RESOURCE AND PATIENT MANAGEMENT SYSTEM

IHS USER SECURITY AUDIT

(BUSA)

User Manual

Version 1.0 Patch 1
August 2019

Office of Information Technology
Division of Information Technology

Table of Contents

Document Revision History

Version	Date	Author	Description	Sections
1.0	September 2014	GDIT	Initial Release	All
1.1	August 2019	GDIT SESS team	v1.1 update	All

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. Specifically, this addendum provides additional information on utilizing the new reporting utility available for Electronic Prescribing of Controlled Substances (EPCS).

1.0 Introduction

The BUSA package is a utility that enables tracking of user activity. As a requirement for Meaningful Use stage two certification, all activity relating to patient data querying, adding, editing, copying, deleting, and printing must be logged. With the EPCS release, additional information is logged into BUSA to meet Drug Enforcement Administration (DEA) auditing and reporting requirements.

The BUSA package contains a web-enabled reporting interface, which permits this logged data to be filtered, sorted, and displayed. Patch 1 contains a new web-enabled reporting interface, specifically designed to meet the reporting needs of EPCS.

2.0 Package Management

The menu option to manage BUSA is **Edit Security Audit** (**BUSA SECURITY EDIT**). To access this option, the user must be assigned the BUSAZMGR security. Access should be restricted to site managers, who should run it only when necessary.

3.0 Package Operation

BUSA is installed with each of the Security Audit switches turned on. The **Date Logged** field will display the date and time that the link was either turned on or turned off. The **User Logged** field will display the user who performed the action on the link (as shown in Figure 3-1).

```
Edit Security Audit
Current Security Audit Settings:
     Master         Status:        On
                    Date Logged:   MAY 04, 2013@18:58:55
                    User Logged:   DEMO,USER E
     BMXNet         Status:        On
                    Date Logged:   MAY 04, 2013@18:58:55
                    User Logged:   DEMO,USER E
     CIA Broker     Status:        On
                    Date Logged:   MAY 04, 2013@18:58:55
                    User Logged:   DEMO,USER E
     XWB Broker     Status:        On
                    Date Logged:   MAY 04, 2013@18:58:56
                    User Logged:   DEMO,USER E

     Select one of the following:

          M         Master
          B         BMXNet
          C         CIA Broker
          W         XWB Broker

Select Switch:
```

Figure 3-1: Security and switches

Any switch can be disabled (turned off) if the site manager thinks it appropriate as shown in Figure 3-2.

```
     Select one of the following:

          M         Master
          B         BMXNet
          C         CIA Broker
          W         XWB Broker

Select Switch: BMXNet

     Select one of the following:

          1         On
          0         Disabled

Change Status: On// 0  Disabled
Disable Comment: Data growing too fast
```

Figure 3-2: 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—will be logged as shown in Figure 3-3.

```
Edit Security Audit
Current Security Audit Settings:
     Master         Status:        On
                    Date Logged:   MAY 04, 2013@18:58:55
                    User Logged:   DEMO,USER E
     BMXNet         Status:        Disabled
                    Date Logged:   AUG 02, 2013@15:52:02
                    User Logged:   DEMO,USER L
           Disabled Comment:Data growing too fast
     CIA Broker     Status:        On
                    Date Logged:   MAY 04, 2013@18:58:55
                    User Logged:   DEMO,USER E
     XWB Broker     Status:        On
                    Date Logged:   MAY 04, 2013@18:58:56
                    User Logged:   DEMO,USER E

     Select one of the following:

          M         Master
          B         BMXNet
          C         CIA Broker
          W         XWB Broker

Select Switch:
```

Figure 3-3: Audit trail

4.0 GUI Report

4.1 Original BUSA Report Utility

The original Version 1.0 reporting utility can be accessed at the address listed below this paragraph. 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 the namespace of the RPMS live database. See the installation manual for further details on determining these values.

http://IP address:port/csp/namepace/BUSA.MainReportPage.cls

> **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 above address in a Windows screen replacing the IP address, port, and namespace, as described in Section 4.1.
2. The report screen will display. See Figure 4-1.

