RESOURCE AND PATIENT MANAGEMENT SYSTEM

IHS USER SECURITY AUDIT Application Programming Interface

(BUSA)

User Manual

Version 1.0 Patch 4
November 2021

Office of Information Technology
Division of Information Technology

Table of Contents

Preface

The purpose of this User Manual is to provide information required to use the Indian Health Service (IHS) User Security Audit (namespace BUSA) package to capture and report on user activity within a given namespace. It includes information on utilizing the reporting utility available for Electronic Prescribing of Controlled Substances (EPCS).

Prerequisites

To utilize the audit log reporting utility the following is required:

- Experience with browser operation, preferably Chrome or Firefox
- RPMS login credentials for the RPMS site
- The **BUSARPC** option assigned to your RPMS user
- BUSA security key(s) assigned to your RPMS user
- An RPMS user added to the authorized BUSA user list in RPMS

To utilize the audit log remediation functionality the following is required in addition to the above:

- An RPMS user added to the Remediation Utility BUSA user list in RPMS

To utilize the BUSA archiving functionality the following is required:

- Technical ability to manipulate files into the relevant file structure
- Technical ability to identify and maintain file encryption methods
- Requisite system access to perform administrative actions on the RPMS server in both the underlying operating system and inside RPMS itself

1.0 Introduction

The BUSA package is a utility that enables tracking of user activity. As a requirement for Meaningful Use (MU) stage-two certification, all activity relating to patient-data querying, adding, editing, copying, deleting, and printing must be able to be logged. With the EPCS release, additional information gets logged into BUSA to meet Drug Enforcement Administration (DEA) auditing and reporting requirements. The subsequent BUSA version 1.0 Patch 3 release contained even more auditing and reporting functionality to allow IHS to be compliant with 2015 Certified Health IT (CHIT) certification requirements. The latest release, BUSA version 1.0 Patch 4, allows sites to address/remediate entries that show up on the EPCS incident reports.

1.1 Web-Enabled Reporting Interface

The BUSA package contains a Web-enabled reporting interface, which permits this logged data to be filtered, sorted, and displayed. It also contains a Web-enabled reporting interface, specifically designed to meet the reporting needs of EPCS. The Patch 3 release contains a reporting interface which allows users to view BUSA information that has been archived and restored back onto the system.

Important:The examples below were obtained from a test system. Your production RPMS system should be configured in accordance with best practices and security guidelines. If this is the case, all the URLs will begin with HTTPS:// instead of HTTP://, contrary to what is shown in the examples.

1.2 Web-Enabled Remediation Utility

The BUSA patch 4 release contains a web-based utility which allows sites to remediate certain entries that show up on the EPCS related incident reports.

1.3 BUSA Archiving Functionality

The Patch 3 release provides sites with the ability to archive older BUSA information into external files. Once the files have been verified, the associated data can be purged from the system and the external files can be moved to a secure location for storage. When needed, those files can be reloaded onto the system and reviewed.

1.3.1 Audit Data Archive Eligibility Limitations

EPCS requires that two years of audit data be maintained online to drive the audits required for that program. This limitation has been set as the minimum in the archiving application.

Ongoing investigations, litigation, or local policy may impose other requirements that must be considered when deciding what data is eligible to be archived.

1.3.2 When to Archive Audit Data

The first indication of the need to archive audit data is a limited amount of free disk space on the storage structure where audit data resides. A secondary indication is that the database backup windows are extending past their normal schedule.

Other additional indicators are the amount of media space required to store the database backups is more than what is expected, or the site might experience system performance degradation related to limited free space on storage media.

1.3.3 Storing Archived Audit Data

Under HIPAA guidance, audit data should be retained for at least six years. Local HIM guidance or litigation holds may extend this period. Storage media used for the archive data must be durable enough that the recorded data will survive the expected retention time.

> **Note:** Since the retention policy can vary, please refer to the policies implemented by your local governance to ensure your local procedures comply. Ensure that the storage mechanisms and procedures that are utilized take into account the need to remove archived audit information periodically.

The storage environment for the chosen media must be adequate to protect the media from hazards that could present themselves during the expected lifespan. These could include fire, tornadoes, hurricanes, flood, theft, etc. The local COOP plan will be helpful when planning.

The storage media must be encrypted to help prevent unintentional disclosure. Encryption keys should be securely stored separately in a manner that ensures they will be available throughout the expected lifespan of the data.

2.0 Package Management

The following security keys are available to use and control the BUSA application:

- **BUSAZMGR**

  This key is required to utilize the **BUSA Main Menu** (BUSAMENU) and **BUSA SECURITY EDIT** options.

- **BUSAZRPT**

  This key is required to be able to utilize the browser-based reporting tool.

- **BUSAZARCHIVE**

  This key is required to utilize the **BUSA ARCHIVE MENU** and archive activities.

- **BUSAZREMEDIATION**

  This key is required to utilize the browser-based remediation utility.

2.1 Access

Access to the BUSA Main Menu is restricted to site managers, who should run it only when necessary.

3.0 Package Operation

3.1 BUSA RPMS Main Menu

In RPMS, on the **BUSA Main Menu**, are the menu options, **BUSA Archive Menu** (**BA**) and **Edit Security Audit** (**BS**) (Figure 3-1).

The BA menu option allows users with the BUSAZARCHIVE security key to perform archive activities related to audit events.

```
                         ************************
                         **   BUSA Main Menu   **
                         ************************
                      IHS USER SECURITY AUDIT Version 1
                            2020 DEMO HOSPITAL

BA      BUSA Archive Menu ...

BS      Edit Security Audit
```

Figure 3-1: BUSA Archive Menu (BA) option

3.1.1 BUSA Archive Menu

The **BUSA Archive Menu** (Figure 3-2) has five menu options allowing users to perform archive activities related to audit events and one option to report on the auditing activity.

- **Archive BUSA Information**

  Allows the user to archive audit records for a date range. The start date is always the first date on file in the **BUSA AUDIT LOG SUMMARY** file (#9002319.01) or the date of the latest end date for a previous archive process. The end date is one year from the start date or a date two years in the past, whichever is earlier.

- **Verify Archive**

  Allows the user to verify that the archive files were generated successfully. This must be done before purging the original audit records.

- **Purge BUSA Records**

  Allows the user to purge the archived audit records from the current audit summary and detail files.

- **Load BUSA Archive File**

Allows the user to load a previously set of archived audit records to the RPMS database for review in the reporting interface.

- **Remove Restored Records**

  Allows the user to remove the reloaded archived audit records once the review is complete.

- **Archive Report**

  Allows the user to review a previous archive audit process.

```
                    ********************************
                    **   BUSA Data Archive Menu   **
                    ********************************
                   IHS USER SECURITY AUDIT Version 1
                          2020 DEMO HOSPITAL

   AI     Archive BUSA Information

   VA     Verify Archive

   PA     Purge BUSA Records

   LA     Load BUSA Archive File

   RR     Remove Restored Records

   AR     Archive Report
```

Figure 3-2: BUSA Data Archive menu

3.1.1.1 Archive BUSA Information (AI)

The **Archive BUSA Information** option (Figure 3-3) allows users to archive audit records for a date range. The start date is the date associated with the earliest IEN on file. If a previous archive has been created, the start date is the date of the first record after that the last record to be archived.

```
                    *********************************
                    **   Archive BUSA Information   **
                    *********************************
                     IHS USER SECURITY AUDIT Version 1
                           2020 DEMO HOSPITAL

This option allows BUSA information to be archived into files so that the
online information can later be purged from the system. Running this option
will only create the archive file(s). It will not purge any date from the
system. Reporting regulations require that a minimum range of auditing data
remain on the system. The latest date allowed for archiving is: 8/4/2018


The earliest BUSA Summary information on file is for date: 11/19/2013
With IEN: 234
```

Figure 3-3: Archive BUSA Information screen

- EPCS requires that at least two years of auditing data remain on the system, so the latest date allowed for archiving is determined by the current date.
- In addition, the archive can only be run for a maximum of one year from the first audit entry on file.
- The user is prompted for the end date and defaults to the end of the month associated with the earliest date. Once the date is selected, the date and time associated with a specific IEN will display.
- The number of records will be computed including both summary and detail records. Additionally, record cross-references will be archived. Depending on the date range chosen, this computation could take several minutes to complete.

```
Each archive process can be run for a maximum date range of one year from
the first audit entry on file. To get an idea of how much data will be
archived, it is recommended that, at first, a smaller date range, such as
one month, be used. Sites can then increase the date range used for future
archives if the amount of generated archived data can easily be handled.

Enter the date to archive BUSA records to (up to 11/19/2014): 11/30/2013//
11/25/2013   (NOV 25, 2013)

The following record will be the final record archived:
Date/time: 11/25/2013 18:06:35 with IEN: 2607


Calculating the number of entries that will be archived. Each summary
and detail entry will be composed of one or more output records. In
addition, record cross references will also be archived. This
calculation process may take several minutes to complete:


Total BUSA Summary entries to be archived: 2374
Total BUSA Detail entries to be archived: 6840
```

Figure 3-4: Archive BUSA Information date screen

3.1.1.1.1 Archive File Size

Users are asked for the approximate file size for each archive (Figure 3-5) to ensure that the generated files do not grow too large. Subsequent files will be generated when the current file reaches the approximate maximum file size. The minimum file size is 10 MB, and the maximum is 10,000 MB. Users should base their answer on their storage media that they plan on using.

```
Enter the approximate file size for each archive file in this archive set.
The archive process will automatically create a new file when the archive
output has reached this approximate file size. The response should be
entered in Megabytes (MB), omitting commas and fractional values.
The minimum file size is 10 MB, and the maximum file size is 10000 MB.
As a reference a standard CD holds approximately 740 MB and a single
sided DVD holds approximately 4700 MB.

Enter the approximate size of each archive file in Megabytes (MB): 10// 20
```

```
Enter the path of the folder to place the archive file(s) in. Since the
generated files contain patient information, please ensure the location
is encrypted and accessible by only the appropriate personnel.

Enter response: E:\PUB\//

Do you wish to continue: N// YES
```

Figure 3-5: Archive BUSA Information screen continued

- The user is then prompted for the file path for the generated archive file(s). Since these files may contain PII/PHI related to patients, ensure that the location is encrypted and accessible only to appropriate personnel.
- The default location is the **RPMS SITE** file **FILE EXPORT PATH** field, which has restricted access and is encrypted by policy.
- Enter the file path target and confirm that you wish to continue.

3.1.1.1.2 System Resources

Users are warned that the archive process may tax system resources, so queuing as a background process is recommended. Users are prompted to queue the process. Entering **NO** allows the process to complete in the foreground (Figure 3-6).

```
This process may make extensive use of system resources. It may also
require a large amount of storage space to complete. Please also make
sure that your system is not overloaded while this process is running
as it may impact system performance. In addition, this process may take
several hours to complete. It is therefore highly recommended that the
archive process be tasked off as a background process.

Would you like to queue this process: Y// NO

Running the archive process in the foreground:

Creating file: BUSA_PRECERT_2906_3131119_234.txt

Archive process completed successfully. Please run the Verify Archive
option to confirm that the archive files were generated correctly.
```

Figure 3-6: System Resources warning screen

When run in the foreground, the files created are displayed to the screen and a successful completion message is displayed.

> **Note:** Once completed, it is advised that the **Verify Archive** option is run to ensure that the archive files are correctly formatted.

3.1.1.2 Verify Archive (VA)

The **Verify Archive** option allows users to verify archived audit records prior to purging (Figure 3-7).

The option lists the archived files that are available for verification and prompts the user if they wish to verify the files available. If they choose to verify, a prompt displays with the secure file location.

As with the Archive option, the process can be queued or run in the foreground. If run in the foreground, the status displays to the screen.

```
                  ****************************************
                  **   Verify Archived BUSA Information   **
                  ****************************************
                       IHS USER SECURITY AUDIT Version 1
                              2020 DEMO HOSPITAL

The following files have been created and are waiting to be verified:


CREATION DATE     FILENAME                                          # RECORDS
08/05/2020 15:07  BUSA_PRECERT_2906_3131119_234.txt                     60399

Do you wish to verify these files: N// YES

Enter the path of the folder which contains the archive file(s). Since the
generated files contain patient information, please ensure the location
is encrypted and accessible by only the appropriate personnel.

Enter response: E:\PUB\//

This process may make extensive use of system resources. Please make
sure that your system is not overloaded while this process is running
as it may impact system performance. In addition, this process may take
several hours to complete. It is therefore highly recommended that the
archive verification process be tasked off as a background process.

Would you like to queue this process: Y// NO

Running the archive verification process in the foreground:

Verifying file: BUSA_PRECERT_2906_3131119_234.txt
Verification succeeded

Archive verification process completed successfully. The records can now
be purged.
```

Figure 3-7: Verify Archive option screen

If the verification process completed successfully, the user is informed that the archived records can now be purged.

If errors or warnings are found, the following indication will display ****Errors present**** or ****Warnings present**** and the user will be prompted with the opportunity to review them.

3.1.1.3 Purge BUSA Records (PU)

Once audit records are archived to one or more files and the archive has been verified, the audit records can be purged from the RPMS database (Figure 3-8). If the files passed verification, but had warnings, the user is prompted to view the warnings.

```
                    ************************************
                    **   Purge Archived BUSA Records   **
                    ************************************
                       IHS USER SECURITY AUDIT Version 1
                             2020 DEMO HOSPITAL

The following files have been verified.
The data contained in them can now be purged.

File                                                  Status
BUSA_PRECERT_2906_3131119_234.txt                     Verification succeeded
                                                        **Warnings present**

One or more of the files passed verification but had warnings.


Filename: BUSA_PRECERT_2906_3131119_234.txt

Record 52666       '^BUSAD("C","IFCR",6670)' "C" cross reference exists in
RPMS but is corrupted


Press Enter to Continue:

To purge the auditing information from the system, a final check is
required to confirm the existence of the archived files.
After the purge is complete, it is recommended that these files
be moved to a secure location where they will not accidentally
get deleted.

Enter the path of the folder which contains the archive file(s). Since the
generated files contain patient information, please ensure the location
is encrypted and accessible by only the appropriate personnel.

Enter response: E:\PUB\//

Searching for verified files in the chosen path:
Searching for file: BUSA_PRECERT_2906_3131119_234.txt ...found

All of the verified files have been located. Are you sure that
you want to purge the information contained in these files off
of the system? Once the data has been removed, it can only be
reloaded as archived auditing files. Type the full word 'YES'
at the prompt to proceed with the information purge.

Purge auditing information: NO// YES

This process may make extensive use of system resources. Please make
```

```
sure that your system is not overloaded while this process is running
as it may impact system performance. In addition, this process may take
several hours to complete. It is therefore highly recommended that the
archive purge process be tasked off as a background process.

Would you like to queue this process: Y// NO

Running the archive purge process in the foreground:

Purging BUSA records archived to file: BUSA_PRECERT_2906_3131119_234.txt

Archive purge process completed successfully. The records have now been
properly archived.
```

Figure 3-8: Purge BUSA records screen

If **YES** is entered to review the warnings, the warning detail is displayed on the screen (Figure 3-9). If there is only one file to verify with warnings, the warning detail will automatically display.

Press Enter to continue with the purge process. A reminder appears stating that the files must be moved to a secure location where they will be preserved, if necessary, to review at a later date.

```
Filename: BUSA_PRECERT_2906_3131119_234.txt

Record 52666       '^BUSAD("C","IFCR",6670)' "C" cross reference exists in
RPMS but is corrupted


Press Enter to Continue:

To purge the auditing information from the system, a final check is
required to confirm the existence of the archived files.
After the purge is complete, it is recommended that these files
be moved to a secure location where they will not accidentally
get deleted.

Enter the path of the folder which contains the archive file(s). Since the
generated files contain patient information, please ensure the location
is encrypted and accessible by only the appropriate personnel.

Enter response: E:\PUB\//
```

Figure 3-9: Purge BUSA warning screen

Next, the user is prompted for the location of the archived files again to confirm their existence before performing the purge.

If the verified files are found, a prompt appears to begin the purge by entering **YES** at the "Purge auditing information" prompt (Figure 3-10).

```
Searching for verified files in the chosen path:
Searching for file: BUSA_PRECERT_2906_3131119_234.txt ...found
```

```
All of the verified files have been located. Are you sure that
you want to purge the information contained in these files off
of the system? Once the data has been removed, it can only be
reloaded as archived auditing files. Type the full word 'YES'
at the prompt to proceed with the information purge.

Purge auditing information: NO// YES
```

Figure 3-10: BUSA begin purge prompt

Finally, users may queue the process as a background task, if appropriate (Figure 3-11). Default to **(Y)ES** to queue or **NO** to run in the foreground. If run in the foreground, the files will be listed as the records are purged with a successful completion message.

```
This process may make extensive use of system resources. Please make
sure that your system is not overloaded while this process is running
as it may impact system performance. In addition, this process may take
several hours to complete. It is therefore highly recommended that the
archive purge process be tasked off as a background process.

Would you like to queue this process: Y// NO

Running the archive purge process in the foreground:

Purging BUSA records archived to file: BUSA_PRECERT_2906_3131119_234.txt

Archive purge process completed successfully. The records have now been
properly archived.
```

Figure 3-11: BUSA purge process run in foreground

Note: Purging audit records will not automatically recover space in the RPMS database. The database must then be compressed/compacted to free up the space. If this is the first time that BUSA purging has been done, it is highly recommended that a support request to the IHS Support Team be logged to walk the site through the steps to compress/compact the database so that the process is completed successfully.

3.1.1.4 Load BUSA Archive File (LA)

The **Load BUSA Archive File** option (Figure 3-12) allows a user to load previously archived files into the database to review in the reporting utility.

These files are loaded into a separate area in RPMS apart from the regular audit records so that they can be removed again when their review is completed. The user will be prompted for the specific filename(s) (case sensitive) to reload.

```
                    ***************************************
                    **   Load Archived BUSA Information   **
                    ***************************************
                        IHS USER SECURITY AUDIT Version 1
                               2020 DEMO HOSPITAL


This option will allow an external BUSA archived file to be loaded into
the BUSA archive files so that the information contained in it can be
reviewed. This option will not interfere with existing BUSA auditing
functionality and reporting.

You will now be prompted to enter the name of the files that are to be
loaded. The filename lookup is case sensitive. After entering all of the
filenames to be loaded, hit enter to continue.

Enter the filename to load: BUSA_PRECERT_2906_3131119_234.txt
Enter the filename to load:
```

Figure 3-12: Load BUSA Archive File option screen

Users are prompted to enter the path that contains the archive file(s) to be loaded (Figure 3-13). This should be in a secure location as well. Once the files are confirmed in the location, users are prompted to begin loading the audit records for review.

```
Enter the path of the folder which contains the archive file(s). Since the
generated files contain patient information, please ensure the location
is encrypted and accessible by only the appropriate personnel.

Enter response: E:\PUB\//

Searching for archived files in the chosen path:
Searching for file: BUSA_PRECERT_2906_3131119_234.txt ...found

All of the archived files have been located. Are you sure that
you want to load the information contained in these files into
the online BUSA archive files. Type the full word 'YES' to
load the files.

Load auditing information: NO// YES
```

Figure 3-13: Enter BUSA archive file path screen

The loading process may also be queued. If run in the foreground, the file(s) display as they are loaded successfully (Figure 3-14).

```
This process may make extensive use of system resources. Please make
sure that your system is not overloaded while this process is running
as it may impact system performance. In addition, this process may take
several hours to complete. It is therefore highly recommended that the
archive load process be tasked off as a background process.

Would you like to queue this process: Y// NO

Running the archive load process in the foreground:
```

```
Loading file: BUSA_PRECERT_2906_3131119_234.txt
Load succeeded

Archive load process completed successfully.
The records have now been loaded.
```

Figure 3-14: BUSA archive loading process

A final successful completion message will display after all the files are loaded.

At this point, the BUSA Zen Archive report, which replicates that existing BUSA Zen Main Audit report, can be used to review the reloaded audit records.

