018 3:17:15 PM
Extracted On: 11/8/2018 3:20:41 PM
Transmitted On:

Export Schedule

Start Date: 1/1/2016 12:00:00 AM
End Date: 12/31/2018 11:59:59 PM
Extract Format: JSON

Patient

Name DEMO.JOHN DOE
IEN 26530

Exception Detail

Message

Object reference not set to an instance of an object.

Stack Trace

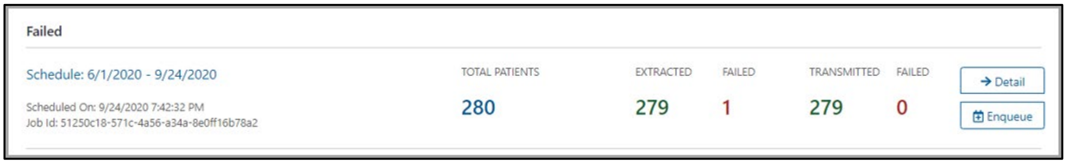
```
at Extractor.Core.Translators.PatientTranslator.Translate(Patient patient, Tenant tenant) in
C:\bit9prog\dev\repos\ECQM\ECQM\Extractor\Extractor.Core\Translators\PatientTranslator.cs:line 19 at
Extractor.Core.Services.ExtractionService.GenerateCat1Async(Tenant tenant, Int64 patientId, DateTime startDate, DateTime endDate, MeasureTarget
measureTarget) in C:\bit9prog\dev\repos\ECQM\ECQM\Extractor\Extractor.Core\Services\ExtractionService.cs:line 194 at
Extractor.App.ServiceQueue.ExtractionHostedService.ProcessJob(Job job) in
C:\bit9prog\dev\repos\ECQM\ECQM\Extractor\Extractor.App\ServiceQueue\ExtractionHostedService.cs:line 108 at
Extractor.App.ServiceQueue.ExtractionHostedService.BackgroundProcessing() in
C:\bit9prog\dev\repos\ECQM\ECQM\Extractor\Extractor.App\ServiceQueue\ExtractionHostedService.cs:line 82
```

Figure 2-21: Failed Reason Detail window

17. Click the **Back to Batch** button to return to the **Detail** window.

18. Click the **Back to Export** button to return to the **Export** window.

19. Click the **Enqueue** button under the **Failed** section (Figure 2-22) to re-export as needed.



Failed

Schedule: 6/1/2020 - 9/24/2020

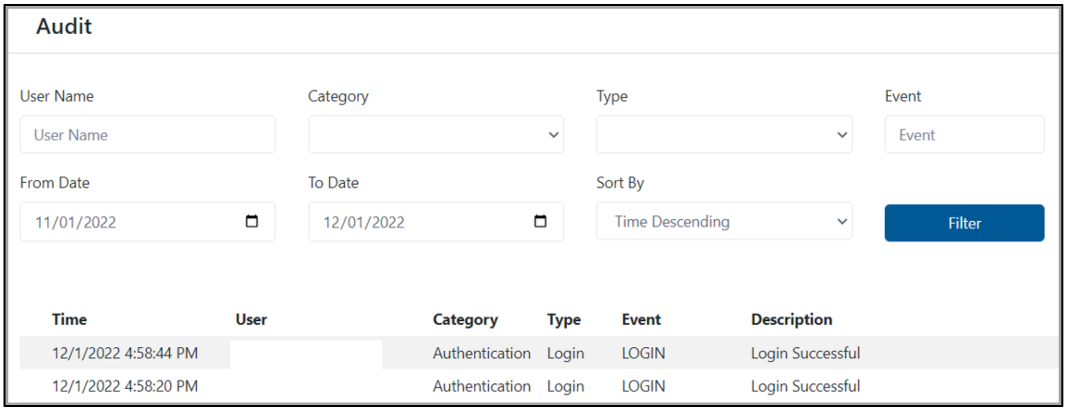
Scheduled On: 9/24/2020 7:42:32 PM
Job Id: 51250c18-571c-4a56-a34a-8e0ff16b78a2

TOTAL PATIENTS	EXTRACTED	FAILED	TRANSMITTED	FAILED
280	279	1	279	0

Figure 2-22: Failed Section window

2.2.4 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 (BUSAZRPT).



From Date: 11/01/2022

To Date: 12/01/2022

Sort By: Time Descending

Time	User	Category	Type	Event	Description
12/1/2022 4:58:44 PM		Authentication	Login	LOGIN	Login Successful
12/1/2022 4:58:20 PM		Authentication	Login	LOGIN	Login Successful

Figure 2-23: Audit window

To filter actions in the Audit window:

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 the **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.

2.2.5 Delete

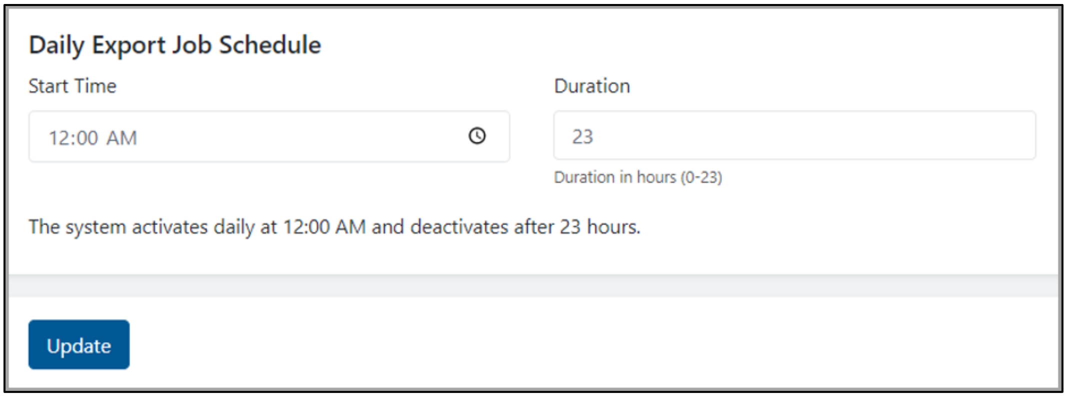
Use the **Delete** button to delete a site that is no longer needed.

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

2.3 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.



Daily Export Job Schedule

Start Time: 12:00 AM

Duration: 23

Duration in hours (0-23)

The system activates daily at 12:00 AM and deactivates after 23 hours.

Figure 2-24: Background Job Schedule dialog

2. Enter/Select **Start Time**. The default value is **12:00 AM**. Enter the **Start Time** in the **00:00 AM/PM** format.
3. Define the **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 website: https://home.ihs.gov/security/index.cfmhttp://security.ihs.gov/.

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

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

A.1 All RPMS Users

In addition to these rules, each application may include additional 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.
- 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 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 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 clinicians, 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

Acronym	Term Meaning
BMI	Body Mass Index
CEHRT	Certified Electronic Health Record Technology
CAH	Critical Access Hospitals
CMS	Centers for Medicare and Medicaid Services
CQM	Clinical Quality Measures
eCQM	electronic Clinical Quality Measures
ED	Emergency Department
EH	Eligible Hospital
EC	Eligible Clinician
HIT	Health Information Technology
HMPC	Home Management Plan of Care
IHS	Indian Health Service
OIT	Office of Information Technology
ONC	Office of the National Coordinator for Health Information Technology
PI	Promoting Interoperability
QRDA	Quality Reporting Document Architecture
RPMS	Resource and Patient Management System

Contact Information

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

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

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

Email: itsupport@ihs.gov