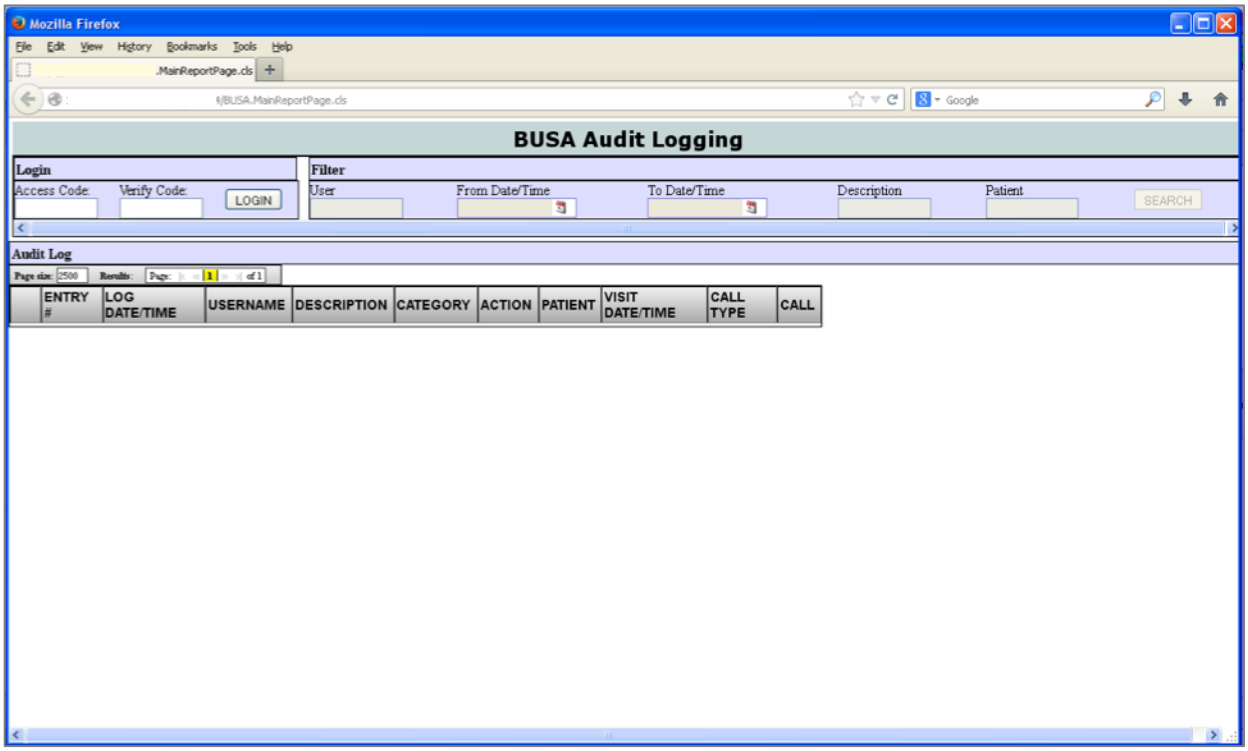


Figure 4-1: Initial BUSA audit report display (prior to login)

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

4. Click **Login**.

Users who are assigned the BUSAZRPT security key and were 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 4-2.