3.1.1.5 Remove Restored Records (RR)

The **Remove Restored Records** option (Figure 3-15) allows users to remove previously loaded archived files when the review is no longer necessary.

```
                    ****************************************
                    **   Remove Restored BUSA Information   **
                    ****************************************
                         IHS USER SECURITY AUDIT Version 1
                                2020 DEMO HOSPITAL
ENTRY     FILENAME
1         BUSA_PRECERT_2906_3131119_234.txt

Select the ENTRY # to be removed or hit enter to continue: 1

You have chosen to remove the records associated with the
following file out of the BUSA archives:

BUSA_PRECERT_2906_3131119_234.txt
```

Figure 3-15: Remove Restored Records option

The option will list the files loaded that are available to be removed. Select the Entry # in the list to be removed.

The user is then prompted to confirm the removal of the reloaded records. Users must type **YES** to continue (Figure 3-17). The default is **NO** to cancel the removal.

```
Are you sure you want to remove these records from the BUSA
Archive Summary and Detail RPMS files? Once the records have
been removed they can be reloaded again if needed. Type the
full word 'YES' to continue.

Remove reloaded records: NO// YES
```

Figure 3-16: Confirm removal of reloaded

As with the other options, users may choose to queue this to run in the background or run in the foreground (Figure 3-17). The default is **Yes** to run in the background.

```
This process may make extensive use of system resources. Please make
sure that your system is not overloaded while this process is running
as it may impact system performance. In addition, this process may take
some time to complete. It is therefore highly recommended that the
reloaded record archive removal process be tasked off as a background
process.

Would you like to queue this process: Y// NO
```

Figure 3-17: Remove restored records background process request

When run in the foreground, the files are listed as the audit records are removed (Figure 3-18). A message indicating the successful completion displays to the user.

```
Running the reloaded record removal process in the foreground:

Removing records reloaded from archive file:
BUSA_PRECERT_2906_3131119_234.txt

The reloaded record removal process completed successfully.
The records have now been properly removed.
```

Figure 3-18: Reloaded record removal process screen

3.1.1.6 Archive Report (AR)

The **Archive Report** option (Figure 3-19) allows the user to review archive status history for:

- **All History**
- **Created files** – Archived
- **Purged files** – Archived, verified, and purged
- **Verified files** – Archived and verified

Select the report type desired.

```
                          ****************************
                          **   BUSA Archive Report   **
                          ****************************
                         IHS USER SECURITY AUDIT Version 1
                                2020 DEMO HOSPITAL

Select the archive status history to display


     Select one of the following:

          A         All History
          C         Created files
```

```
          P         Purged files
          V         Verified files
          Q         Quit

Select the report type: All History
```

Figure 3-19: Archive Report option screen

The user may select how many records per page to display for readability (Figure 3-20). The default is 10.

Data is displayed by Archive # to include:

- # – Sequential archive identifier
- FILENAME – Name of file created
- ARCHIVE DATE – Date/time of first audit record archived in the file
- CRT (Created Date) – Date the archive file was created
- VER (Verified Y/N) – Has the file been verified – Yes or No
- PRG (Purged Y/N) – Have the audit records in the file been purged – Yes or No
- LOAD (Loaded Y/N) – Has the file been loaded for review – Yes or No

```
Enter the records per page to display:  (2-9999): 10//
#    FILENAME                          ARCHIVE DATE    CRT    VER PRG LOAD

1    BUSA_PRECERT_2906_3131119_234.txt  11/19/13 08:13  08/20    Y   Y
```

Figure 3-20: Archive records to display screen

Users may select an Entry to review the detail (Figure 3-21). This detail identifies the date and time of each action and the user associated with that action.

Actions include:

- **Archive**
- **Verify**
- **Purge**
- **Restore**

```
Select the ENTRY # to view the detail or enter to exit: 1
ENTRY DETAIL:

ARCHIVE TIMESTAMP: AUG 05, 2020@15:07:16
  ARCHIVE USER: DEMO,TRENTON
  ARCHIVE START DATE: NOV 19, 2013@08:13:31
  ARCHIVE END DATE: NOV 25, 2013@18:06:35
  FIRST ARCHIVE BUSA RECORD: 234        LAST ARCHIVE BUSA RECORD: 2607
  TOTAL RECORDS IN ARCHIVE: 60399       VERIFICATION COMPLETE: YES
```

```
  VERIFICATION DATE: AUG 05, 2020@15:07:44
  VERIFICATION USER: DEMO,TRENTON
  ARCHIVE FILENAME: BUSA_PRECERT_2906_3131119_234.txt
  ARCHIVE PURGE DATE: AUG 05, 2020@15:09:55
  ARCHIVE PURGE USER: DEMO,TRENTON STATUS: ARCHIVED
RESTORED ARCHIVE DATE: AUG 05, 2020@15:16:16
  RESTORED ARCHIVE USER: DEMO,TRENTON
  RESTORED ARCHIVE RECORDS: 60399
  RESTORED ARCHIVE PURGE DATE: AUG 05, 2020@15:17:18
  RESTORED ARCHIVE PURGE USER: DEMO,TRENTON
```

Figure 3-21: Select an Entry to Review screen

3.1.1.7 Review Restored Records in Browser

Similar to the existing Audit report in the browser, the reloaded audit records can be reviewed using the link **BUSA.ArchiveReportPage.cls** rather than **BUSA.MainReportPage.cls** (Figure 3-22).

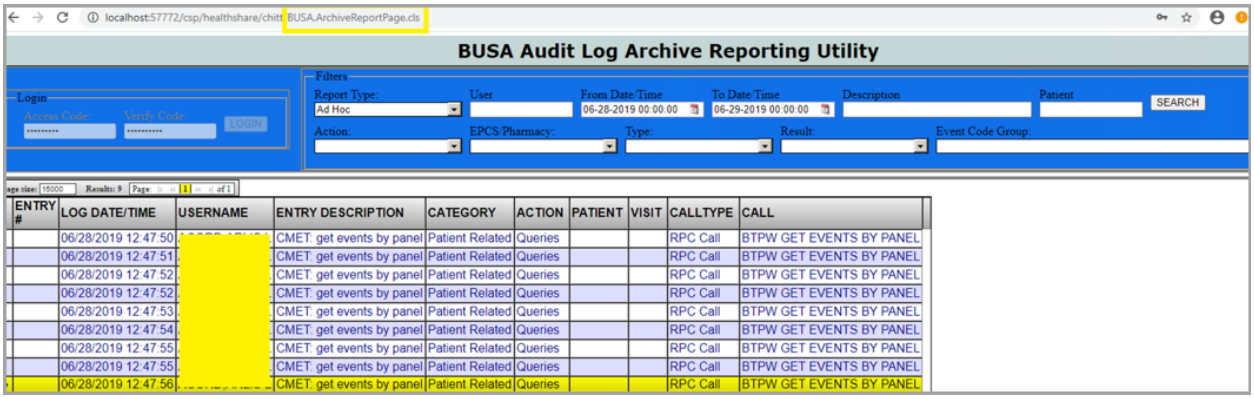

Figure 3-22: Viewing restored records window

3.1.2 Edit Security Audit

BUSA is installed with each of the Security Audit switches turned on. Patch 3 contains a new FileMan switch which can also be enabled/disabled.

```
                          ************************
                          **   BUSA Main Menu   **
                          ************************
                      IHS USER SECURITY AUDIT Version 1
                           2020 DEMO HOSPITAL

   BA     BUSA Archive Menu ...

   BS     Edit Security Audit
```

Figure 3-23: BUSA Archive Menu (BS) option

The **Date Logged** field displays the date and time that the link was either turned on or turned off. The **User Logged** field displays the user who performed the action on the link, as shown in Figure 3-24.

```
Edit Security Audit
Current Security Audit Settings:
     Master         Status:        On
                    Date Logged:   AUG 05, 2020@16:05:52
                    User Logged:   DEMO,USER
     BMXNet         Status:        On
                    Date Logged:   AUG 05, 2020@16:05:52
                    User Logged:   DEMO,USER
     CIA Broker     Status:        On
                    Date Logged:   AUG 05, 2020@16:05:52
                    User Logged:   DEMO,USER
     XWB Broker     Status:        On
                    Date Logged:   AUG 05, 2020@16:05:52
                    User Logged:   DEMO,USER
     FileMan        Status:        Disabled
                    Date Logged:   AUG 06, 2020@11:57:58
                    User Logged:   DEMO,USER
           Disabled Comment:Disabling FileMan auditing in production

     Select one of the following:

          M         Master
          B         BMXNet
          C         CIA Broker
          W         XWB Broker
          F         FileMan

Select Switch:
```

Figure 3-24: Enabling and disabling switches

Anytime a switch is turned off or on, an audit trail of the information—when the function was performed and by whom—is logged, as shown in Figure 3-25.

```
Edit Security Audit
     Select one of the following:

          M         Master
          B         BMXNet
          C         CIA Broker
          W         XWB Broker
          F         FileMan

Select Switch: W  XWB Broker

     Select one of the following:

          1         On
          0         Disabled

Change Status: On// 0  Disabled
Disable Comment: Disabled for testing
Select Switch:
```

```
     XWB Broker     Status:        Disabled
                    Date Logged:   AUG 06, 2020@16:18:21
                    User Logged:   DEMO,USER
           Disabled Comment:Disabled for testing
```

Figure 3-25: Audit trail

4.0 GUI Report

4.1 BUSA Main Report Utility

The Main BUSA reporting utility can be accessed at the following address:

http://*ip address*:*port*/csp/*namespace*/BUSA.MainReportPage.cls.

Sites should replace the internet protocol (IP) address with the address of the Resource and Patient Management System (RPMS) server, the port with the proper port number, and replace namespace with either the namespace of the RPMS live database or with BUSA. The value of namespace is determined by how the site chose to set up the CSP application for the BUSA version 1.0 release. See version 1.0 release of the *IHS User Security Audit (BUSA) Installation Guide and Release Notes* for further details on determining these values.

Note:	The report utility displays best in Firefox or Chrome. Internet Explorer has an issue with displaying row heights too large.

4.1.1 BUSA Report Utility Log In

1. Paste the following address in a Windows browser (preferably Firefox or Chrome), replacing the *ip address, port,* and *namespace*, as described in Section 4.1.

   http://*ip address*:*port*/csp/*namespace*/BUSA.MainReportPage.cls

   The BUSA Main Audit Log Reporting Utility window displays. Figure 4-1 shows the initial display.

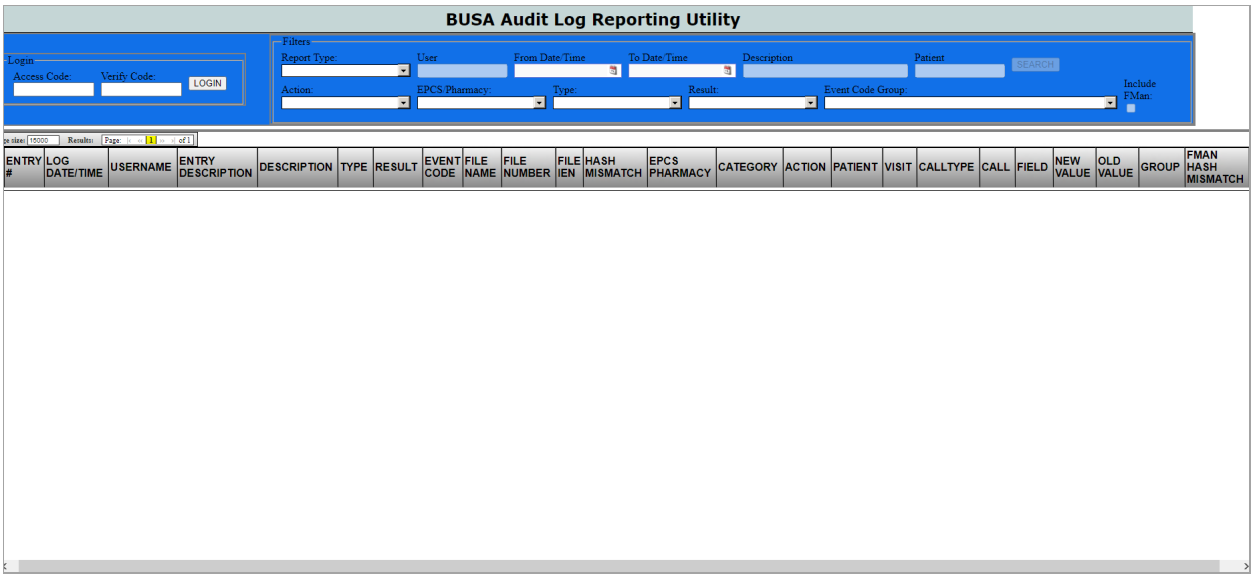

Figure 4-1: Initial BUSA Audit Report display (prior to login)

2. Enter the RPMS **Access Code** and **Verify Code** to log in.

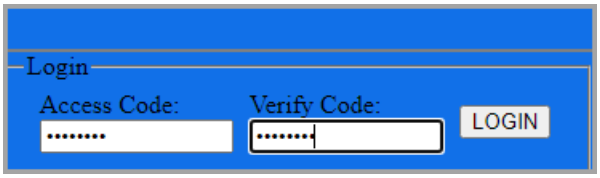

Figure 4-2: BUSA login fields

3. Click **LOGIN**.

Users who are assigned the BUSAZRPT security key and set up as report users during the BUSA installation process, will gain access to the BUSA filtering properties as shown in Figure 4-3.

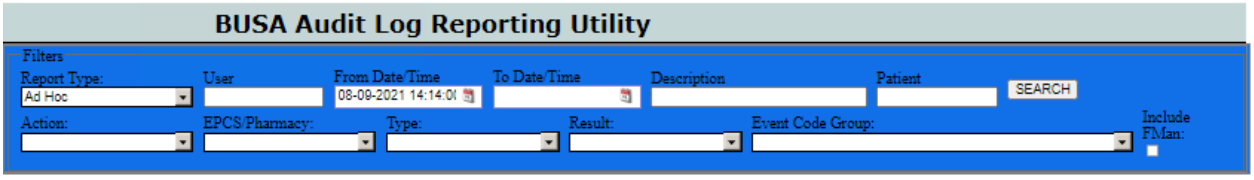

Figure 4-3: Authorized BUSA user successfully logged in

4.1.2 Conduct Filter Searches

Users can select multiple report types and as many filter options (Figure 4-4) as needed to produce customized audit reports.

When doing a search, if the number of records returned is still large, consider using additional filters. The number of results indicates the number of records found.

The filter options, as shown in Figure 4-4, are as follows:

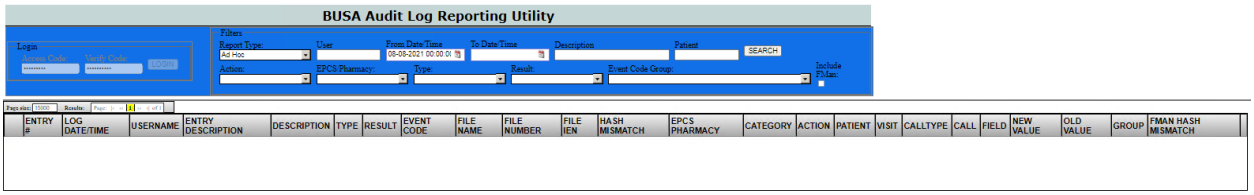

Figure 4-4: BUSA search filter fields

4.1.2.1 Report Type Search

To search for a specific report type, click the arrow in the **Report Type** field. The following reports are available as shown in Figure 4-5:

- **Ad Hoc:** The Ad Hoc Report display format shows BUSA information in the same format as the original BUSA report utility. The **Entry Description** field frequently contains multiple pieces of information per record, with each piece delimited by a vertical bar (|) character.
- **BUSA FileMan –** This report is similar to the List report, as it decomposes the Description field into separate columns. However, unlike the List report, this report is focused on displaying the FileMan audit columns including **File Name**, **File Number**, **File IEN**, and **FMan Hash Mismatch**.

  A value in the FMan Hash Mismatch column indicates that the audit event may have been tampered with.

- **FileMan Report** – Events with new and old values will only be recorded when FileMan detailed auditing is enabled.

  Note: It is recommended that the site disable FileMan detailed auditing, as the number of audit events recorded will have a negative impact on performance and could quickly exhaust the disk space available to the databases.

  This report displays the before and after values by file and field, as well as deletions. After values are displayed in the **New Value** column and before values are displayed in the **Old Value** column. The **Action** column indicates Additions, Changes and Deletions.

As in the BUSA FileMan report, the **FMan Hash Mismatch** column indicates that the audit event may have been tampered with.

- **List** – This report type display separates the delimited Description field data into individual columns like **Type**, **Result**, and **Event Code** to allow easier review and export.

Note: FMan audit entries still have delimiters.

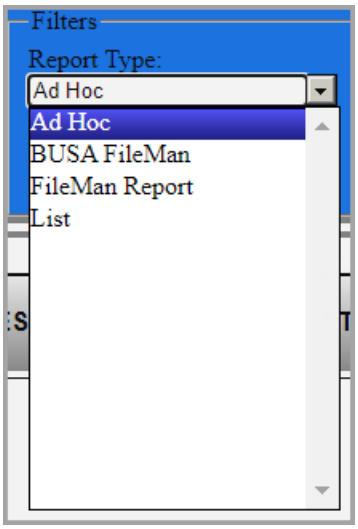

Figure 4-5: Report Types filter

4.1.2.2 User Search

Type the **Last Name** or **Last Name,First Name** to search and focus on the events related to a specific user. Partial lookups are allowed and a **Starts with** field match can be performed.

4.1.2.3 From Date/Time and To Date/Time Search

When doing a search, at a minimum, users should select the **From Date/Time** (see Figure 4-6) and **To Date/Time** (see Figure 4-7) filters to focus the date range of events and to limit the number of records returned.

- **From Date/Time:** Enter a starting date/time for the search.

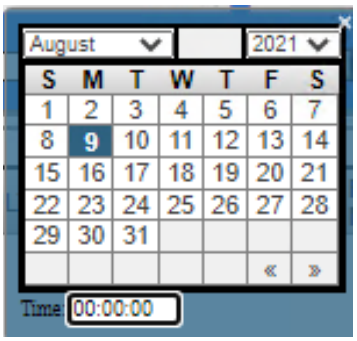

Figure 4-6: From Date/Time filter calendar

- **To Date/Time:** Enter an ending date/time for the search.

Figure 4-7: To Date/Time filter calendar

4.1.2.4 Description

Type a search term like EHR or Lab to focus on a particular event. Partial lookups are allowed, and a **String contains** field match can be performed.

4.1.2.5 Patient

Use the **Last Name** or **Last Name,First Name criteria** to search and focus on the events related to a specific patient. Partial lookups are allowed and a **Starts with** field match can be performed.

4.1.2.6 Action

Use Additions, Changes, Deletions, etc. to review specific types of actions recorded. Click the arrow in the **Action** field (see Figure 4-8). The following criteria can be selected:

- **Access to patient information:** Not applicable at this time.

- **Additions:** Adding new data.
- **Change to audit log status:** Any action to enable or disable auditing for certain modules of the certified EHR.
- **Change to encryption status:** Not applicable at this time.
- **Change to user privileges:** Any action to modify user class or XPAR parameters.
- **Changes:** Any modification of existing data.
- **Deletions:** Any deletion of existing data.
- **Emergency access:** Not applicable at this time.
- **Print: Any printing of patient data from an application.**
- **Queries:** Any event that produces a list of patient data.

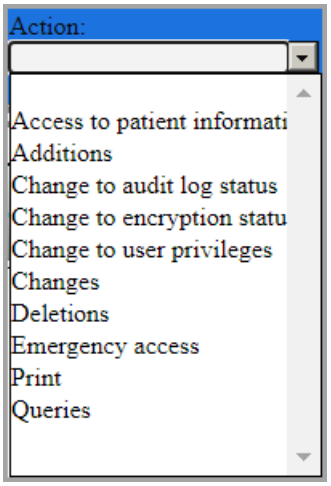

Figure 4-8: Action filter list

4.1.2.7 EPCS/Pharmacy

This filter is based on the value of the List report **EPCS Pharmacy** column values (E, P, or EP). (See Figure 4-9.) The options available for selection for this filter are as follows:

- **Both E/P:** Returns only BUSA entries with an EPCS Pharmacy value of **EP**.
- **Either E/P:** Returns BUSA entries with an EPCS Pharmacy value of **E**, **P**, or **EP**
- **EPCS:** Returns BUSA entries with an EPCS Pharmacy value of **E** or **EP**.
- **Pharmacy:** Returns BUSA entries with an EPCS Pharmacy value of **P** or **EP**.