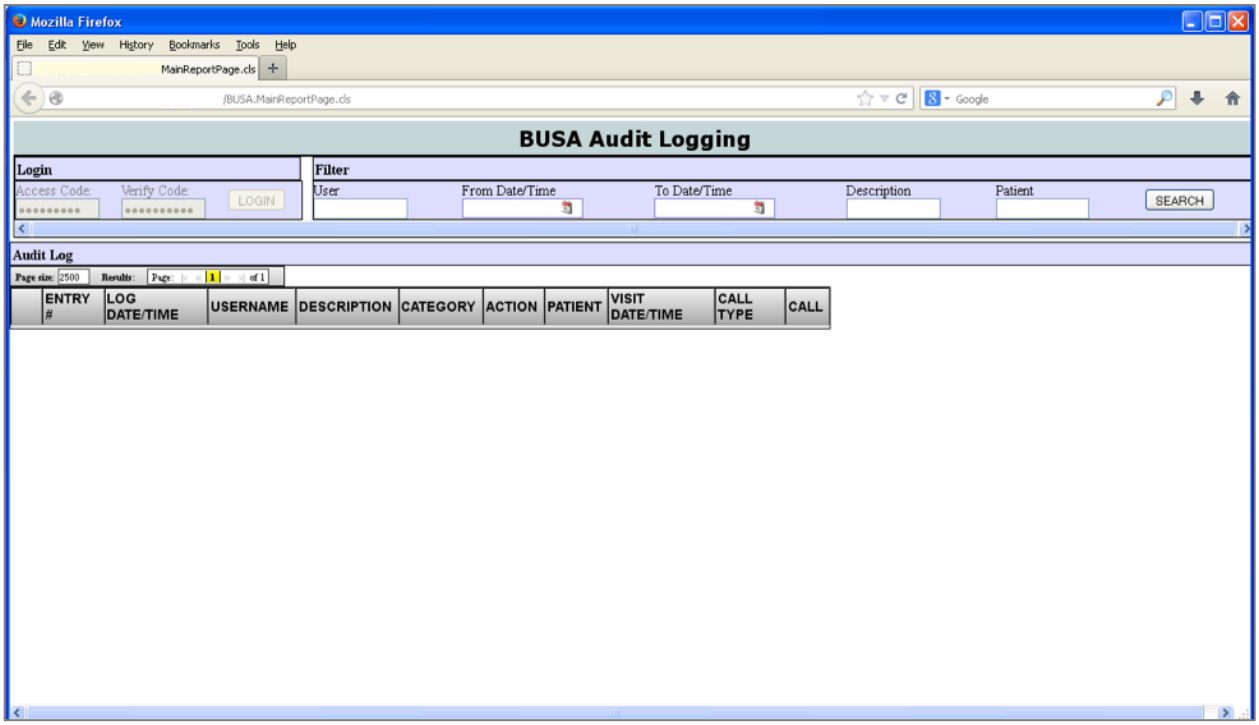


Figure 4-2: Authorized BUSA users with successful log in

4.1.2 Conduct Searches

Users can select as many filter options needed to produce customized audit reports. After selecting report filters, click the **Search** button to run a report.

At minimum, users should select the **From Date/Time** and **To Date/Time** filters to limit the number of records returned. 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 4-3, are as follows:

- **User**: Enter the **Last Name** or **Last Name,First Name** to specify a user. Partial lookups are allowed and a **Starts with** field match can be performed.
- **From Date/Time** and **To Date/Time**: Enter a date/time range.

- **Description**: Any description that was assigned to an event. Partial lookups are allowed and a **Starts with** field match can be performed.
- **Patient**: Specify patients using **Last Name** or **Last Name,First Name**. Partial lookups are allowed and a **Starts with** field match can be performed.

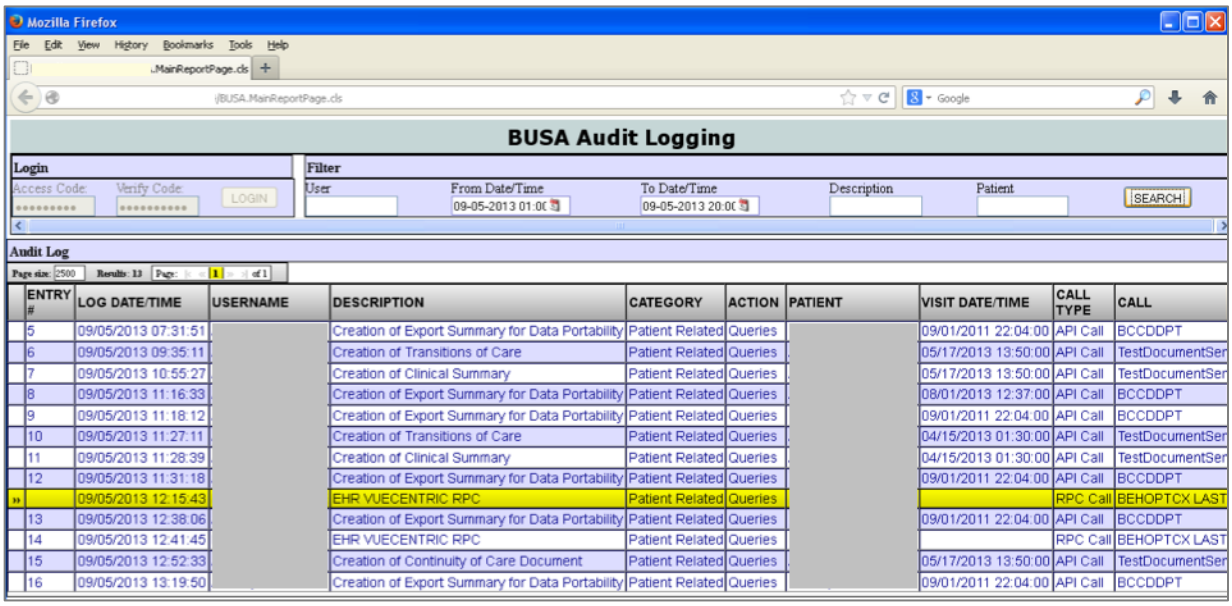


Figure 4-3: Performing a search using filters

4.1.3 Sorting Results

Search results can also be sorted. After obtaining results, users can click on any of the column headers to search the results in an ascending order. Click the column header a second time to sort the display in descending order. See Figure 4-4 for a display of a descending sort by date/time.

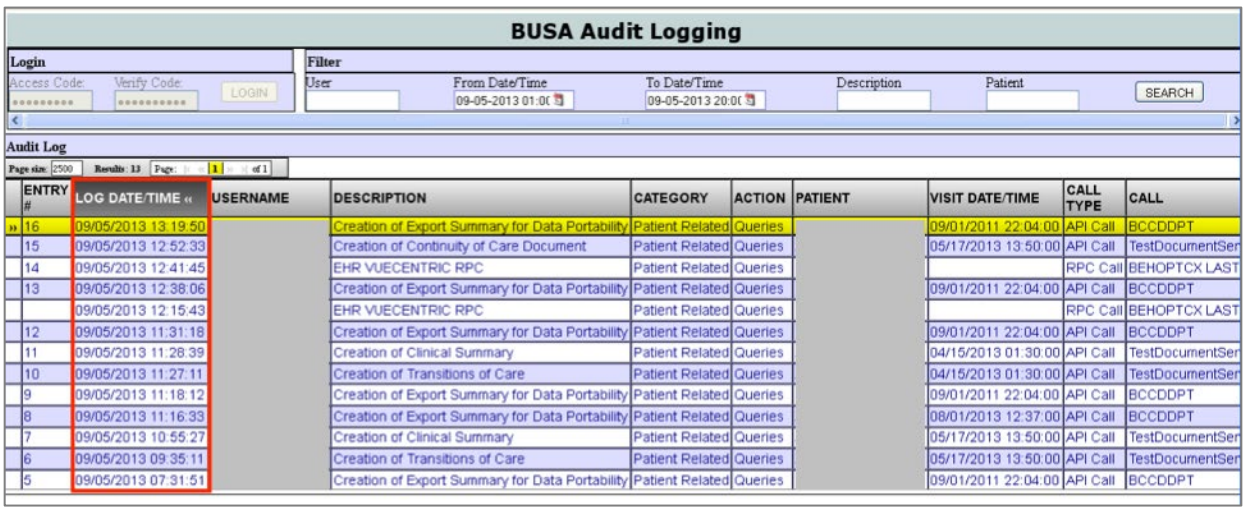


Figure 4-4: Sample display sorting by Log Date/Time in descending order

4.2 EPCS BUSA Report Utility

The new EPCS BUSA Report Utility delivered with patch 1 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 the namespace of the RPMS live database. See the installation manual for further details on determining these values.