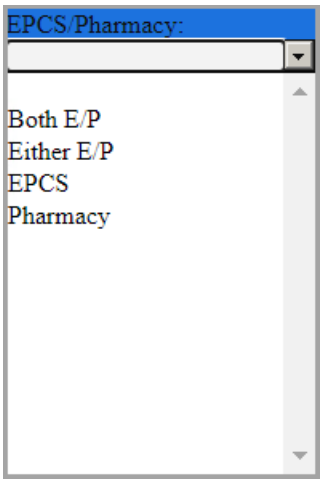

Figure 4-9: EPCS/Pharmacy filter list

4.1.2.8 Type

Select the arrow in the **Type** field (see Figure 4-10). This filter is based on the value of the List report **Type** column values. The options available for selection for this filter are as follows:

- **Credentials:** Type column value **C**
- **FileMan Audits:** Type column value **F**
- **General:** Type column value **G**
- **Keys:** Type column value **K**
- **Login:** Type column value **L**
- **Menus:** Type column value **M**
- **Options:** Type column value **O**
- **Pharmacy:** Type column value **P**
- **Provider Profile:** Type column value **PP**
- **Rx:** Type column value **X**
- **Services:** Type column value **S**
- **User Class:** Type column value **UCM**
- **XPAR Parameters:** Type column value **NP**

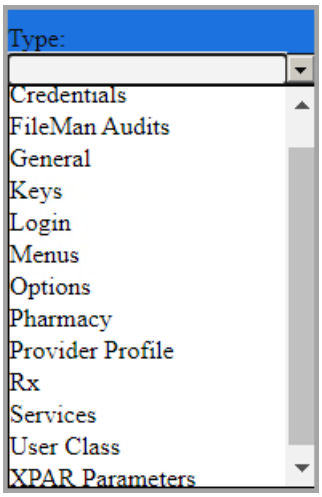

Figure 4-10: Type filter list

4.1.2.9 Result

Select the arrow in the **Result** field (see Figure 4-11). This filter is based on the value of the List report **Result** column values. The options available for selection for this filter are:

- **Failure:** Result column value F. Can capture all failures of a search.
- **Success:** Result column value S. Can capture all failures of a search.

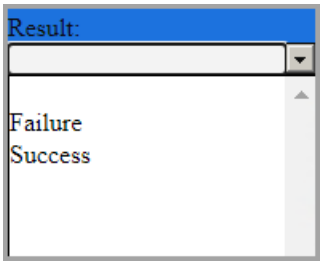

Figure 4-11: Result filter list

4.1.2.10 Enter Code Group

The following are classifications of events related to EPCS. Select the arrow in the **Enter Code Group** field. The following criteria can be selected:

- **Integrity Checks (Tampering)**
- **Logical Access Control – Access Pharmacy Menus**

- **Logical Access Control – Credentialing**
- **Logical Access Control – Logins**
- **Logical Access Control – Pharmacy Keys**
- **Logical Access Control – Pharmacy Menus**
- **Logical Access Control – Writing Med Orders**
- **Miscellaneous**
- **Multi-Factor Authenticate**
- **Ordering/Pharmacy Processing**
- **Provider Profile**
- **Time Synchronization**

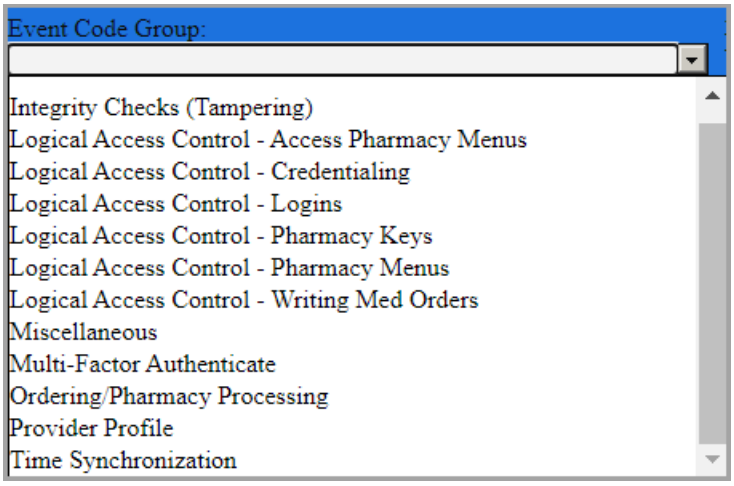

Figure 4-12: Event Code Group filter list

4.1.2.11 Include FMan

Select this check box to include detailed information about data changes if the FileMan detailed auditing is enabled. If BUSA FileMan or FileMan Report are selected from the Report Type list, then this check box is automatically selected.

Figure 4-13: Include FMan check box

After selecting the appropriate report filters, click the **SEARCH** button to run a report.

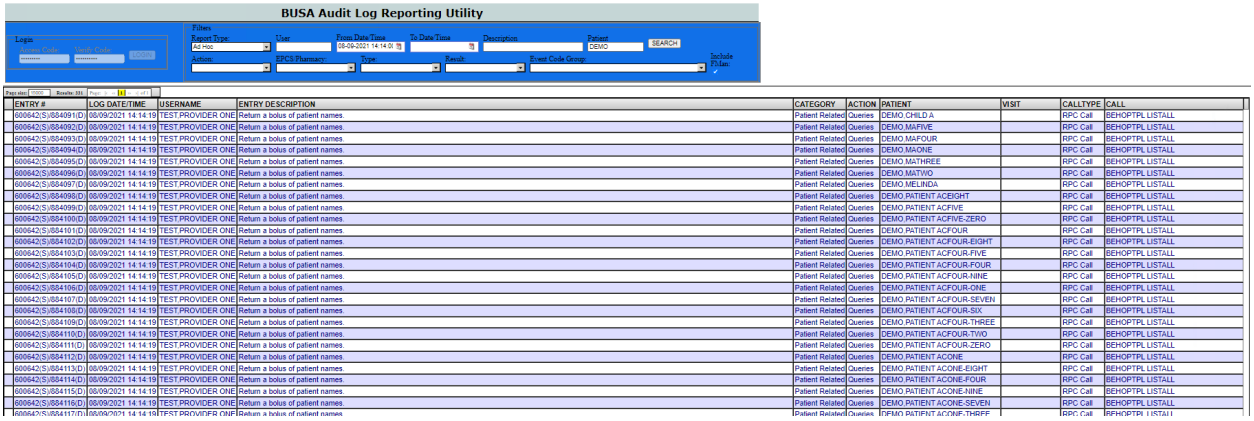

Figure 4-14: Performing a search using filters

4.1.3 Sorting Results

Search results can also be sorted. After obtaining results, click any of the column headers to change the search the results to an ascending order.

Click the column header a second time to return the sort display back to descending order.

See Figure 4-15 for a display of an ascending sort by **Visit**.

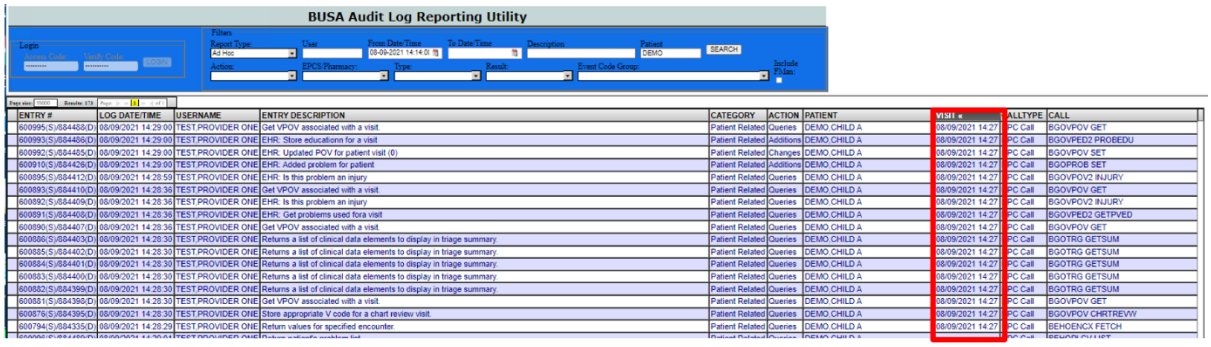

Figure 4-15: Sample display sorting by Visit date/time in ascending order

4.2 BUSA Archive Report Utility

The Archive reporting utility delivered with BUSA Patch 3 can be accessed at the following address:

http://ip address:port/csp/namespace/BUSA.ArchiveReportPage.cls

Sites should replace the internet protocol (IP) address with the address of the Resource and Patient Management System (RPMS) server, the port with the proper port number, and replace namespace with either the namespace of the RPMS live database or with BUSA. The value of namespace is determined by how the site chose to set up the CSP application for the BUSA version 1.0 release. See version 1.0 release of the *IHS User Security Audit (BUSA) Installation Guide and Release Notes* for further details on determining these values.

> **Note:** The report utility displays best in Firefox or Chrome. Internet Explorer has an issue with displaying row heights too large.

The Archive Report Utility is new for Version 1 Patch 3 and only utilized to review reloaded audit records. It is not intended for regular use. It works identically to the Audit Report Utility.

4.3 EPCS BUSA Report Utility

The EPCS BUSA Report Utility can be accessed by going to the address listed below. Sites should replace the IP address with the address of the RPMS server, port with the proper port number, and replace namespace with either the namespace of the RPMS live database or with BUSA. The value of namespace is determined by how the site chose to set up the CSP application for the BUSA version 1.0 release. See version 1.0 release of the *IHS User Security Audit (BUSA) Installation Guide and Release Notes* for further details on determining these values.

http://*IP address*:*port*/csp/*namespace*/BUSA.EPCSMainReportPage.cls

See the *IHS User Security Audit (BUSA) Installation Guide and Release Notes* for further details on determining these values.

> **Note**: The EPCS report utility displays best using Firefox or Chrome. Internet Explorer has an issue with display row heights too large.

4.3.1 EPCS BUSA Report Utility Log In

1. Paste the following address in a Windows screen, replacing the *ip address, port,* and *namespace*, as appropriate:

http://*IP address*:*port*/csp/*namespace*/BUSA.EPCSMainReportPage.cls

The report screen displays. See Figure 4-16.

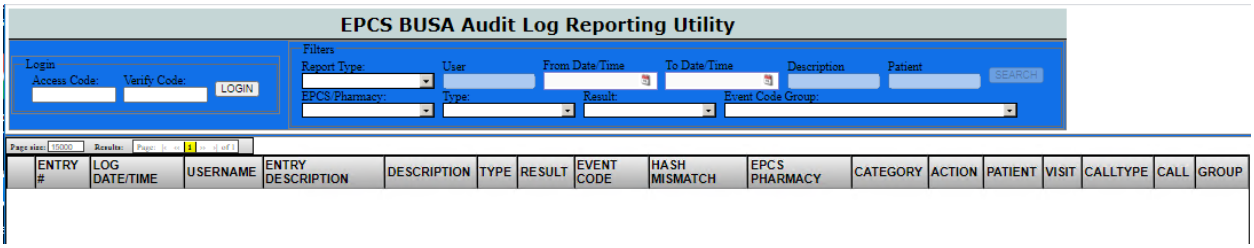

Figure 4-16: Initial EPCS BUSA audit report display (prior to login)

2. Enter the **RPMS Access Code** and verify code to login.

3. Click **Login**.

Users who are assigned the BUSAZRPT security key and are set up as report users during the BUSA installation process will gain access to the filtering properties on the right side of the page as shown in Figure 4-17.

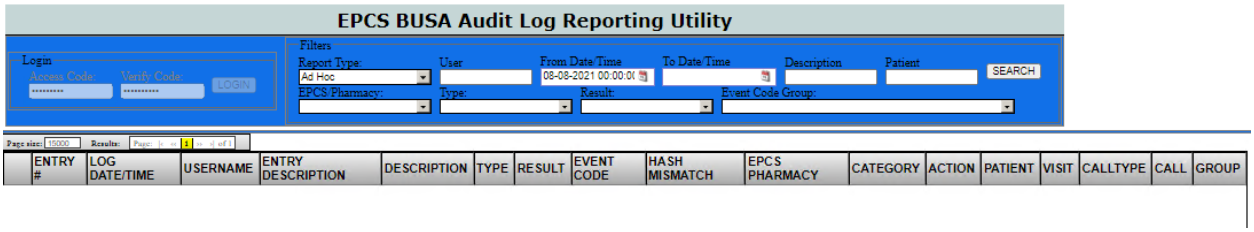

Figure 4-17: Authorized BUSA users with successful EPCS BUSA Report Utility log in

4.3.2 Conduct EPCS Filter Searches

Users can select multiple report types and as many filter options as needed to produce customized reports.

When doing a search, if the number of records returned is still large, consider using additional filters. The number of results indicates the number of records found.

4.3.2.1 Choosing EPCS Report Type

The EPCS BUSA Report Utility allows users to view data in the following two formats (as shown in Figure 4-18):

- **Ad Hoc**
- **List**

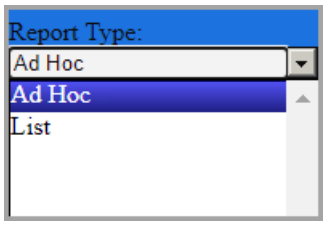

Figure 4-18: EPCS BUSA Report Utility

To switch between the two formats, in the Filters section, select **Ad Hoc** or **List** from the **Report Type** field. After changing the display format, the search must be executed again to update the display.

4.3.2.2 Ad Hoc Report Display Format

The Ad Hoc Report display format shows BUSA information in the same format as the original BUSA report utility. The **Entry Description** field frequently contains multiple pieces of information per record, with each piece delimited by a vertical bar (|) character. Figure 4-19 shows a sample Ad Hoc report.

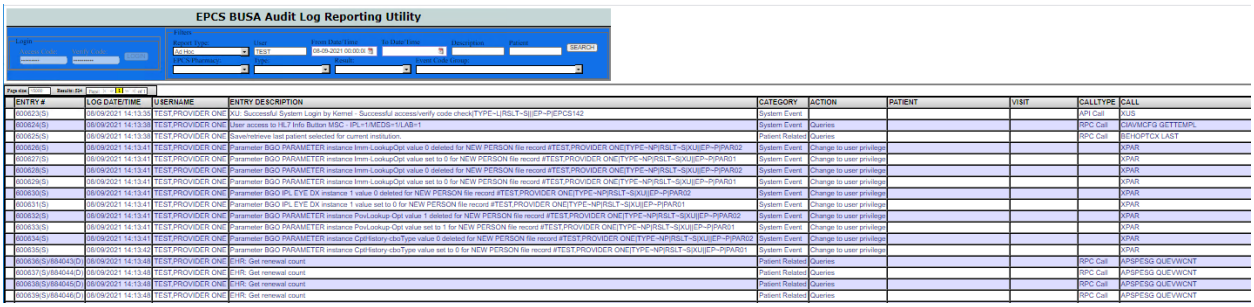

Figure 4-19: Sample Ad Hoc report format

4.3.2.3 List Report Display Format

The List report-type display format shows BUSA information in a format that separates the delimited Entry Description field information into separate pieces so it can be exported as separate data values. Figure 4-20 shows a sample List Report.

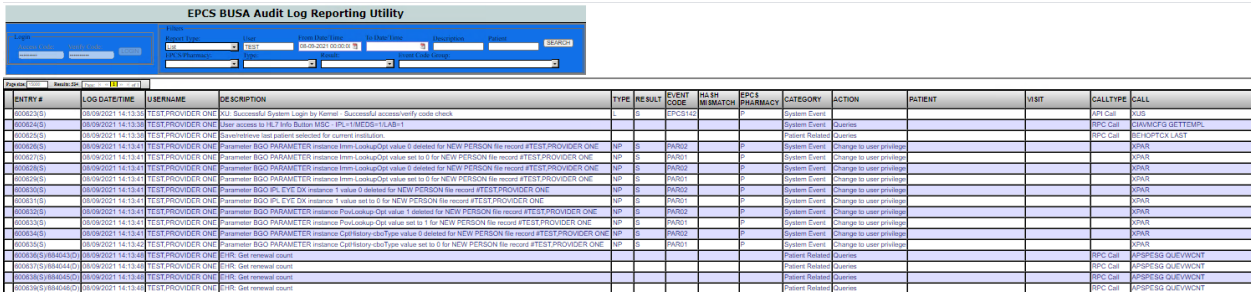

Figure 4-20: Sample List Report Format

4.3.3 Applying Filters and Performing Searches

Along with the filtering options described in Section 4.1.2, the EPCS Report Type contains several additional filters. Users can select as many of these additional filter options as needed. After selecting or modifying any report filters, click the **SEARCH** button to recompile the report.

4.3.3.1 EPCS/Pharmacy

This filter is based on the value of the List report **EPCS Pharmacy** column values (E, P, or EP). The options available for selection for this filter are as follows:

- **Both E/P**: Returns only BUSA entries with an EPCS Pharmacy value of **EP**.
- **Either E/P**: Returns BUSA entries with an EPCS Pharmacy value of **E**, **P**, or **EP**.
- **EPCS**: Returns BUSA entries with an EPCS Pharmacy value of **E** or **EP**.
- **Pharmacy**: Returns BUSA entries with an EPCS Pharmacy value of **P** or **EP**.

4.3.3.2 Type

This filter is based on the value of the List report **Type** column values. The options available for selection for this filter are as follows:

- **Credentials**: Type column value **C**
- **General**: Type column value **G**
- **Keys**: Type column value **K**
- **Login**: Type column value **L**
- **Menus**: Type column value **M**
- **Options**: Type column value **O**
- **Pharmacy**: Type column value **P**

- **Provider Profile:** Type column value **PP**
- **Rx**: Type column value **X**
- **Services**: Type column value **S**

4.3.3.3 Result

This filter is based on the value of the List report **Result** column values. The options available for selection for this filter are:

- **Success**: Result column value **S**
- **Failure**: Result column value **F**

4.3.3.4 Event Code Group

The List report Event Code column contains a number of event codes. This filter combines these event codes into related groupings. Each selection listed below contains event codes in the specified range.

- Integrity Checks (Tampering): EPCS event code range 100–119
- Logical Access Control – Access Pharmacy Menus: EPCS event code range 154–155
- Logical Access Control – Credentialing: EPCS event code range 120–127
- Logical Access Control – Logins: EPCS event code range 140–149
- Logical Access Control – Pharmacy Keys: EPCS event code range 130–139
- Logical Access Control – Pharmacy Menus: EPCS event code range 150–153
- Logical Access Control – Writing Med Orders: EPCS event code range 128–129
- Miscellaneous: EPCS event code range 156–169
- Multi-Factor Authenticate: EPCS event code range 50–59
- Ordering/Pharmacy Processing: EPCS event code range 60–99
- Provider Profile: EPCS event code range 30–49
- Time Synchronization: EPCS event code range 0–9

4.3.4 Sorting Results

As with the original BUSA report utility, search results in the EPCS BUSA report utility can be sorted. After obtaining results, users can click any of the column headers to sort the results in an ascending order. Click the column header a second time to sort the display in descending order. See Figure 4-21 for a report example, sorted in ascending order by the **Entry #** column.

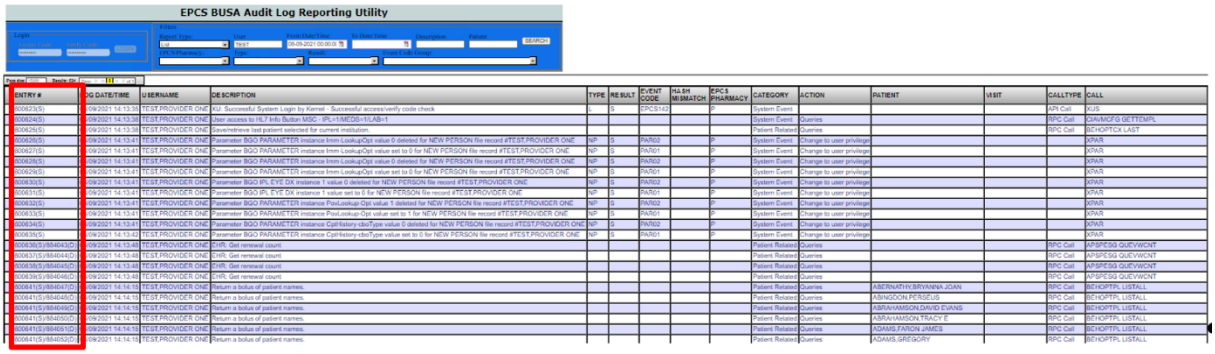

Figure 4-21: EPCS BUSA List report sorted by ENTRY # (ascending order)

5.0 Remediation Utility

The BUSA Version 1.0 Patch 4 release contains a remediation utility that allows sites to filter out some flagged entries on the EPCS Incident Reports or BUSA Zen Reports once the flagged entries have been reviewed and addressed. For example, Figure 5-1 shows a sample EPCS Incident Report error listing. A number of these entries can be remediated so that they will not continue to show up on the reports every day.