http://IP address:port/csp/namepace/BUSA.EPCSMainReportPage.cls

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

4.2.1 EPCS BUSA Report Utility Log In

1. Paste the above address in a Windows screen, replacing the IP address, port and namespace, as appropriate.
2. The report screen will display. See Figure 4-5.

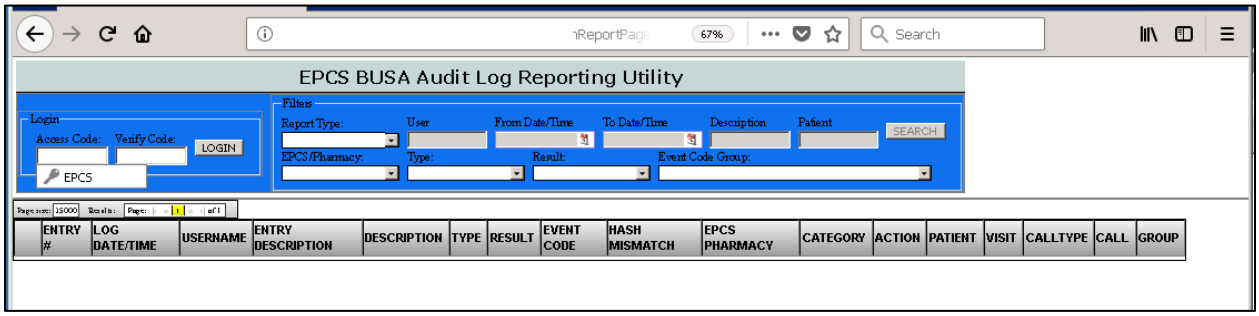


Figure 4-5: Initial EPCS BUSA audit report display (prior to login)

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

Users who are assigned the BUSAZRPT security key and were 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 4-6.

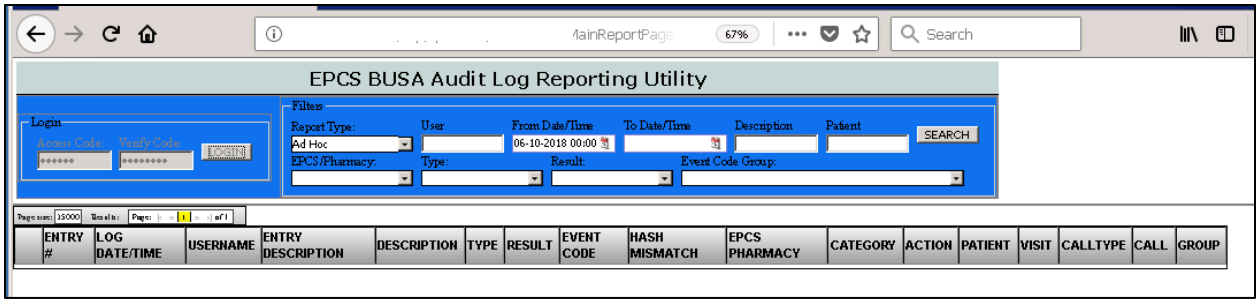


Figure 4-6: Authorized BUSA users with successful EPCS BUSA Report Utility log in

4.2.2 Choosing EPCS Report Type

The EPCS BUSA Report Utility allows users to view data in two different formats: Ad Hoc and List. To switch between the two formats, in the Filters section, select **Ad Hoc** or **List** from the **Report Type** box. After changing the display format, the search must be executed again to update the display.