> **Note**: The remediation process only filters events out of various reports. The underlying log entries are still contained in the BUSA database.

```
      THRESHOLD SUMMARY
================================================
Please initiate appropriate incident response to look into identified issues.

*** Large percentage of pharmacists added. This could indicate an attempt to
***  tamper with system.
*** Issue found in BUSA integrity check process, possible system problem.
***     Number of records is incorrect in BUSA integrity check process
*** Integrity Check Count:      99015 Caclulated count:     136529
***     Missing 6 BUSAS IENs:
***          599400
***          599401
***          599402
***          599403
***          599404
***          599405
***     HASH Mismatch found in 1 BUSAS IEN:
***          560310  on: 11/12/2010
*** Issue found in EPCS Monitoring Hash Check process, possible system problem.
***     Hash Check failed on 8/5/2021 2:00:07 am for: 25-OZ,JESSICA
***     Hash Check failed on 8/5/2021 8:00:06 am for: 25-OZ,JESSICA
***     Hash Check failed on 8/5/2021 8:09:41 am for: 25-OZ,JESSICA
*** Issue found in CS Order Integrity Compile process, possible system problem.
***     Missing IEN identified:
***          ORPA(101.52) is missing entry for IEN: 1417
***          ORPA(101.52) is missing entry for IEN: 1422
***          ORPA(101.52) is missing entry for IEN: 1438
***          ORPA(101.52) is missing entry for IEN: 1444
***          ORPA(101.52) is missing entry for IEN: 1445
***          ORPA(101.52) is missing entry for IEN: 1446
***          ORPA(101.52) is missing entry for IEN: 1458
***          ORPA(101.52) is missing entry for IEN: 1459
***          ORPA(101.52) is missing entry for IEN: 1460
***          ORPA(101.52) is missing entry for IEN: 1464
***          ORPA(101.52) is missing entry for IEN: 1465
***          ORPA(101.52) is missing entry for IEN: 1466
***          ORPA(101.52) is missing entry for IEN: 1635
***          ORPA(101.52) is missing entry for IEN: 1638
***          ORPA(101.52) is missing entry for IEN: 1647
***          ORPA(101.52) is missing entry for IEN: 1650

================================================
Please initiate appropriate incident response to look into identified issues.

*** Missing IENs identified in ^BUSAS log files. This could indicate an attempt
```

```
***  to compromise audit logging, please investigate.
         Total IENs for reporting period:        524
       Missing IENs for reporting period:          6

       Last Missing IEN: 599405  Date Before missing IEN: 3210805.07471
```

Figure 5-1: Sample EPCS Incident Report Error Listing

Figure 5-2 shows a BUSA Zen report that contains entries with HASH Mismatch errors that can be addressed with the new remediation utility.

ENTRY #	LOG DATE/TIME	USERNAME	DESCRIPTION	TYPE	RESULT	EVENT CODE	HASH MISMATCH	EPCS PHARMACY	CATEGORY	ACTION	PATIENT
600068(S)/883926(D)	08/06/2021 13:18:31	TEST,PROVIDER ONE	Return a bolus of patient names.						Patient Related	Queries	TEST,PATIENT TWO
600068(S)/883930(D)	08/06/2021 13:18:31	TEST,PROVIDER ONE	Return a bolus of patient names.				Yes (883930(D))		Patient Related	Queries	TEST,PATIENT TWO
600069(S)/883971(D)	08/06/2021 13:18:31	TEST,PROVIDER ONE	Selects patient & returns key information.						Patient Related	Queries	TEST,PATIENT TWO
600070(S)/883972(D)	08/06/2021 13:18:41	TEST,PROVIDER ONE	Selects patient & returns key information.						Patient Related	Queries	TEST,PATIENT REG
600071(S)/883973(D)	08/06/2021 13:18:43	TEST,PROVIDER ONE	Selects patient & returns key information.				Yes (883973(D))		Patient Related	Queries	TEST,PATIENT TWO
600072(S)/883974(D)	08/06/2021 13:18:44	TEST,PROVIDER ONE	Check for possible duplicates.				Yes (883974(D))		Patient Related	Queries	TEST,PATIENT TWO
600073(S)/883975(D)	08/06/2021 13:18:44	TEST,PROVIDER ONE	Return message if data on the legacy system.						Patient Related	Queries	TEST,PATIENT REG

Figure 5-2: Sample BUSA Zen Report showing HASH Mismatch errors

Note: The EPCS Incident Report compile that runs every night only compiles data from the previous two years. If errors have been appearing on the report for over 2 years, then to clean them out, the following commands should be run from the programmer's prompt to clean out the old, compiled data and re-compile it. This process could take some time to run.

>K ^XTMP("BEHOEPIC")

>D COMP^BEHOEPIC

Running the above command will clear out old, compiled data that no longer is needed for reporting. If the EPCS Incident Report still contains errors after the cleanup and recompile has run, then the steps below can be run to remediate the errors.

To remediate entries on the report, two users are required. One user will enter the remediated record information and save it and the second user will verify the remediated record. Records cannot be verified by the same user that last modified the record. Remediated records can be updated multiple times prior to being verified. The remediation on a record will not go into effect until it has been verified. Once a record has been verified, it can be modified. Any changes, however, will not go into effect until they have again been verified. Until that verification occurs, any previously verified version of the record will remain in effect. Remediated records can also be deleted. If an existing remediated record is marked as deleted, the deletion will not go into effect until that entry has been verified.

The following instructions describe how to filter out some entries on the EPCS Incident Reports using the new remediation utility.

> **Note:** The EPCS Incident Reports that are run are based off the previous day's compiled data. Therefore, any remediation record that gets entered and verified may take up to two days to filter information from the reports as the next day's report that is automatically mailed out will be based on the current day's compiled data (which was most likely compiled prior to the remediation record entry). Filtered data will appear in the following day's report that gets automatically sent. For remediation entries defined to address HASH Mismatch errors showing up on the BUSA Zen reports, any remediation performed will immediately be reflected in the Zen reports as soon as it has been verified.

5.1 Process for creating a new remediation entry

The following instructions describe how to create a new remediation entry so that a specified error or errors will no longer appear on the EPCS incident reports or in the BUSA Zen reports. The instructions below focus on addressing one specific error, Missing BUSA IENSs, that appear on the EPCS incident reports. The remediation utility, however, can be used to address a number of different errors. Furthermore, it has the capability of being customized in the future to address errors on other reports that are designed to utilize the utility.

5.1.1 Identify Missing BUSAS IEN Errors on the EPCS Incident Report

The EPCS Incident Report will often display errors as shown in Figure 5-3. Make a note of any of the IENs listed that should be filtered from the daily reports.

```
***     Missing 6 BUSAS IENs:
***          599400
***          599401
***          599402
***          599403
***          599404
***          599405
```

Figure 5-3: EPCS Incident Report showing Missing BUSAS IEN errors

5.1.2 Log into the BUSA Remediation Utility

The Remediation utility delivered with BUSA Patch 4 can be accessed at the following address:

http://*ip address:port/csp/namespace/BUSA.RemediationLogin.cls*

Sites should replace the IP address with the address of the RPMS server, the port with the proper port number, and the namespace with either the namespace of the RPMS live database or with BUSA. The value of namespace is determined by how the site chose to set up the CSP application for the BUSA version 1.0 release. See version 1.0 release of the *IHS User Security Audit (BUSA) Installation Guide and Release Notes* for further details on determining these values.

> **Note:** The report utility displays best in Firefox or Chrome. Internet Explorer has an issue with displaying row heights too large.

1. Paste the following address in a Windows browser (preferably Firefox or Chrome), replacing the *ip address, port,* and *namespace*, as described above.

   http://*ip address*:*port*/csp/*namespace*/BUSA.RemediationLogin.cls

   The BUSA Remediation Utility Login page should display. Figure 5-4 shows the initial display.

Figure 5-4: BUSA Remediation Utility Login Screen

2. Enter the RPMS **Access Code** and **Verify Code** to log in.
3. Click **Login**.

Users who are assigned the BUSAZREMEDIATION security key and are set up as remediation utility users during the BUSA Version 1.0 Patch 4 installation will then be transferred to the BUSA Remediation Utility screen as shown in Figure 5-5. Depending on whether an AGMP cleanup process was run during the Patch 4 installation, there may already be an entry present. That entry should not be modified.

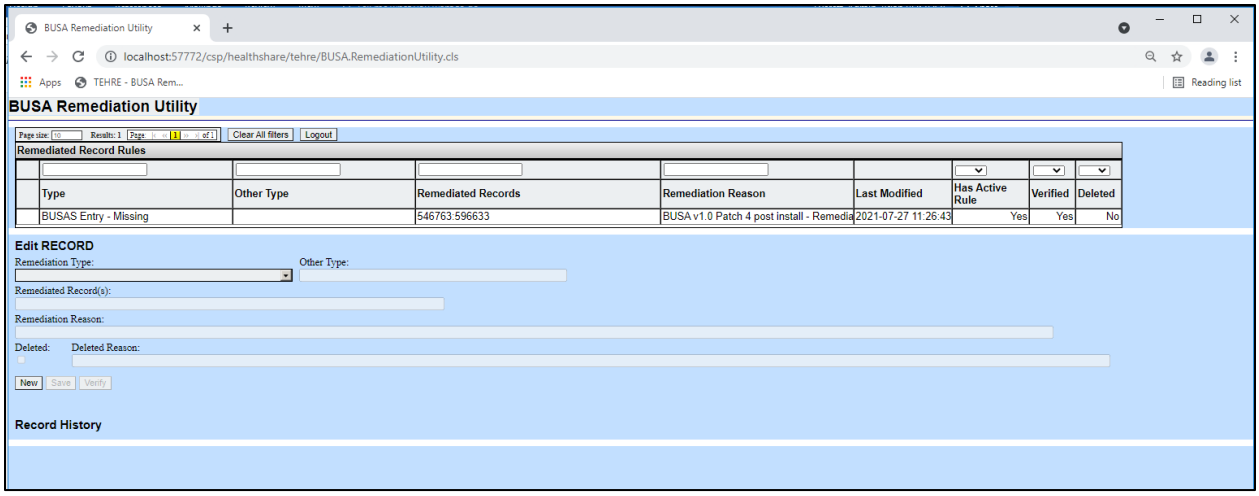

Figure 5-5: Remediation Utility Edit Screen

5.1.3 Create a new Remediation Utility Entry

1. Click on the **New** button as shown in Figure 5-6.

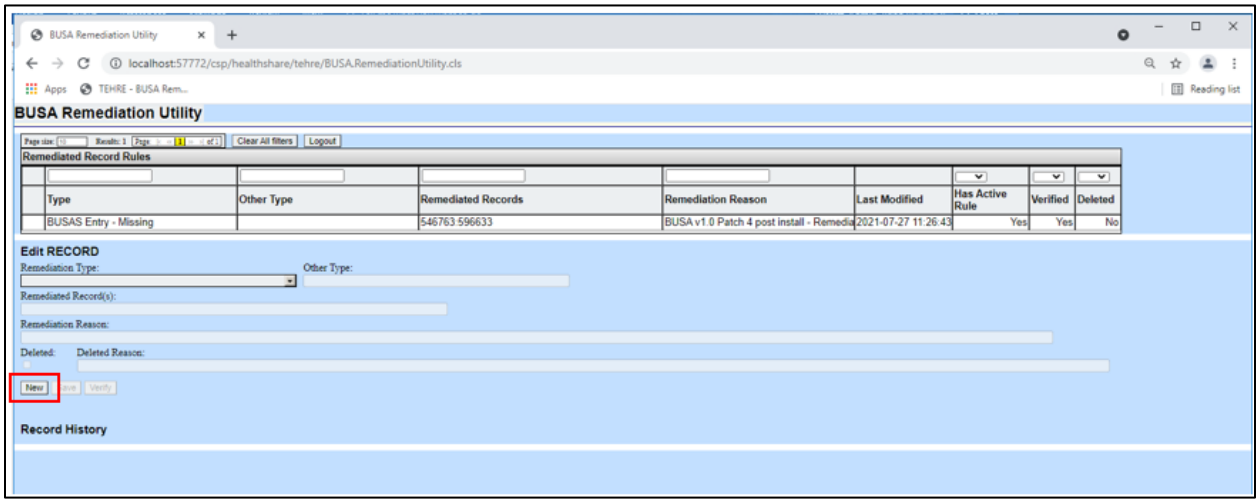

Figure 5-6: Creating a new Remediation Entry

2. In the **Edit RECORD** section, select **BUSAS Entry – Missing** from the Remediation Type drop-down list.

3. In the **Remediation Record(s)** field, enter the records to be remediated. Multiple records or ranges can be entered with each record separated by a comma. A space can be entered (but is not required) after each comma which will allow longer lists of records to display better in the utility. Ranges can be entered by entering a start date:end date. For example, entering 1, 3:5, 6, 9 into the Remediation Record(s) field will remediate entries 1, 3, 4, 5, 6 and 9.

4. Enter a reason why the records are being remediated.

5. Once all the information has been entered, click the **Save** button as highlighted in Figure 5-7.

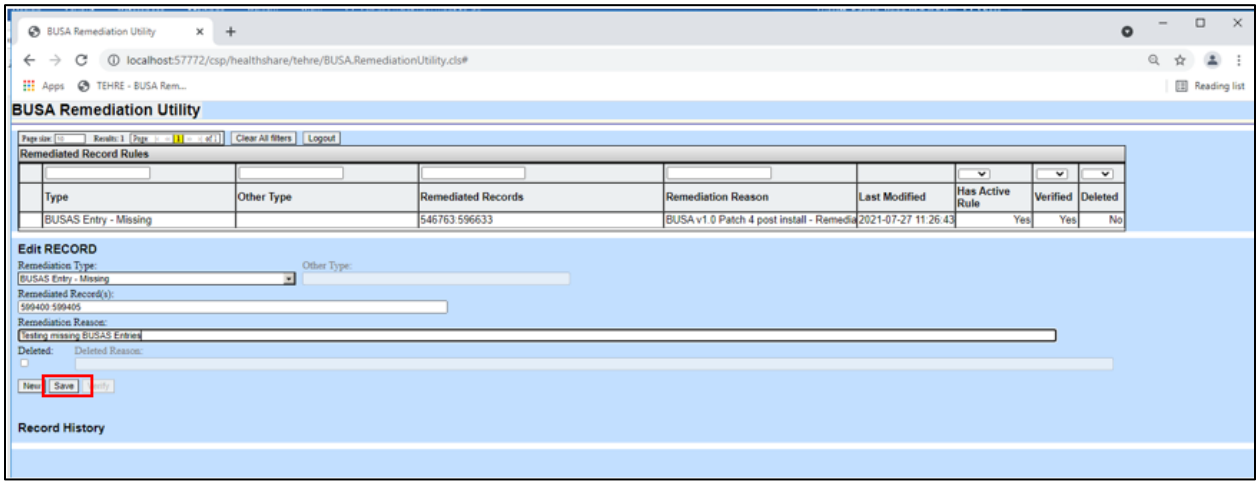

Figure 5-7: Remediation Utility Save Record Button

6. After clicking **Save**, a success message shown in Figure 5-8 should display.

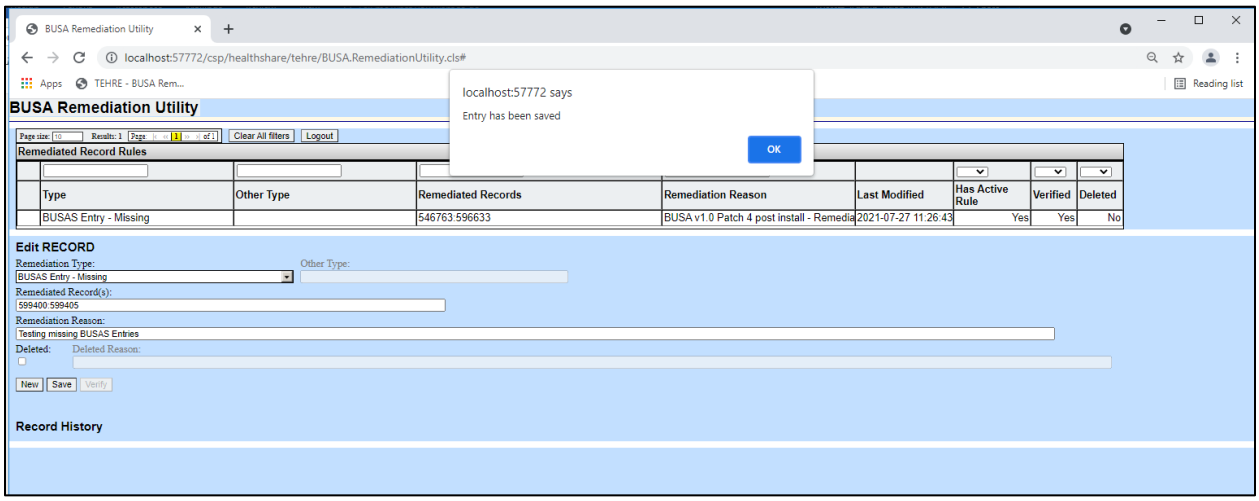

Figure 5-8: Successful record save message

7. Upon saving the record, the new remediation rule should be added to the list of rules as shown in Figure 5-9.

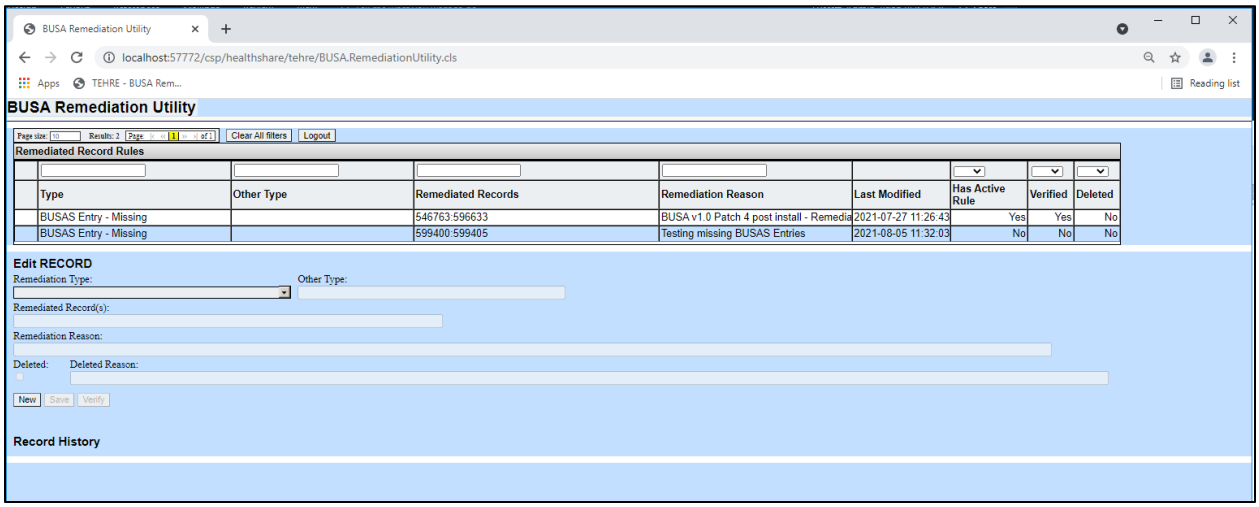

Figure 5-9: Updated remediation record in table

8. Clicking on the new rule will display the remediated record along with its history. The record will show as being created but the verify information will be blank. The **Active Rule** column will display as **No** signifying that the remediation for that entry is not in effect. Figure 5-10 shows the detailed display of the remediated record entry.

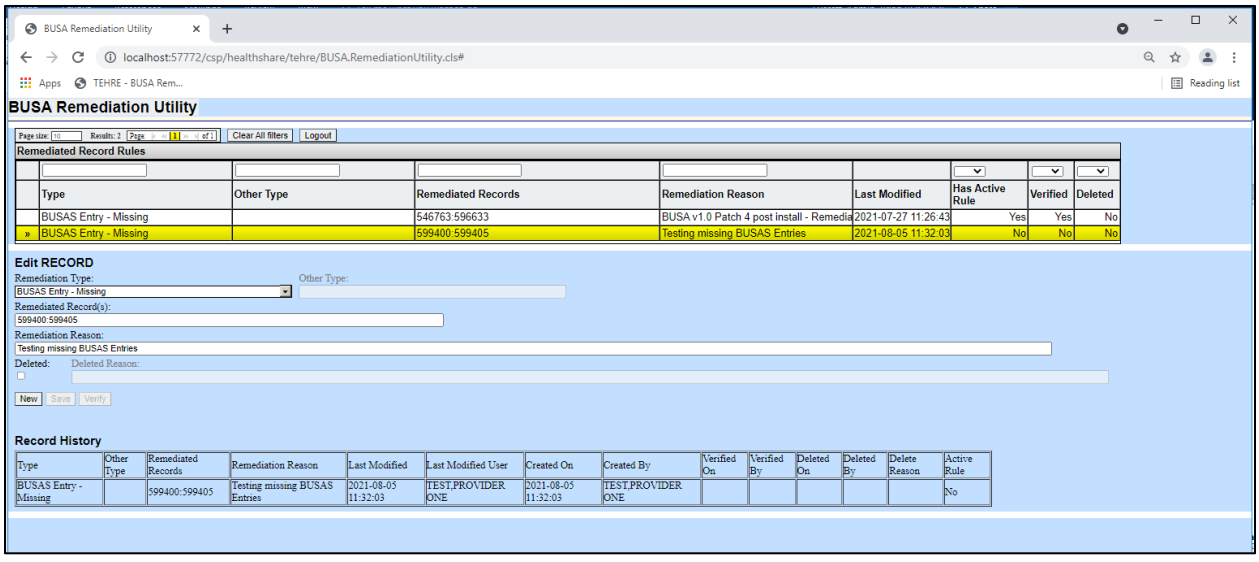

Figure 5-10: Detailed display of the remediated record entry

5.1.4 Verify the new Remediation Utility Entry

1. A user other than the last user to modify the remediation record entry should log into the remediation utility as described in Section 5.1.2.

2. Selecting the newly created remediation entry will cause the record information to be displayed and the Verify button to be enabled as shown in Figure 5-11. If the user makes any changes to the existing record at this point the Verify button will be disabled. They can save their changes, but another user will then have to verify them.

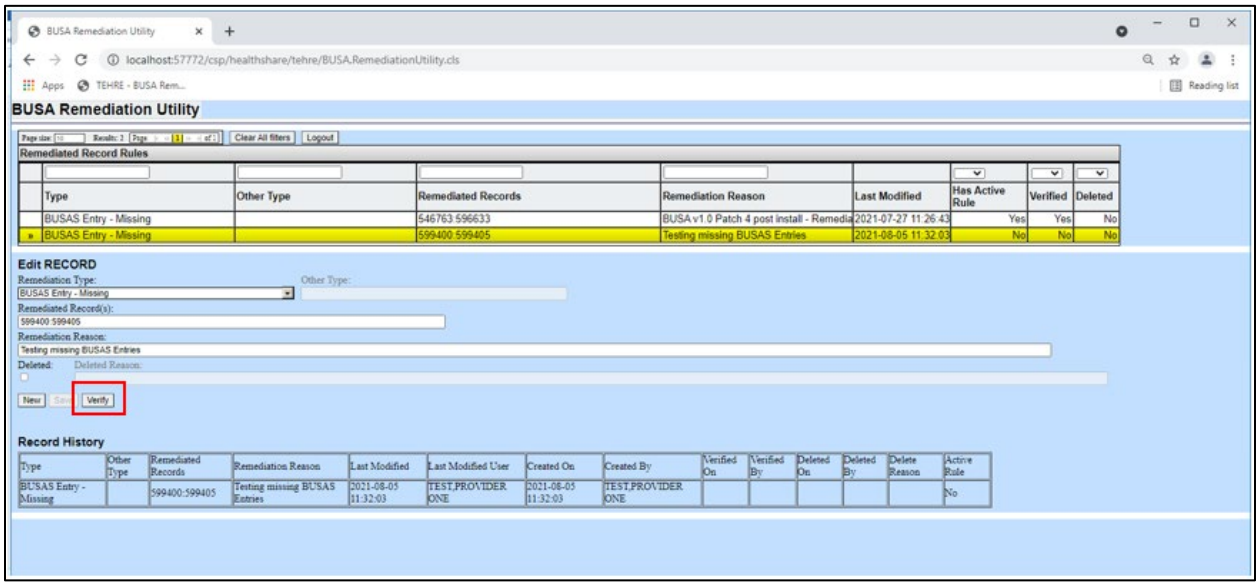

Figure 5-11: Verify record display dialog

3. Clicking the **Verify** button will cause the confirmation message shown in Figure 5-12 to display.

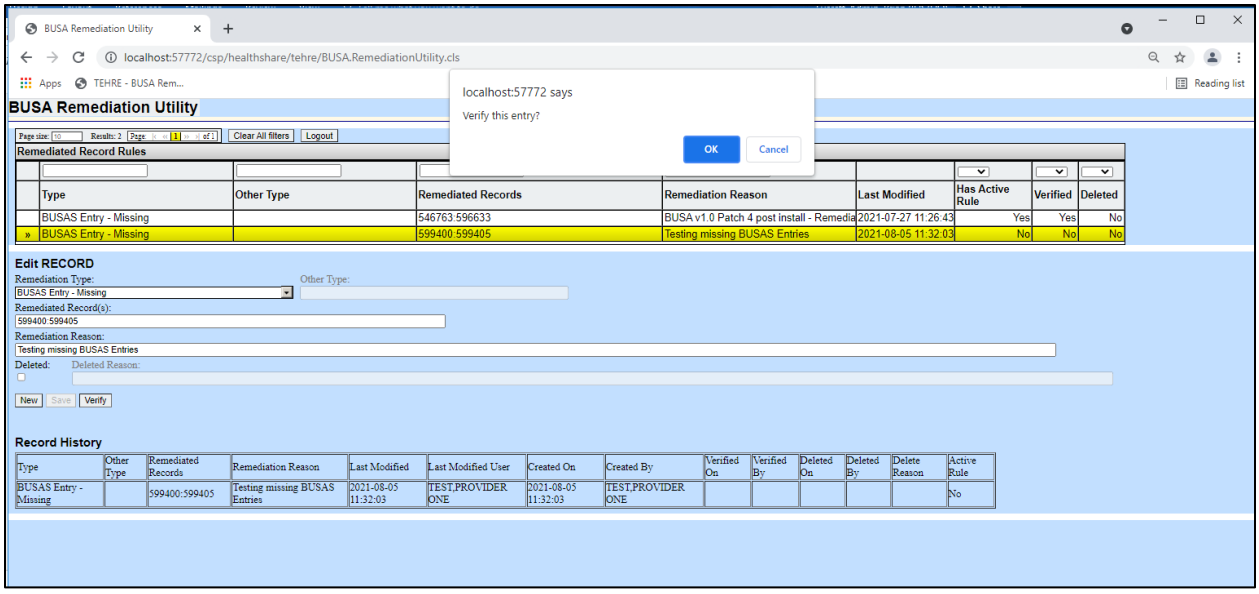

Figure 5-12: Verify confirmation message

4. Clicking **OK** will then result in a message saying that the record has been successfully verified as shown in Figure 5-13.

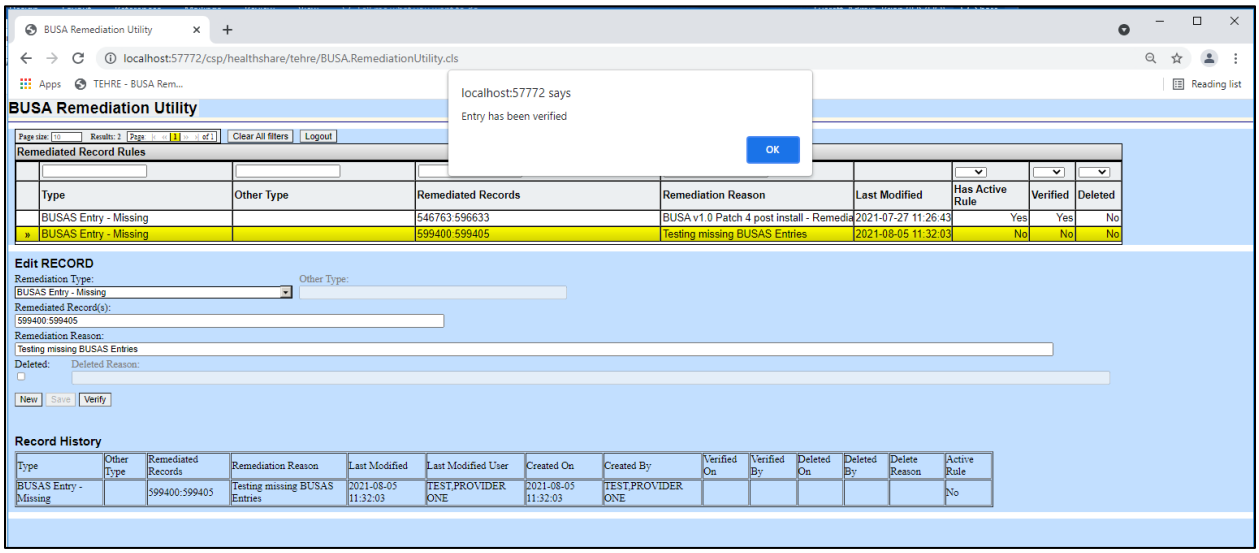

Figure 5-13: Successful verification message

5. Selecting the updated record (now showing as being Verified with an Active Rule) will display the record and its history as shown in Figure 5-14.

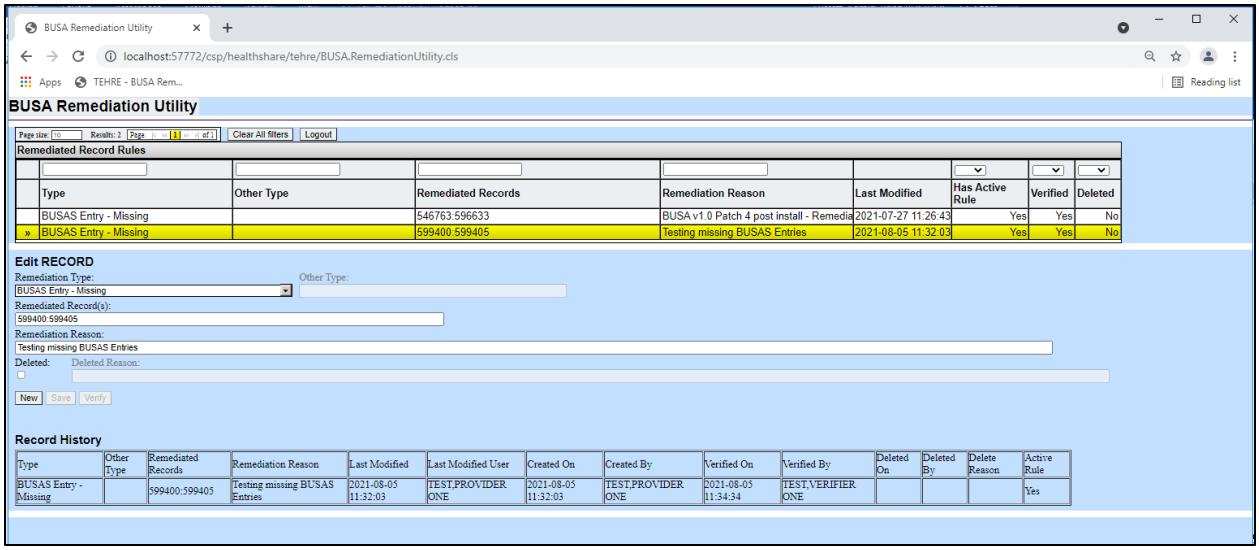

Figure 5-14: Verified record detailed display

6. As mentioned in the summary for Section 5.0, the EPCS Incident Report will not immediately filter out the errors. Because the next day's report uses data that has already been compiled, it will still contain the filtered-out errors. The following day's report however should properly filter them out. If you would like to immediately view the report with the information filtered out perform the following steps. Note that the first step does a great deal of data processing and should only be attempted when there is not a heavy load on the system.

   a. At the programmer's prompt enter the following:

      >D TASK^BEHOEPIC

   b. Run the 'BEHO EPCS AUDIT LOG SUMMARY' option in RPMS and use a Report Date of 'TODAY'.

```
Select OPTION NAME: BEHO EPCS AUDIT LOG SUMMARY       EPCS Audit Log
Summary
EPCS Audit Log Summary
Report is available in Roll and scroll only!
The report can be exported to the HFS host system or mailed from MailMan.
A site has the ability to assign a user (i.e. security officer) to access
the report.
Report DATE: T  (AUG 06, 2021)
DEVICE:
```

Figure 5-15: Running the BEHO EPCS AUDIT LOG SUMMARY option in RPMS

   c. Whether you choose to wait for two days for the correct information to appear or if you run the above steps to immediately filter it out, the resulting report should no longer contain the missing BUSA IEN errors. See Figure 5-16 for the updated EPCS Incident Report.

```
      THRESHOLD SUMMARY
================================================
Please initiate appropriate incident response to look into identified issues.

*** Large percentage of pharmacists added. This could indicate an attempt to
***  tamper with system.
*** Issue found in BUSA integrity check process, possible system problem.
***     Number of records is incorrect in BUSA integrity check process
*** Integrity Check Count:      99049 Caclulated count:     136563
***     HASH Mismatch found in 1 BUSAS IEN:
***          560310  on: 11/12/2010
*** Issue found in EPCS Monitoring Hash Check process, possible system problem.
***     Hash Check failed on 8/5/2021 2:00:07 am for: 25-OZ,JESSICA
***     Hash Check failed on 8/5/2021 8:00:06 am for: 25-OZ,JESSICA
***     Hash Check failed on 8/5/2021 8:09:41 am for: 25-OZ,JESSICA
***     Hash Check failed on 8/5/2021 11:35:58 am for: 25-OZ,JESSICA
*** Issue found in CS Order Integrity Compile process, possible system problem.
***     Missing IEN identified:
***          ORPA(101.52) is missing entry for IEN: 1417
***          ORPA(101.52) is missing entry for IEN: 1422
***          ORPA(101.52) is missing entry for IEN: 1438
***          ORPA(101.52) is missing entry for IEN: 1444
***          ORPA(101.52) is missing entry for IEN: 1445
***          ORPA(101.52) is missing entry for IEN: 1446
***          ORPA(101.52) is missing entry for IEN: 1458
***          ORPA(101.52) is missing entry for IEN: 1459
***          ORPA(101.52) is missing entry for IEN: 1460
***          ORPA(101.52) is missing entry for IEN: 1464
***          ORPA(101.52) is missing entry for IEN: 1465
***          ORPA(101.52) is missing entry for IEN: 1466
***          ORPA(101.52) is missing entry for IEN: 1635
***          ORPA(101.52) is missing entry for IEN: 1638
***          ORPA(101.52) is missing entry for IEN: 1647
***          ORPA(101.52) is missing entry for IEN: 1650

================================================
Please initiate appropriate incident response to look into identified issues.
```

Figure 5-16: Updated EPCS Incident Report

5.2 Process for editing an existing remediation entry

Once a remediation entry has been created and verified, it becomes active. It is possible however, to modify a record once it has been verified. The following instructions describe how to edit an existing remediation entry. The instructions below focus on addressing one error, Missing ORPA(101.52) Record, that frequently appears on the EPCS incident reports, but can be applied to any existing remediated entry.

5.2.1 Identify additional Missing ORPA(101.52) IEN Errors on the EPCS Incident Report

The sample EPCS Incident Report, shown in Figure 5-17 contains a number of errors relating to missing ORPA(101.52) records. Make a note of any of the IENs listed that should be filtered from the daily reports.

```
      THRESHOLD SUMMARY
================================================
Please initiate appropriate incident response to look into identified issues.

*** Large percentage of pharmacists added. This could indicate an attempt to
***  tamper with system.
*** Issue found in BUSA integrity check process, possible system problem.
***     Number of records is incorrect in BUSA integrity check process
*** Integrity Check Count:      99078 Caclulated count:     136592
***     HASH Mismatch found in 1 BUSAS IEN:
***          560310  on: 11/12/2010
*** Issue found in EPCS Monitoring Hash Check process, possible system problem.
***     Hash Check failed on 8/5/2021 2:00:07 am for: 25-OZ,JESSICA
***     Hash Check failed on 8/5/2021 8:00:06 am for: 25-OZ,JESSICA
***     Hash Check failed on 8/5/2021 8:09:41 am for: 25-OZ,JESSICA
***     Hash Check failed on 8/5/2021 11:35:58 am for: 25-OZ,JESSICA
***     Hash Check failed on 8/5/2021 12:02:25 pm for: 25-OZ,JESSICA
*** Issue found in CS Order Integrity Compile process, possible system problem.
***     Missing IEN identified:
***          ORPA(101.52) is missing entry for IEN: 1458
***          ORPA(101.52) is missing entry for IEN: 1459
***          ORPA(101.52) is missing entry for IEN: 1460
***          ORPA(101.52) is missing entry for IEN: 1464
***          ORPA(101.52) is missing entry for IEN: 1465
***          ORPA(101.52) is missing entry for IEN: 1466
***          ORPA(101.52) is missing entry for IEN: 1635
***          ORPA(101.52) is missing entry for IEN: 1638
***          ORPA(101.52) is missing entry for IEN: 1647
***          ORPA(101.52) is missing entry for IEN: 1650

================================================
Please initiate appropriate incident response to look into identified issue
```

Figure 5-17: EPCS Incident Report showing Missing ORPA(101.52) errors

5.2.2 Locate the existing remediated entry for that error type

Log into the remediation utility as described in Section 5.1.2. Locate the existing remediation entry for the ORPA(101.52) Entry – Missing error type. See Figure 5-18 for the specified entry.

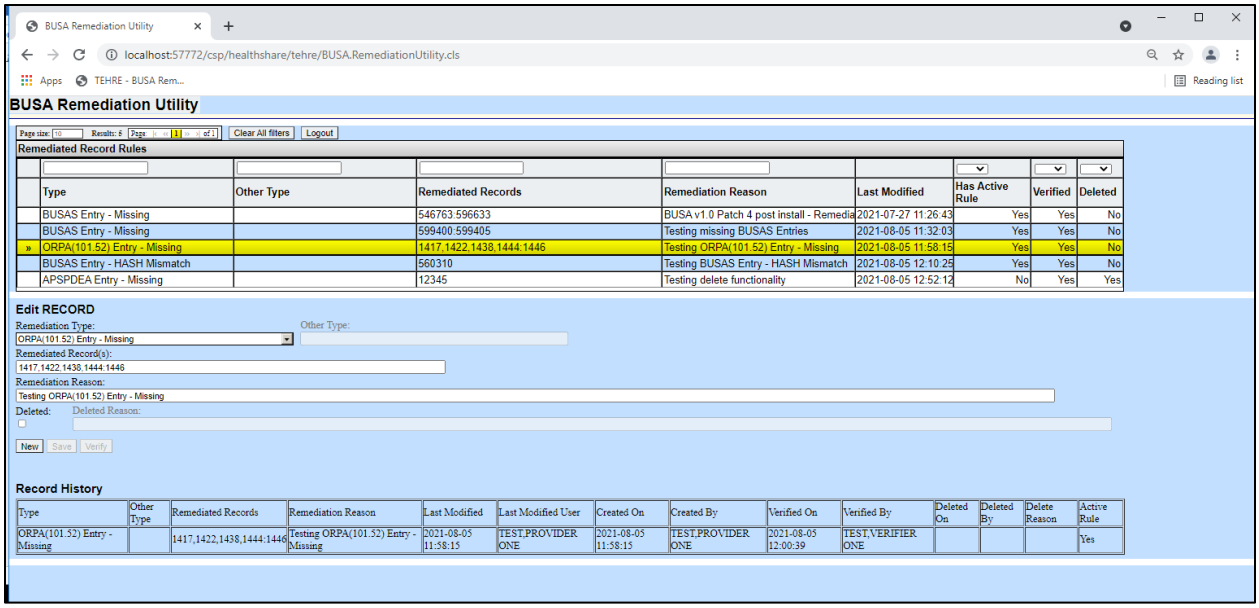

Figure 5-18: Remediation utility highlighting the existing 'ORPA(101.52) Entry – Missing' error type

5.2.3 Edit the existing entry to include the additional error IEN values

1. Update the entry to include the additional IENs that are appearing on the EPCS Incident Report and click to save as shown in Figure 5-19.