4.2.2.1 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 will now frequently contain multiple pieces of information per record, with each piece delimited by a vertical bar (|) character. Figure 4-7 shows a sample Ad Hoc report.

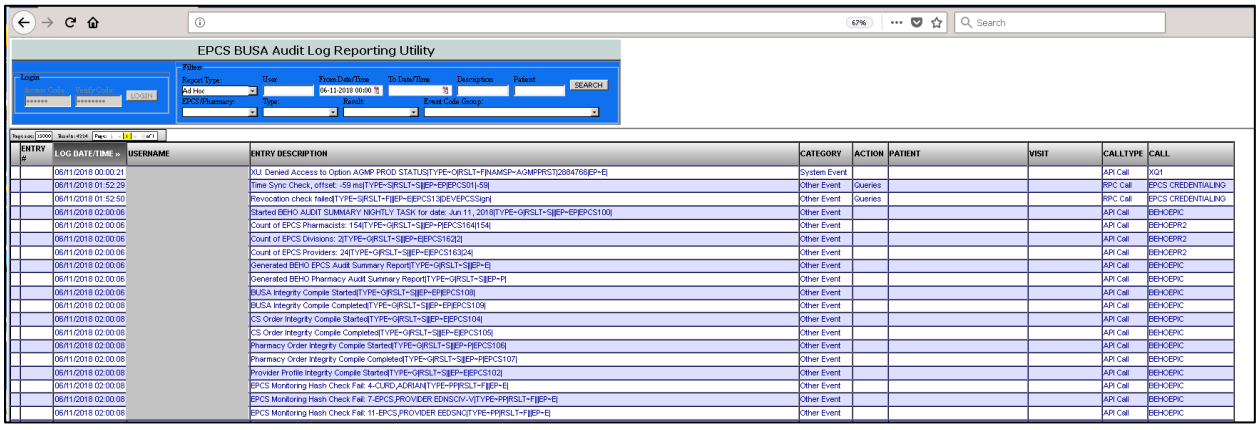


Figure 4-7: Sample Ad Hoc report format

4.2.2.2 List Report Display Format

The List Report 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 4-8 shows a sample List Report.

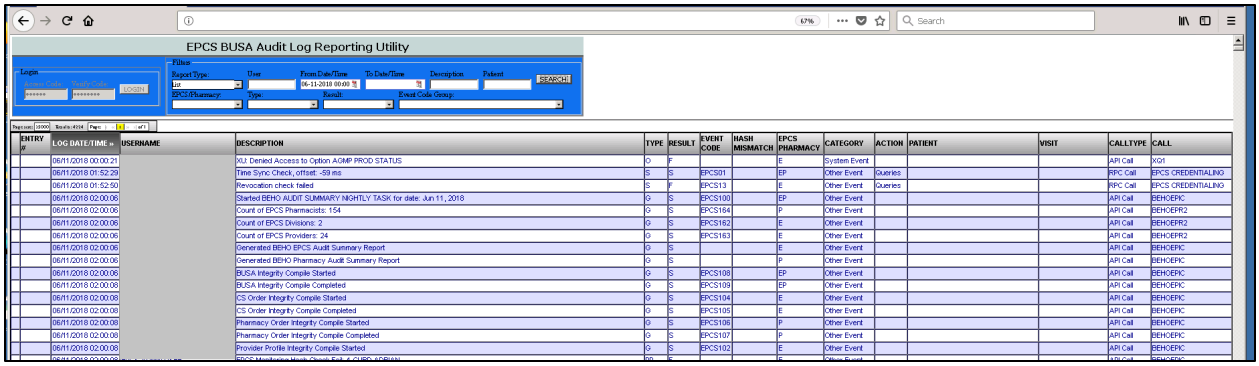


Figure 4-8: Sample List Report Format

4.2.3 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.

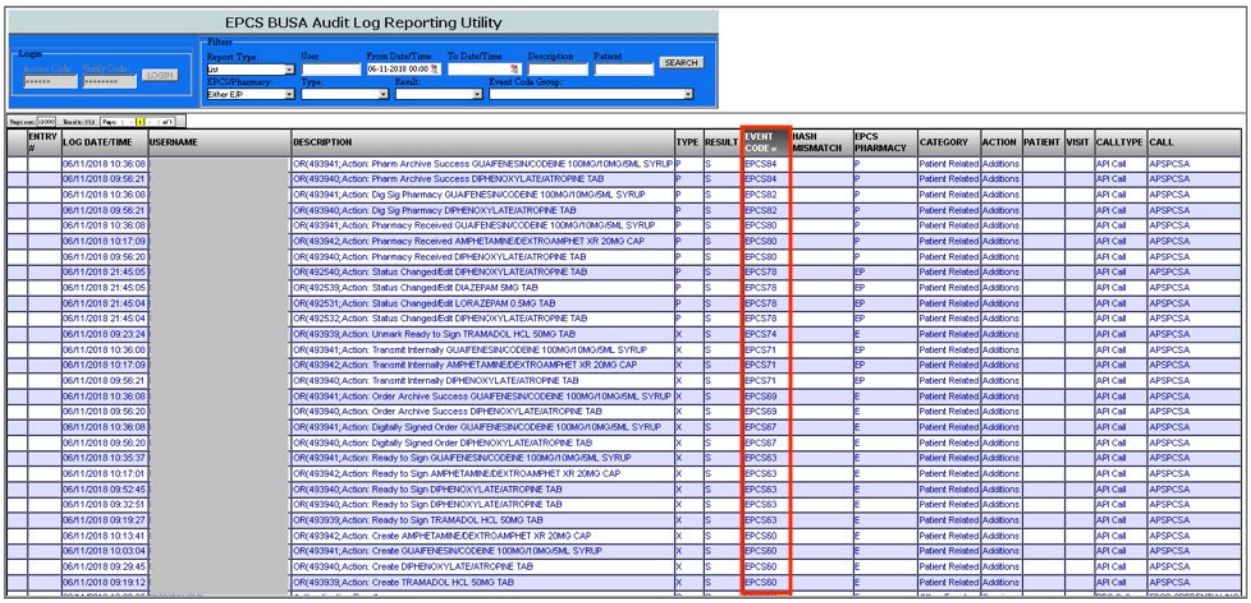
The additional filtering options available with the EPCS Report Type consist of the following:

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

4.2.4 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 on any of the column headers to search the results in an ascending order. Click the column header a second time to sort the display in descending order. See Figure 4-9 for a display of a report example, sorted in descending order by the **Event Code** column.