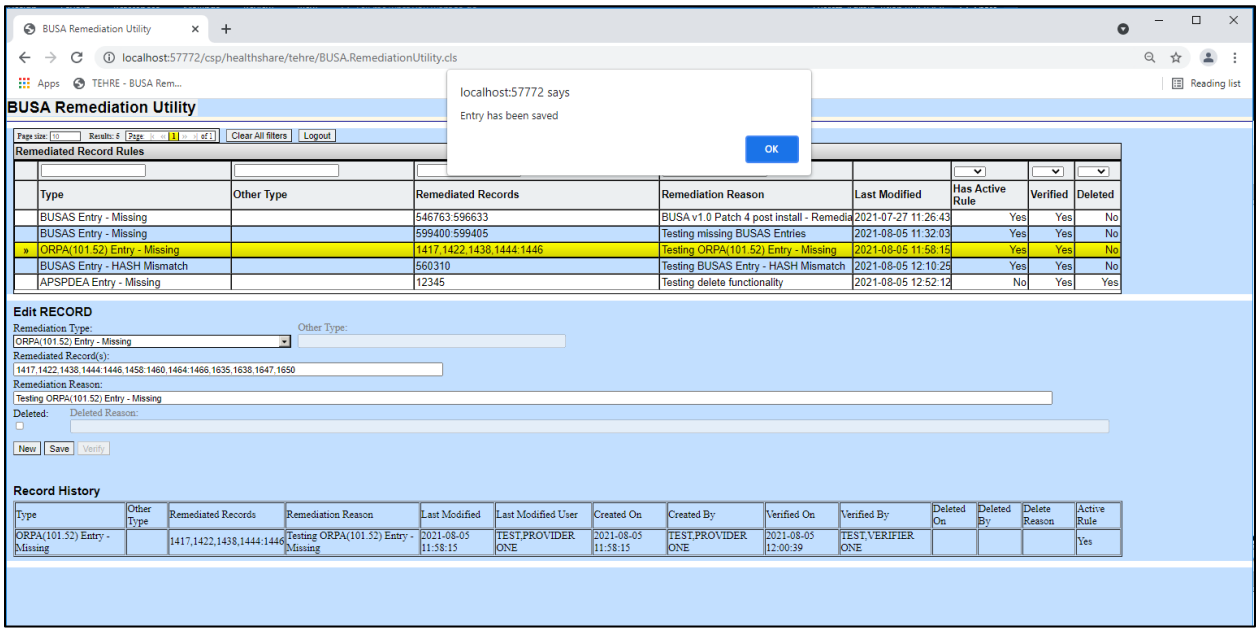

Figure 5-19: Updated ORPA(101.52) remediated entry

2. Review the updated entry as shown in Figure 5-20. Note that the entry now shows as having an active rule, but that it is not currently verified. Reviewing the record history of the entry shows that the original version of the rule is still active. The update of the entry is still waiting to be verified and is therefore not active yet.

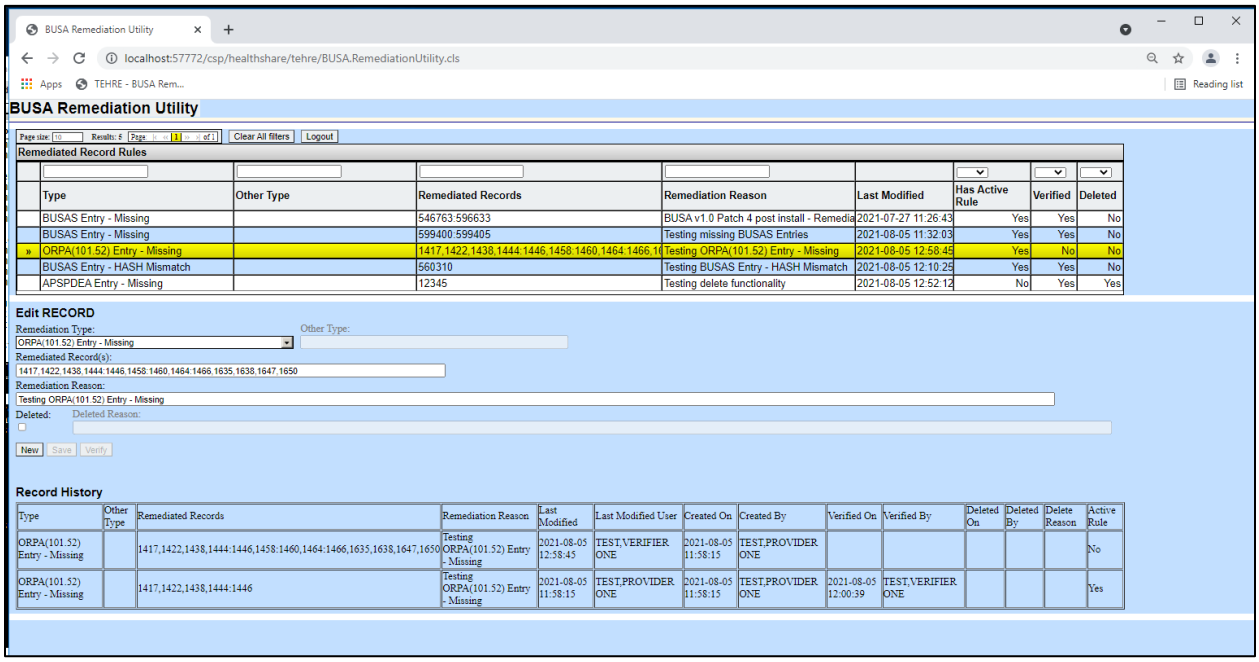

Figure 5-20: Current display of updated 'ORPA(101.52) Entry - Missing' remediated entry

5.2.4 Verify the updated entry

1. A user other than the last user to modify the remediation record entry should log into the remediation utility as described in Section 5.1.2.

2. Locate the updated entry and verify it as described in Section 5.1.4

3. Confirm that the additional remediated records do not show up on the EPCS Incident Report. Note, as discussed in Section 5.1.4 bullet point 6, that the newly remediated data will not immediately be filtered from the report.

5.3 Process for deleting an existing remediation entry

Remediated entries can be marked as deleted so that they no longer get filtered. Once an entry has been marked as deleted, it cannot be made active again. If the deletion were performed in error, a new remediation entry must be created and verified. If a remediated entry has an active rule in place and is marked as deleted, the rule in place will still be active until the entry is verified. Follow these instructions to properly delete a remediated entry.

5.3.1 Locate the remediation entry to be deleted and mark as deleted

1. Log into the remediation utility as described in Section 5.1.2. Locate the existing remediation entry that is to be deleted and select it.

2. Check the **Deleted** box in the **Edit RECORD** section and then enter a value for the **Deleted Reason** field as shown in Figure 5-21.

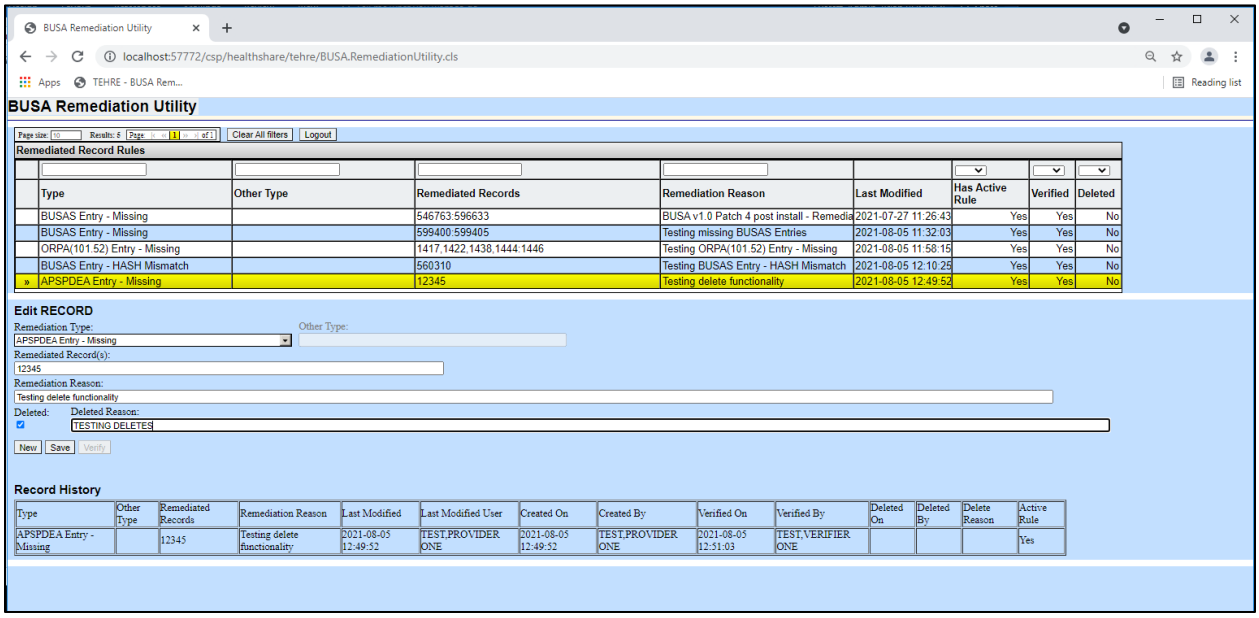

Figure 5-21: Deleting a remediation record

3. Upon clicking the **Save** button, the user will be prompted to confirm whether they wish to delete the entry or not. See Figure 5-22 for a sample confirmation message.

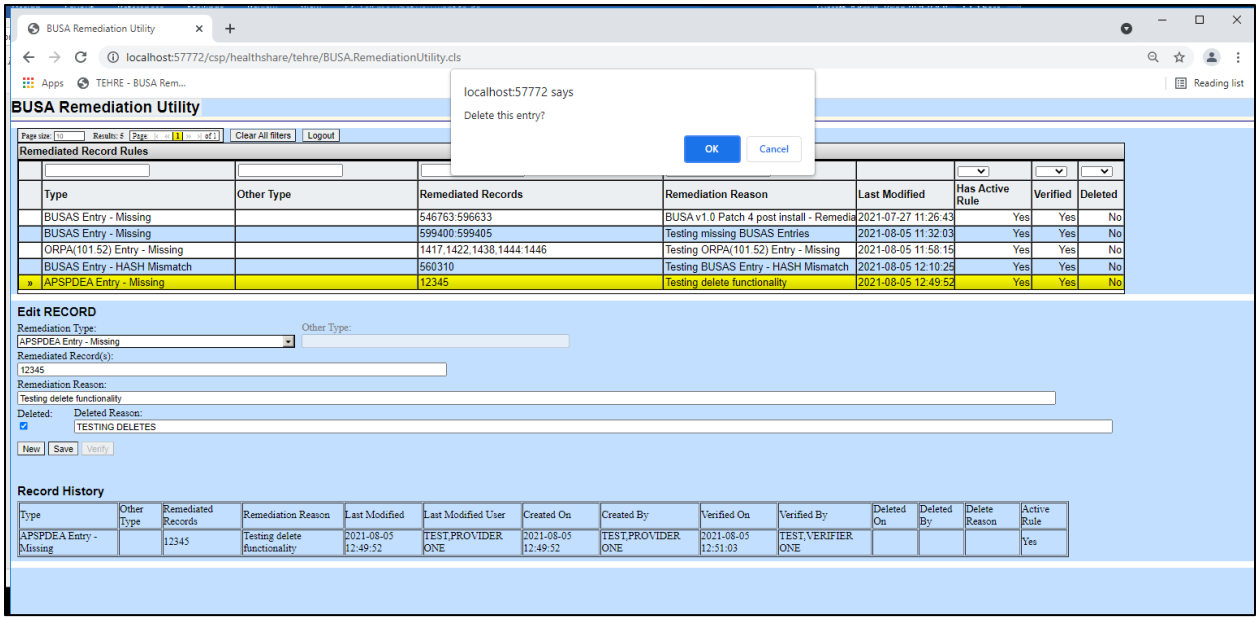

Figure 5-22: Remediation record delete confirmation

4. After clicking OK, the user will receive a message (see Figure 5-23) saying that the record has been successfully saved. At this point the record has been marked as deleted but if it has an active rule in place, that rule will still be active. The record must be verified for it to go into effect.

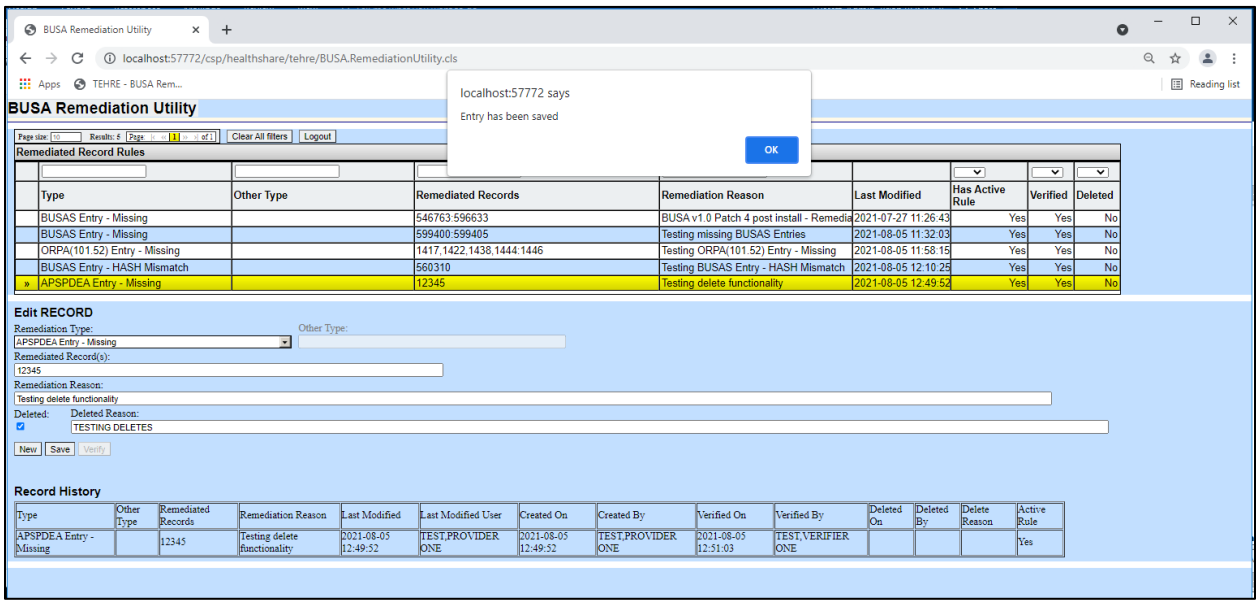

Figure 5-23: Delete remediation entry save success

5.3.2 Verify the deleted entry

1. A user other than the last user to modify the remediation record entry should log into the Remediation Utility as described in Section 5.1.2.

2. Locate the updated entry and verify it as described in Section 5.1.4

3. Review the final entry to make sure that it is marked s verified and deleted and that it does not have an active rule in place. See Figure 5-24 for a sample display of a verified deleted record.

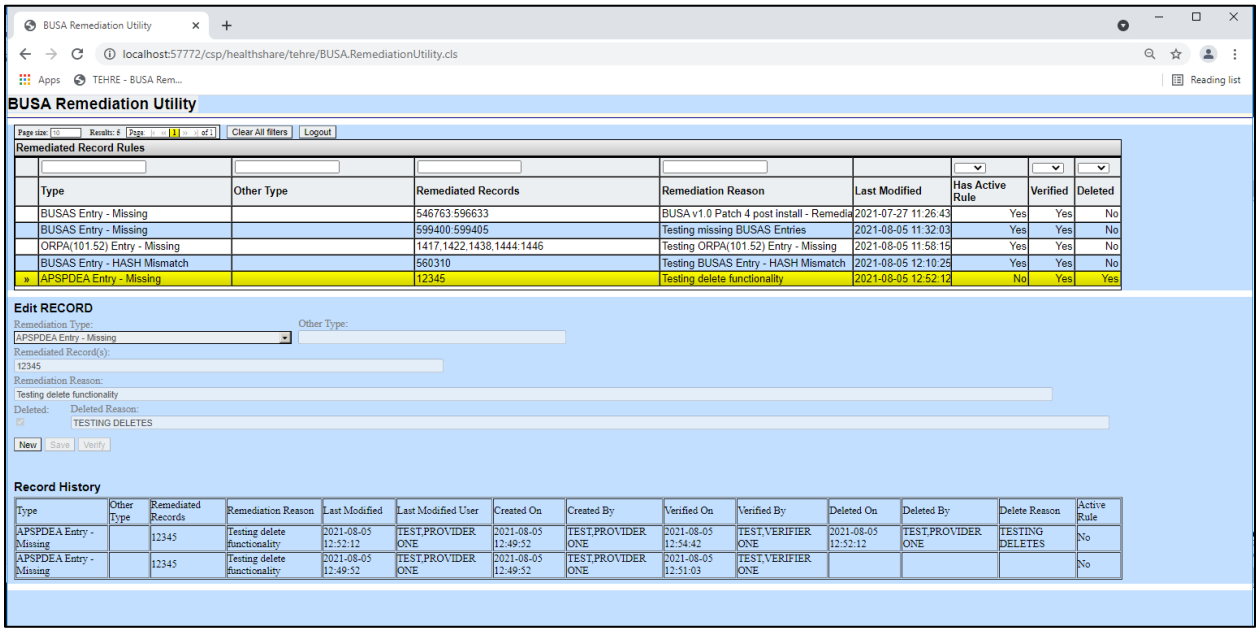

Figure 5-24: Review of the verified deleted entry

4. Confirm that the information previously filtered out of the EPCS Incident Report or BUSA Zen reports show up again as expected. Note that, as discussed in Section 5.1.4 bullet point 6, that the newly remediated data will not immediately be filtered from the report.

Appendix A EPCS Audit Event Codes

The e-prescribing of controlled substances functionality uses the BUSA audit log to act as the central audit log repository. BUSA is used as the collection and correlation point for e-prescribing of controlled substances audit reporting. A reporting interface based on the Zen reporting tool has been established to conduct reviews and ad hoc reporting for EPCS related audit events.

The standard BUSA audit record layout has been retained, with one exception. A hash field has been added to the record layout. It holds a SHA256 hash of the audit record and supports integrity checks on the audit logs. While it is a required field for EPCS related audit events, it is optional for other RPMS audit events. The field is available for use by other applications in RPMS, if desired.

To preserve the existing use of BUSA, the content of EPCS audit records are encoded into the existing **Description** field. The segments are entered as a pipe delimited string. The elements are laid out as follows:

Description|Type|Status|||Event Domain|Event Code|Additional Info

- **Description** – External/Human Friendly Description of Event.
- **Type** – The Type piece identifies the type of audit event and takes the form of TYPE~<value> with value is defined as one of the following:
  - C – Audit events related to issuing and terminating accounts.
  - L – Login Audit Events.
  - K – Audit events related to the assignment and removal of keys.
  - M – Audit events related to the assignment and removal of menus.
  - O – Audit events related to the selection of options (e.g., menus or commands).
  - P – Audit events related to pharmacy actions.
  - PP – Audit events related to managing and verifying a provider profile.
  - S – Audit events related to systems services (e.g., time synchronization or certificate checks).
  - X – Audit events related to ordering controlled substance medications.
- **Status** – The Status piece identifies the result of the action and takes the form of RSLT~<value> with value is defined as one of the following:
  - S – The action reported by the audit event was successful.
  - F – The action reported by the audit event failed.

- Event Domain – The EPCS Application piece identifies the EPCS area that the audit event is associated with and takes the form EP~<value> with value is defined as one of the following:
  - E – The action reported by the audit event is associated with the EPCS prescribing application (e.g., order a controlled substance medication).
  - P – The action reported by the audit event is associated with the EPCS pharmacy application. (e.g., dispense a controlled substance medication.)
  - EP – The action reported by the audit event is applicable to both the EPCS prescribing and EPCS pharmacy application (e.g., server time is out of synchronization).
- Event Code – The Event Code piece provides a unique identifier for the audit event. The event code takes the form of EPCS#, where the # represents a one to three-digit sequence number.
- Additional Information – This piece is used to house specific data items related to the audit event to make reporting easier.

The following are the EPCS audit events grouped by category:

A.1 Time Synchronization Audit Events

Audit events are generated by the EPCS Monitoring Service.

Table A-1: Time synchronization check success

Audit Event	Time synchronization check success
BUSA Audit Entry	Time Sync Check, <offset>
Type	S – Services
Status	S – Success
Event Domain	EP – Applicable EPCS Ordering and EPCS Pharmacy
Event Code	EPCS01
Additional Information	Time Offset in Milliseconds (ms).
Name Space	BEH
Option	N/A
MailMan Alert	Alert generated when time offset is +/- 3 minutes. Elevated alert generated when time offset is +/- 5 minutes.

Table A-2: Time synchronization check success

Audit Event	Time synchronization check failed
BUSA Audit Entry	Time Synch Check
Type	S- Services

Audit Event	Time synchronization check failed
Status	F – Failed
Event Domain	EP – Applicable EPCS Ordering and EPCS Pharmacy
Event Code	EPCS02
Additional Information	Time Offset in ms.
Name Space	BEH
Option	N/A
MailMan Alert	No

A.2 EPCS Signing Certificate Check

Multi-Factor Authentication – Cryptographic Token Events.

Audit events are generated by the BEH 2FA Service.

Table A-3: Authentication Attempt, Success (ability to conduct MFA call)

Audit Event	Authentication Attempt, Success (ability to conduct MFA call)
BUSA Audit Entry	Authentication Attempt
Type	S – Service
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS51
Additional Information	N/A
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-4: Authentication Attempt, Fail (ability to conduct MFA call)

Audit Event	Authentication Attempt, Fail (ability to conduct MFA call)
BUSA Audit Entry	Authentication Attempt
Type	S – Service
Status	F – Fail
Event Domain	E – EPCS Ordering
Event Code	EPCS52
Name Space	BEH
Option	N/A

Audit Event	Authentication Attempt, Fail (ability to conduct MFA call)
Additional Information	N/A
MailMan Alert	No

Table A-5: Audit Event, Authentication Result, Success

Audit Event	Authentication Result, Success
BUSA Audit Entry	Authentication Result
Type	S – Service
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS53
Name Space	BEH
Option	N/A
Additional Information	N/A
MailMan Alert	No

Table A-6: Authentication Result, Fail

Audit Event	Authentication Result, Fail
BUSA Audit Entry	Authentication Result
Type	S – Service
Status	F – Fail
Event Domain	E – EPCS Ordering
Event Code	EPCS54
Name Space	BEH
Option	N/A
Additional Information	N/A
MailMan Alert	No

A.3 Provider Profile Audit Events

Audit events are generated by the BEH EPCS Credentialing GUI.

Table A-7: Create Provider Profile, Success

Audit Event	Create Provider Profile, Success
BUSA Audit Entry	Pending Profile Created, Provider: <IEN> – <Name>
Type	PP – Provider Profile

Audit Event	Create Provider Profile, Success
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS30
Additional Information	IEN of Provider
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-8 :Create Provider Profile, Fail

Audit Event	Create Provider Profile, Fail
BUSA Audit Entry	Pending Profile Created, Provider: <IEN> – <Name>
Type	PP – Provider Profile
Status	F – Fail
Event Domain	E – EPCS Ordering
Event Code	EPCS31
Additional Information	IEN of Provider
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-9: Delete Provider Profile, Success

Audit Event	Delete Provider Profile, Success
BUSA Audit Entry	Pending Profile Deleted, Provider: <IEN> – <Name>
Type	PP – Provider Profile
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS32
Additional Information	IEN of Provider
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-10: Delete Provider Profile, Fail

Audit Event	Delete Provider Profile, Fail
BUSA Audit Entry	Pending Profile Deleted, Provider: <IEN> – <Name>

Audit Event	Delete Provider Profile, Fail
Type	PP – Provider Profile
Status	F – Fail
Event Domain	E – EPCS Ordering
Event Code	EPCS33
Additional Information	IEN of Provider
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-11: Edit Provider Profile, Success

Audit Event	Edit Provider Profile, Success
BUSA Audit Entry	Pending Profile Committed, Provider: <IEN> – <Name>
Type	PP – Provider Profile
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS34
Additional Information	IEN of Provider
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-12: Edit Provider Profile, Fail

Audit Event	Edit Provider Profile, Fail
BUSA Audit Entry	Pending Profile Committed, Provider: <IEN> – <Name>
Type	PP – Provider Profile
Status	F – Fail
Event Domain	E – EPCS Ordering
Event Code	EPCS35
Additional Information	IEN of Provider
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-13: Provider Profile-Activate, Success

Audit Event	Provider Profile-Activate, Success
BUSA Audit Entry	Pending Profile Activated, Provider: <IEN> – <Name>
Type	PP – Provider Profile
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS36
Additional Information	IEN of Provider
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-14: Provider Profile-Activate, Fail

Audit Event	Provider Profile-Activate, Fail
BUSA Audit Entry	Pending Profile Activated, Provider: <IEN> – <Name>
Type	PP – Provider Profile
Status	F – Fail
Event Domain	E – EPCS Ordering
Event Code	EPCS37
Additional Information	IEN of Provider
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-15: Provider Profile-Revoke, Success

Audit Event	Provider Profile-Revoke, Success
BUSA Audit Entry	Pending Profile Revoked, Provider: <IEN> – <Name>
Type	PP – Provider Profile
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS38
Additional Information	IEN of Provider
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-16: Provider Profile-Revoke, Fail

Audit Event	Provider Profile-Revoke, Fail
BUSA Audit Entry	Pending Profile Revoked, Provider: <IEN> – <Name>
Type	PP – Provider Profile
Status	F – Fail
Event Domain	E – EPCS Ordering
Event Code	EPCS39
Additional Information	IEN of Provider
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-17: Verify Provider Profile, Success

Audit Event	Verify Provider Profile, Success
BUSA Audit Entry	Verify Provider Profile, Provider: <IEN> – <Name>
Type	PP – Provider Profile
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS40
Additional Information	IEN of Provider~<Activated or Inactivated>
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-18: Verify Provider Profile, Fail

Audit Event	Verify Provider Profile, Fail
BUSA Audit Entry	Verify Provider Profile, Provider: <IEN> – <Name>
Type	PP – Provider Profile
Status	F – Fail
Event Domain	E – EPCS Ordering
Event Code	EPCS41
Additional Information	IEN of Provider
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-19: Create EPCS Provider Access Admin, Success

Audit Event	Create EPCS Provider Access Admin, Success
BUSA Audit Entry	Verify EPCS Provider Access Admin: <IEN> – <Name>
Type	PP – Provider Profile
Status	S – Success
Event Domain	EP – Applicable to EPCS Ordering and EPCS Pharmacy
Event Code	EPCS42
Additional Information	IEN of Provider
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-20: Create EPCS Provider Access Admin, Fail

Audit Event	Create EPCS Provider Access Admin, Fail
BUSA Audit Entry	Verify EPCS Provider Access Admin: <IEN> – <Name>
Type	PP – Provider Profile
Status	S – Fail
Event Domain	EP – Applicable to EPCS Ordering and EPCS Pharmacy
Event Code	EPCS43
Additional Information	IEN of Provider
Name Space	BEH
Option	N/A
MailMan Alert	No

A.4 Daily Incident Report Support Audit Events

These events generate point-in-time audit events allowing a Daily Incident Report to be accurately recreated on another date.

Table A-21: EPCS-Enabled Division, Added

Audit Event	EPCS-Enabled Division, Added
BUSA Audit Entry	Division <Division Name> enabled for EPCS
Type	G – General
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS160

Audit Event	EPCS-Enabled Division, Added
Additional Information	IEN of Division
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-22: EPCS-Enabled Division, Removed

Audit Event	EPCS-Enabled Division, Removed
BUSA Audit Entry	Division <Division Name> removed from EPCS processing
Type	G – General
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS 161
Additional Information	IEN of Division
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-23: Count of EPCS-Enabled Divisions

Audit Event	Count of EPCS-Enabled Divisions
BUSA Audit Entry	Count of EPCS-enabled divisions
Type	G – General
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS162
Additional Information	Count of EPCS enabled division.
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-24: Count of EPCS-Enabled Providers

Audit Event	Count of EPCS-Enabled Providers
BUSA Audit Entry	Count of EPCS-enabled providers
Type	G – General
Status	S – Success
Event Domain	E – EPCS Ordering

Audit Event	Count of EPCS-Enabled Providers
Event Code	EPCS163
Additional Information	Count of EPCS enabled providers.
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-25: Count of EPCS Pharmacists

Audit Event	Count of EPCS Pharmacists
BUSA Audit Entry	Count of EPCS Pharmacists
Type	G – General
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS164
Additional Information	Count of EPCS enabled pharmacists
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-26: Count of Total and Revoked Certificates

Audit Event	Count of Total and Revoked Certificates
BUSA Audit Entry	Count of Certificates: <Total certificates>; Revoked: <Number of revoked>
Type	G – General
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS165
Additional Information	Count of Total^Count of Revoked
Name Space	BEH
Option	N/A
MailMan Alert	No

A.5 EPCS Ordering Events

Table A-27: Creation of an Order

Audit Event	Creation of an Order
BUSA Audit Entry	OR(<Order IEN>;Action: Create <Drug>
Type	X – Prescribing
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS60
Additional Information	IEN of Provider or Provider Agent
Name Space	OR
Option	N/A
MailMan Alert	No

Table A-28: Attempt to Order

Audit Event	Attempt to Order
BUSA Audit Entry	OR(<Order IEN>;Action: Attempt to Order <Drug>
Type	X – Prescribing
Status	F – Fail
Event Domain	E – EPCS Ordering
Event Code	EPCS95
Additional Information	N/A
Name Space	OR
Option	N/A
MailMan Alert	No

Table A-29: Alteration of an Order

Audit Event	Alteration of an Order
BUSA Audit Entry	OR(<Order IEN>;Action: EDIT <Drug>
Type	X – Prescribing
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS61
Additional Information	IEN of Provider or Agent
Name Space	OR
Option	N/A

Audit Event	Alteration of an Order
MailMan Alert	No

Table A-30: Status Changed/Edit

Audit Event	Status Changed/Edit
BUSA Audit Entry	OR(<Order IEN>;Action: Status Changed/Edit <Drug>
Type	P – Pharmacy
Status	S – Success
Event Domain	EP – Applicable to EPCS Ordering and EPCS Pharmacy
Event Code	EPCS78
Additional Information	IEN of Provider or Agent
Name Space	OR
Option	N/A
MailMan Alert	No

Table A-31: Delete an Order

Audit Event	Delete an Order
BUSA Audit Entry	OR(<Order IEN>;Action: Delete <Drug>
Type	X – Prescribing
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS62
Additional Information	IEN of Provider or Agent
Name Space	OR
Option	N/A
MailMan Alert	No

Table A-32: DC/Cancel

Audit Event	DC/Cancel
BUSA Audit Entry	OR(<Order IEN>;Action: DC/Cancel <Drug>
Type	X – Prescribing
Status	S – Success
Event Domain	EP – Applicable to EPCS Ordering or EPCS Pharmacy
Event Code	EPCS77
Additional Information	IEN of Provider or Agent
Name Space	OR

Audit Event	DC/Cancel
Option	N/A
MailMan Alert	No

Table A-33: Ready to Sign an Order

Audit Event	Ready to Sign an Order
BUSA Audit Entry	OR(<Order IEN>;Action: Ready to Sign <Drug>
Type	X – Prescribing
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS63
Additional Information	N/A
Name Space	OR
Option	N/A
MailMan Alert	No

Table A-34 :Unmark Ready to Sign

Audit Event	Unmark Ready to Sign
BUSA Audit Entry	OR(<Order IEN>;Action: Unmark Ready to Sign <Drug>
Type	X – Prescribing
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS74
Additional Information	N/A
Name Space	OR
Option	N/A
MailMan Alert	No

Table A-35: Authenticate an Order (Electronic Signature), Success

Audit Event	Authenticate an Order (Electronic signature), Success
BUSA Audit Entry	OR(<Order IEN>;Action: Elec Sig Code Success <Drug>
Type	X – Prescribing
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS64

Audit Event	Authenticate an Order (Electronic signature), Success
Additional Information	N/A
Name Space	OR
Option	N/A
MailMan Alert	No

Table A-36: Authenticate an Order (Electronic signature), Failure

Audit Event	Authenticate an Order (Electronic signature), Failure
BUSA Audit Entry	OR(<Order IEN>; Action: Elec Sig Code Fail <Drug>
Type	X – Prescribing
Status	F – Fail
Event Domain	E – EPCS Ordering
Event Code	EPCS65
Additional Information	“Paper” of “Electronic”
Name Space	OR
Option	N/A
MailMan Alert	No

Table A-37: Digitally Sign an Order, Success

Audit Event	Digitally Sign an Order, Success
BUSA Audit Entry	OR(<Order IEN>;Action: Digitally Signed Order <Drug>
Type	X – Prescribing
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS67
Additional Information	IEN of Provider
Name Space	OR
Option	N/A
MailMan Alert	No

Table A-38: Digitally Sign an Order, Failure

Audit Event	Digitally Sign an Order, Failure
BUSA Audit Entry	OR(<Order IEN>; Action: Digital Sig Failed <Drug>
Type	X – Prescribing
Status	F – Fail

Audit Event	Digitally Sign an Order, Failure
Event Domain	E – EPCS Ordering
Event Code	EPCS 68
Additional Information	N/A
Name Space	OR
Option	N/A
MailMan Alert	No

Table A-39: Create Record Archive, Success

Audit Event	Create Record Archive, Success
BUSA Audit Entry	OR(<Order IEN>;Action: Order Archive Success <Drug>
Type	X – Prescribing
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS69
Additional Information	N/A
Name Space	OR
Option	N/A
MailMan Alert	No

Table A-40: Create Record Archive, Failure

Audit Event	Create Record Archive, Failure
BUSA Audit Entry	OR(<Order IEN>; Action: Order Archive Fail <Drug>
Type	X – Prescribing
Status	F – Fail
Event Domain	P – Pharmacy
Event Code	EPCS70
Additional Information	N/A
Name Space	OR
Option	N/A
MailMan Alert	No

Table A-41: Transmit an Order, Internal Pharmacy

Audit Event	Transmit an Order, Internal Pharmacy
BUSA Audit Entry	OR(<Order IEN>;Action: Transmit Internally <Drug>
Type	X – Prescribing

Audit Event	Transmit an Order, Internal Pharmacy
Status	S – Success
Event Domain	EP – Applicable to EPCS Ordering and EPCS Pharmacy
Event Code	EPCS71
Additional Information	N/A
Name Space	OR
Option	N/A
MailMan Alert	No

Table A-42: Transmit an Order, Surescripts

Audit Event	Transmit an Order, Surescripts
BUSA Audit Entry	OR(<Order IEN>;Action: Transmitted to SS <Drug>
Type	P – Pharmacy
Status	S – Success
Event Domain	EP – Applicable to EPCS Ordering and EPCS Pharmacy
Event Code	EPCS72
Additional Information	N/A
Name Space	OR
Option	N/A
MailMan Alert	No

A.6 EPCS Pharmacy Events

Table A-43: Unable to Transmit

Audit Event	Unable to Transmit
BUSA Audit Entry	OR(<Order IEN>;Action: Unable to Transmit <Drug>
Type	P – Pharmacy
Status	F – Fail
Event Domain	EP – Applicable to EPCS Ordering and EPCS Pharmacy
Event Code	EPCS73
Additional Information	N/A
Name Space	APSP
Option	N/A
MailMan Alert	No

Table A-44:Transmit Failed

Audit Event	Transmit Failed
BUSA Audit Entry	OR(<Order IEN>;Action: Transmit Failed <Drug>
Type	P – Pharmacy
Status	F – Fail
Event Domain	EP – Applicable to EPCS Ordering and EPCS Pharmacy
Event Code	EPCS76
Additional Information	N/A
Name Space	APSP
Option	N/A
MailMan Alert	No

Table A-45: Order Received, Success

Audit Event	Order Received, Success
BUSA Audit Entry	OR(<Order IEN>;Action: Pharmacy Received <Drug>
Type	P – Pharmacy
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS80
Additional Information	N/A
Name Space	APSP
Option	N/A
MailMan Alert	No

Table A-46: Order Received, Failure

Audit Event	Order Received, Failure
BUSA Audit Entry	OR(<Order IEN>;Action: Unable to Process <Drug>
Type	P – Pharmacy
Status	F - Fail
Event Domain	P – EPCS Pharmacy
Event Code	EPCS81
Additional Information	N/A
Name Space	APSP
Option	N/A
MailMan Alert	No

Table A-47: Digitally Signed, Success

Audit Event	Digitally Signed, Success
BUSA Audit Entry	OR(<Order IEN>;Action: Dig Sig Pharmacy <Drug>
Type	P – Pharmacy
Status	S – Success
Event Domain	P - EPCS Pharmacy
Event Code	EPCS82
Additional Information	N/A
Name Space	APSP
Option	N/A
MailMan Alert	No

Table A-48: Digitally Signed, Fail

Audit Event	Digitally Signed, Fail
BUSA Audit Entry	OR(<Order IEN>;Action: Pharm Digital Sig Failed <Drug>
Type	P – Pharmacy
Status	F – Fail
Event Domain	P – EPCS Pharmacy
Event Code	EPCS83
Additional Information	N/A
Name Space	APSP
Option	N/A
MailMan Alert	No

Table A-49: Pharmacy Record Archive, Success

Audit Event	Pharmacy Record Archive, Success
BUSA Audit Entry	OR(<Order IEN>; Action: Order Archive Fail <Drug>
Type	P – Pharmacy
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS84
Additional Information	N/A
Name Space	APSP
Option	N/A
MailMan Alert	No

Table A-50: Pharmacy Record Archive, Fail

Audit Event	Pharmacy Record Archive, Fail
BUSA Audit Entry	OR(<Order IEN>; Action: Order Archive Fail <Drug>
Type	P – Pharmacy
Status	F – Fail
Event Domain	P – EPCS Pharmacy
Event Code	EPCS85
Additional Information	N/A
Name Space	APSP
Option	N/A
MailMan Alert	No

Table A-51: Discontinue Due to Hash Failure

Audit Event	Discontinue Due to Hash Failure
BUSA Audit Entry	OR(<Order IEN>;Action: Discontinue due hash failure <Drug>
Type	P – Pharmacy
Status	F – Fail
Event Domain	P – EPCS Pharmacy
Event Code	EPCS97
Additional Information	N/A
Name Space	APSP
Option	N/A
MailMan Alert	No

Table A-52: Alteration of a Prescription

Audit Event	Alteration of a Prescription
BUSA Audit Entry	OR(<Order IEN>;Action: Edit <Drug>
Type	P – Pharmacy
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS87
Additional Information	N/A
Name Space	APSP
Option	N/A
MailMan Alert	No

Table A-53: Attest a Hard-Copy Order (Electronic signature), Success

Audit Event	Attest a Hard-Copy Order (Electronic signature), Success
BUSA Audit Entry	OR(<Order IEN>;Action: Elec Sig Code Success <Drug>
Type	P – Pharmacy
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS98
Additional Information	N/A
Name Space	APSP
Option	N/A
MailMan Alert	No

Table A-54: Attest a Hard-Copy Order (Electronic Signature), Fail

Audit Event	Attest a Hard-Copy Order (Electronic Signature), Fail
BUSA Audit Entry	OR(<Order IEN>;Action: Elec Sig Code Fail <Drug>
Type	P – Pharmacy
Status	F – Fail
Event Domain	P – EPCS Pharmacy
Event Code	EPCS96
Additional Information	N/A
Name Space	APSP
Option	N/A
MailMan Alert	No

Table A-55: Verify Pharmacy Hash

Audit Event	Verify Pharmacy Hash
BUSA Audit Entry	OR(<Order IEN>;Action: Verify Pharmacy Hash <Drug>
Type	P – Pharmacy
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS89
Additional Information	N/A
Name Space	APSP
Option	N/A
MailMan Alert	No

Table A-56: Pharmacy Edit

Audit Event	Pharmacy Edit
BUSA Audit Entry	OR(<Order IEN>;Action: Pharmacy Edit <Drug>
Type	P – Pharmacy
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS90
Additional Information	N/A
Name Space	APSP
Option	N/A
MailMan Alert	No

Table A-57: Cancel RX

Audit Event	Cancel RX
BUSA Audit Entry	OR(<Order IEN>;Action: Cancel RX <Drug>
Type	P – Pharmacy
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS91
Additional Information	N/A
Name Space	APSP
Option	N/A
MailMan Alert	No

Table A-58: Changed Accepted

Audit Event	Changed Accepted
BUSA Audit Entry	OR(<Order IEN>;Action: Changed accepted <Drug>
Type	P – Pharmacy
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS92
Additional Information	N/A
Name Space	APSP
Option	N/A
MailMan Alert	No

Table A-59: Surescripts Received

Audit Event	Surescripts Received
BUSA Audit Entry	OR(<Order IEN>;Action: Surescripts Received <Drug>
Type	P – Pharmacy
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS93
Additional Information	N/A
Name Space	APSP
Option	N/A
MailMan Alert	No

Table A-60: Retransmitted

Audit Event	Retransmitted
BUSA Audit Entry	OR(<Order IEN>;Action: Retransmitted <Drug>
Type	P – Pharmacy
Status	S – Success
Event Domain	EP – Applicable to EPCS Ordering and EPCS Pharmacy
Event Code	EPCS94
Additional Information	N/A
Name Space	APSP
Option	N/A
MailMan Alert	No

Table A-61: Printed RX

Audit Event	Printed RX
BUSA Audit Entry	OR(<Order IEN>;Action: Printed RX <Drug>
Type	P – Pharmacy
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS75
Additional Information	N/A
Name Space	APSP
Option	N/A
MailMan Alert	No

Table A-62: Reprinted RX

Audit Event	Reprinted RX
BUSA Audit Entry	OR(<Order IEN>;Action: Reprinted Rx <Drug>
Type	P – Pharmacy
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS79
Additional Information	N/A
Name Space	APSP
Option	N/A
MailMan Alert	No

Table A-63: Dispense

Audit Event	Dispense
BUSA Audit Entry	OR(<Order IEN>; Action: Dispense <Drug>
Type	P – Pharmacy
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS88
Additional Information	IEN of Dispensing Pharmacist
Name Space	APSP
Option	N/A
MailMan Alert	No

A.7 Integrity Checks

Audit events generated from BEHO AUDIT SUMMARY TASK.

Table A-64: BEHO AUDIT SUMMARY TASK Start

Audit Event	BEHO AUDIT SUMMARY TASK Start
BUSA Audit Entry	Started BEHO AUDIT SUMMARY TASK for date: <Date>
Type	S – Service
Status	S – Success
Event Domain	EP – Applicable to EPCS Ordering and EPCS Pharmacy
Event Code	EPCS100

Audit Event	BEHO AUDIT SUMMARY TASK Start
Additional Information	N/A
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-65 :BEHO AUDIT SUMMARY TASK Complete

Audit Event	BEHO AUDIT SUMMARY TASK Complete
BUSA Audit Entry	Completed BEHO AUDIT SUMMARY TASK for date: <Date>
Type	S – Service
Status	S – Success
Event Domain	EP – Applicable to EPCS Ordering and EPCS Pharmacy
Event Code	EPCS101
Additional Information	N/A
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-66: Provider Profile Integrity Check Results – EPCS102

Audit Event	Provider Profile Integrity Check Results
BUSA Audit Entry	Provider Profile Integrity Compile Started
Type	S – Service
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS102
Additional Information	N/A
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-67: Provider Profile Integrity Check Results – EPCS103

Audit Event	Provider Profile Integrity Check Results
BUSA Audit Entry	Provider Profile Integrity Compile Complete. X out of Y logged in BUSA
Type	S – Service
Status	S – Success

Audit Event	Provider Profile Integrity Check Results
Event Domain	E – EPCS Ordering
Event Code	EPCS103
Additional Information	N/A
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-68: CS Order Integrity Check Results – EPCS104

Audit Event	CS Order Integrity Check Results
BUSA Audit Entry	CS Order Integrity Compile Started
Type	S – Service
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS104
Additional Information	N/A
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-69: CS Order Integrity Check Results – EPCS105

Audit Event	CS Order Integrity Check Results
BUSA Audit Entry	CS Order Integrity Compile Completed
Type	S – Service
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS105
Additional Information	N/A
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-70: Audit Record Integrity Check Results – EPCS108

Audit Event	Audit Record Integrity Check Results
BUSA Audit Entry	BUSA Integrity Compile Started
Type	S – Service

Audit Event	Audit Record Integrity Check Results
Status	S – Success
Event Domain	EP – Applicable to EPCS Ordering and EPCS Pharmacy
Event Code	EPCS108
Additional Information	N/A
Name Space	BEH
Option	N/A
MailMan Alert	No

Table A-71: Audit Record Integrity Check Results – EPCS109

Audit Event	Audit Record Integrity Check Results
BUSA Audit Entry	BUSA Integrity Compile Completed
Type	S – Service
Status	S – Success
Event Domain	EP – Applicable to EPCS Ordering and EPCS Pharmacy
Event Code	EPCS109
Additional Information	N/A
Name Space	BEH
Option	N/A
MailMan Alert	No

A.8 Logical Access Control Credentialing Events

Assignment and removal of keys for Provider Profile Admin and Provider Access Admin.

Table A-72: Add Profile Edit Key (XUEPCSEDIT) to User, Success (EPCS120)

Audit Event	Add Profile Edit Key (XUEPCSEDIT) to User, Success
BUSA Audit Entry	XU: Allocated key XUEPCSEDIT to <User Name>
Type	K – Key
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS120
Additional Information	IEN of User
Name Space	XU
Option	N/A

Audit Event	Add Profile Edit Key (XUEPCSEDIT) to User, Success
MailMan Alert	No

Table A-73: Add Profile Edit Key (XUEPCSEDIT) to User, Success (EPCS121)

Audit Event	Add Profile Edit Key (XUEPCSEDIT) to User, Success
BUSA Audit Entry	XU: Allocated key XUEPCSEDIT to <User Name>
Type	K – Key
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS121
Additional Information	IEN of User
Name Space	XU
Option	N/A
MailMan Alert	No

Table A-74: Remove Profile Edit Key (XUEPCSEDIT) from User, Success (EPCS122)

Audit Event	Remove Profile Edit Key (XUEPCSEDIT) from User, Success
BUSA Audit Entry	XU: Deallocated key XUEPCSEDIT from <User Name>
Type	K – Key
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS122
Additional Information	IEN of User
Name Space	XU
Option	N/A
MailMan Alert	No

Table A-75: Remove Profile Edit Key (XUEPCSEDIT) from User, Success (EPCS123)

Audit Event	Remove Profile Edit Key (XUEPCSEDIT) from User, Success
BUSA Audit Entry	XU: Removed delegated key XUEPCSEDIT from <User Name>
Type	K – Key
Status	S - Success

Audit Event	Remove Profile Edit Key (XUEPCSEDIT) from User, Success
Event Domain	E – EPCS Ordering
Event Code	EPCS123
Additional Information	IEN of User
Name Space	XU
Option	N/A
MailMan Alert	No

Table A-76: Add Profile Verify Key (XUZEPCSVERIFY) to User, Success (EPCS124)

Audit Event	Add Profile Verify Key (XUZEPCSVERIFY) to User, Success
BUSA Audit Entry	XU: Allocated key XUZEPCSVERIFY to <User Name>
Type	K – Key
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS124
Additional Information	IEN of User
Name Space	XU
Option	N/A
MailMan Alert	No

Table A-77: Add Profile Verify Key (XUZEPCSVERIFY) to User, Success (EPCS125)

Audit Event	Add Profile Verify Key (XUZEPCSVERIFY) to User, Success
BUSA Audit Entry	XU: Delegated key XUZEPCSVERIFY to <User Name>
Type	K – Key
Status	S – Success
Event Domain	E –EPCS Ordering
Event Code	EPCS125
Additional Information	IEN of User
Name Space	XU
Option	N/A
MailMan Alert	No

Table A-78: Remove Profile Verify Key (XUZEPCSVERIFY) from User, Success (EPCS126)

Audit Event	Remove Profile Verify Key (XUZEPCSVERIFY) from User, Success
BUSA Audit Entry	XU: Deallocated key XUZEPCSVERIFY from <User Name>
Type	K – Key
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS126
Additional Information	IEN of User
Name Space	XU
Option	N/A
MailMan Alert	No

Table A-79: Remove Profile Verify Key (XUZEPCSVERIFY) from User, Success (EPCS127)

Audit Event	Remove Profile Verify Key (XUZEPCSVERIFY) from User, Success
BUSA Audit Entry	XU: Removed delegated key XUZEPCSVERIFY from <User Name>
Type	K – Key
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS127
Additional Information	IEN of User
Name Space	XU
Option	N/A
MailMan Alert	No

A.9 Logical Access Control – Writing Med Orders

Table A-80: Authorized to Write Med Orders Turned On

Audit Event	Authorized to Write Med Orders Turned On
BUSA Audit Entry	XU: Authorized to Write Medical Orders for user <Provider Name>
Type	K – Key
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS128

Audit Event	Authorized to Write Med Orders Turned On
Additional Information	IEN of Provider
Name Space	XU
Option	N/A
MailMan Alert	No

Table A-81: Authorized to Write Med Orders Turned Off

Audit Event	Authorized to Write Med Orders Turned Off
BUSA Audit Entry	XU: Not Authorized to Write Medical Orders for user <Provider Name>
Type	K – Key
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS129
Additional Information	IEN of Provider
Name Space	XU
Option	N/A
MailMan Alert	No

A.10 Logical Access Control Pharmacy Keys

Table A-82: Add Pharmacy Key (PSDRPH, PSORPH) to User, Success (EPCS130)

Audit Event	Add Pharmacy Key (PSDRPH, PSORPH) to User, Success
BUSA Audit Entry	XU: Allocated key PSORPH to <Pharmacist Name>
Type	K – Key
Status	S – Success
Event Domain	P – Pharmacy
Event Code	EPCS130
Additional Information	IEN of Pharmacist
Name Space	XU
Option	N/A
MailMan Alert	No

Table A-83: Add Pharmacy Key (PSDRPH, PSORPH) to User, Success (EPCS131)

Audit Event	Add Pharmacy Key (PSDRPH, PSORPH) to User, Success
BUSA Audit Entry	XU: Allocated key PSDRPH to <Pharmacist Name>
Type	K – Key
Status	S – Success
Event Domain	P – Pharmacy
Event Code	EPCS131
Additional Information	IEN of Pharmacist
Name Space	XU
Option	N/A
MailMan Alert	No

Table A-84: Add Pharmacy Key (PSDRPH, PSORPH) to User, Success (EPCS132)

Audit Event	Add Pharmacy Key (PSDRPH, PSORPH) to User, Success
BUSA Audit Entry	XU: Delegated key PSORPH to <Pharmacist Name>
Type	K – Key
Status	S – Success
Event Domain	P – Pharmacy
Event Code	EPCS132
Additional Information	IEN of Pharmacist
Name Space	XU
Option	N/A
MailMan Alert	No

Table A-85: Add Pharmacy Key (PSDRPH, PSORPH) to User, Success (EPCS133)

Audit Event	Add Pharmacy Key (PSDRPH, PSORPH) to User, Success
BUSA Audit Entry	XU: Delegated key PSDRPH to <Pharmacist Name>
Type	K – Key
Status	S – Success
Event Domain	P – Pharmacy
Event Code	EPCS133
Additional Information	IEN of Pharmacist
Name Space	XU

Audit Event	Add Pharmacy Key (PSDRPH, PSORPH) to User, Success
Option	N/A
MailMan Alert	No

Table A-86: Remove Pharmacy Key (PSDRPH, PSORPH) from User, Success (EPCS134)

Audit Event	Remove Pharmacy Key (PSDRPH, PSORPH) from User, Success
BUSA Audit Entry	XU: Deallocated key PSORPH from <Pharmacist Name>
Type	K – Key
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS134
Additional Information	IEN of Pharmacist
Name Space	XU
Option	N/A
MailMan Alert	No

Table A-87: Remove Pharmacy Key (PSDRPH, PSORPH) from User, Success (EPCS135)

Audit Event	Remove Pharmacy Key (PSDRPH, PSORPH) from User, Success
BUSA Audit Entry	XU: Deallocated key PSDRPH from <Pharmacist Name>
Type	K – Key
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS135
Additional Information	IEN of Pharmacist
Name Space	XU
Option	N/A
MailMan Alert	No

Table A-88: Remove Pharmacy Key (PSDRPH, PSORPH) from User, Success (EPCS136)

Audit Event	Remove Pharmacy Key (PSDRPH, PSORPH) from User, Success
BUSA Audit Entry	XU: Removed delegated key PSORPH from <Pharmacist Name>
Type	K – Key

Audit Event	Remove Pharmacy Key (PSDRPH, PSORPH) from User, Success
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS136
Additional Information	IEN of Pharmacist
Name Space	XU
Option	N/A
MailMan Alert	No

Table A-89: Remove Pharmacy Key (PSDRPH, PSORPH) from User, Success (EPCS137)

Audit Event	Remove Pharmacy Key (PSDRPH, PSORPH) from User, Success
BUSA Audit Entry	XU: Removed delegated key PSDRPH <Pharmacist Name>
Type	K – Key
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS137
Additional Information	IEN of Pharmacist
Name Space	XU
Option	N/A
MailMan Alert	No

A.11 Logical Access Controls – Pharmacy Menus

Table A-90: Add Pharmacy Menu to User, Success (EPCS150)

Audit Event	Add Pharmacy Menu to User, Success
BUSA Audit Entry	XU: Assigned Primary Menu <menu name> to user <Pharmacist Name>
Type	M – Menu
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS150
Additional Information	IEN of Pharmacist
Name Space	XU
Option	N/A
MailMan Alert	No

Table A-91: Add Pharmacy Menu to User, Success (EPCS151)

Audit Event	Add Pharmacy Menu to User, Success
BUSA Audit Entry	XU: Assigned Secondary Menu <menu name> to user <Pharmacist Name>
Type	M – Menu
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS151
Additional Information	IEN of Pharmacist
Name Space	XU
Option	N/A
MailMan Alert	No

Table A-92: Remove Pharmacy Menu from User, Success (EPCS152)

Audit Event	Remove Pharmacy Menu from User, Success
BUSA Audit Entry	XU: Removed Primary Menu <menu name> from user <Pharmacist Name>
Type	M – Menu
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS152
Additional Information	IEN of Pharmacist
Name Space	XU
Option	N/A
MailMan Alert	No

Table A-93: Remove Pharmacy Menu from User, Success (EPCS153)

Audit Event	Remove Pharmacy Menu from User, Success
BUSA Audit Entry	XU: Removed Secondary Menu <menu name> from user <Pharmacist Name>
Type	M – Menu
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS153
Additional Information	IEN of Pharmacist
Name Space	XU

Audit Event	Remove Pharmacy Menu from User, Success
Option	N/A
MailMan Alert	No

A.12 Logical Access Control – Access Pharmacy Menus

Table A-94: Access Pharmacy Options, Success

Audit Event	Access Pharmacy Options, Success
BUSA Audit Entry	XU: Selected Option Pharmacist Menu <Menu Option>
Type	O – Option
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS154
Additional Information	N/A
Name Space	XU
Option	N/A
MailMan Alert	No

Table A-95: Access Pharmacy Options, Fail

Audit Event	Access Pharmacy Options, Fail
BUSA Audit Entry	XU: Denied Access to <Menu Option>
Type	O – Option
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS155
Additional Information	N/A
Name Space	XU
Option	N/A
MailMan Alert	No

A.13 Logical Access Control – Login

Table A-96: Login Success (EPCS140)

Audit Event	Login Success
BUSA Audit Entry	XU: Successful System Login
Type	L – Login

Audit Event	Login Success
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS140
Additional Information	N/A
Name Space	XU
Option	N/A
MailMan Alert	No

Table A-97: Login Attempt Fail (EPCS141)

Audit Event	Login Attempt Fail
BUSA Audit Entry	XU: Failed System Login Attempt – Invalid Verify Code Attempt <#>
Type	L – Login
Status	F – Fail
Event Domain	E –EPCS Ordering
Event Code	EPCS141
Additional Information	N/A
Name Space	XU
Option	N/A
MailMan Alert	No

Table A-98: Login Success (EPCS142)

Audit Event	Login Success
BUSA Audit Entry	XU: Successful System Login
Type	L – Login
Status	S – Success
Event Domain	P – EPCS Pharmacy
Event Code	EPCS142
Additional Information	N/A
Name Space	XU
Option	N/A
MailMan Alert	No

Table A-99: Login Attempt Fail (EPCS143)

Audit Event	Login Attempt Fail
BUSA Audit Entry	XU: Failed System Login Attempt – Invalid Verify Code Attempt <#>
Type	L – Login
Status	F – Fail
Event Domain	P – EPCS Pharmacy
Event Code	EPCS143
Additional Information	N/A
Name Space	XU
Option	N/A
MailMan Alert	No

Table A-100: Login Success (EPCS144)

Audit Event	Login Success
BUSA Audit Entry	XU: Successful System Login
Type	L – Login
Status	S – Success
Event Domain	EP – Applicable to EPCS Ordering and EPCS Pharmacy
Event Code	EPCS144
Additional Information	N/A
Name Space	XU
Option	N/A
MailMan Alert	No

Table A-101: Login Attempt Fail (EPCS145)

Audit Event	Login Attempt Fail
BUSA Audit Entry	XU: Failed System Login Attempt – Invalid Verify Code Attempt <#>
Type	L – Login
Status	F – Fail
Event Domain	EP – Applicable to EPCS Ordering and EPCS Pharmacy
Event Code	EPCS145
Additional Information	N/A
Name Space	XU
Option	N/A

Audit Event	Login Attempt Fail
MailMan Alert	No

Appendix B 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.cfm.

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

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

B.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).

B.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.

B.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.

B.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.

B.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.

B.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.

B.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).

B.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.

B.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.

B.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.

B.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.

B.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.

B.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.

B.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.

B.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.

B.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

BUSA

Namespace for the IHS User Security Audit.

Centers for Medicare & Medicaid Services

An agency within the HHS.

Meaningful Use

Meaningful Use is a term used by the Centers for Medicare and Medicaid Services to ensure that providers and hospitals that have adopted certified EHR are using the technology to further the goals of information exchange among health care professionals. Eligible Providers (EPs) and Eligible Hospitals (EHs) will achieve meaningful use if the EP or EH (a) demonstrate use of certified EHR technology in a meaningful manner, (b) demonstrate the certified EHR technology provides for electronic exchange of health information to improve quality of care, and (c) use certified EHR technology to submit information on clinical quality and other measures.

Resource and Patient Management System

A series of integrated software components that includes clinical, administrative, and financial functions.

Acronym List

Acronym	Meaning
CHIT	2015 Certified Health IT
CISO	Chief Information Security Officer
CMS	Centers for Medicare & Medicaid Services
DEA	Drug Enforcement Administration
EH	Eligible Hospital
EHR	Electronic Health Record
EP	Eligible Provider
EPCS	Electronic Prescribing of Controlled Substances
HIPAA	Health Insurance Portability and Accountability Act
HHS	Department of Health and Human Services
ID	Identification
IHS	Indian Health Service
IP	Internet Protocol
ISSO	Information System Security Officer
IT	Information Technology
MU	Meaningful Use
PC	Personal Computer
ROB	Rules of Behavior
RPMS	Resource and Patient Management System
SAC	Standards and Conventions
VPN	Virtual Private Network

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