ENTRY #	LOG DATE/TIME	USERNAME	DESCRIPTION	TYPE	RESULT	EVENT CODE	HASH MISMATCH	EPCS PHARMACY	CATEGORY	ACTION	PATIENT	VISIT	CALLTYPE	CALL
	06/11/2018 10:36:08		OR(493941,Action: Pharm Archive Success GUAIFENESIN/CODEINE 100MG/10MG/5ML SYRUP	P	S	EPCS84		P	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 09:56:21		OR(493940,Action: Pharm Archive Success DIPHENOXYLATE/ATROPINE TAB	P	S	EPCS84		P	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 10:36:08		OR(493941,Action: Dig Sig Pharmacy GUAIFENESIN/CODEINE 100MG/10MG/5ML SYRUP	P	S	EPCS82		P	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 09:56:21		OR(493940,Action: Dig Sig Pharmacy DIPHENOXYLATE/ATROPINE TAB	P	S	EPCS82		P	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 10:36:08		OR(493941,Action: Pharmacy Received GUAIFENESIN/CODEINE 100MG/10MG/5ML SYRUP	P	S	EPCS80		P	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 10:17:09		OR(493942,Action: Pharmacy Received AMPHETAMINE/DEXTRO/AMPHET XR 20MG CAP	P	S	EPCS80		P	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 09:56:20		OR(493940,Action: Pharmacy Received DIPHENOXYLATE/ATROPINE TAB	P	S	EPCS80		P	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 21:45:05		OR(492540,Action: Status Changed/Edit DIPHENOXYLATE/ATROPINE TAB	P	S	EPCS78		EP	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 21:45:05		OR(492539,Action: Status Changed/Edit DIAZEPAM 5MG TAB	P	S	EPCS78		EP	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 21:45:04		OR(492531,Action: Status Changed/Edit LORAZEPAM 0.5MG TAB	P	S	EPCS78		EP	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 21:45:04		OR(492532,Action: Status Changed/Edit DIPHENOXYLATE/ATROPINE TAB	P	S	EPCS78		EP	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 09:23:24		OR(493939,Action: Unmark Ready to Sign TRAMADOL HCL 50MG TAB	X	S	EPCS74		E	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 10:36:08		OR(493941,Action: Transmit Internally GUAIFENESIN/CODEINE 100MG/10MG/5ML SYRUP	X	S	EPCS71		EP	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 10:17:09		OR(493942,Action: Transmit Internally AMPHETAMINE/DEXTRO/AMPHET XR 20MG CAP	X	S	EPCS71		EP	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 09:56:21		OR(493940,Action: Transmit Internally DIPHENOXYLATE/ATROPINE TAB	X	S	EPCS71		EP	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 10:36:08		OR(493941,Action: Order Archive Success GUAIFENESIN/CODEINE 100MG/10MG/5ML SYRUP	X	S	EPCS69		E	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 09:56:20		OR(493940,Action: Order Archive Success DIPHENOXYLATE/ATROPINE TAB	X	S	EPCS69		E	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 10:36:08		OR(493941,Action: Digitally Signed Order GUAIFENESIN/CODEINE 100MG/10MG/5ML SYRUP	X	S	EPCS67		E	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 09:56:20		OR(493940,Action: Digitally Signed Order DIPHENOXYLATE/ATROPINE TAB	X	S	EPCS67		E	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 10:35:37		OR(493941,Action: Ready to Sign GUAIFENESIN/CODEINE 100MG/10MG/5ML SYRUP	X	S	EPCS63		E	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 10:17:01		OR(493942,Action: Ready to Sign AMPHETAMINE/DEXTRO/AMPHET XR 20MG CAP	X	S	EPCS63		E	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 09:52:45		OR(493940,Action: Ready to Sign DIPHENOXYLATE/ATROPINE TAB	X	S	EPCS63		E	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 09:32:51		OR(493940,Action: Ready to Sign DIPHENOXYLATE/ATROPINE TAB	X	S	EPCS63		E	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 09:19:27		OR(493939,Action: Ready to Sign TRAMADOL HCL 50MG TAB	X	S	EPCS63		E	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 10:13:41		OR(493942,Action: Create AMPHETAMINE/DEXTRO/AMPHET XR 20MG CAP	X	S	EPCS60		E	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 10:03:04		OR(493941,Action: Create GUAIFENESIN/CODEINE 100MG/10MG/5ML SYRUP	X	S	EPCS60		E	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 09:29:45		OR(493940,Action: Create DIPHENOXYLATE/ATROPINE TAB	X	S	EPCS60		E	Patient Related	Additions			API Call	APSPCSA
	06/11/2018 09:19:12		OR(493939,Action: Create TRAMADOL HCL 50MG TAB	X	S	EPCS60		E	Patient Related	Additions			API Call	APSPCSA

Figure 4-9: EPCS BUSA List report sorted by Event Code (descending order)

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 will be 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 1 to 3 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.

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.

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

Audit Event	Time synchronization check failed
MailMan Alert	No

A.2 EPCS Signing Certificate Check

Multi-Factor Authentication – Cryptographic Token Events

Audit events are generated by the BEH 2FA Service.

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

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
Additional Information	N/A
MailMan Alert	No

Audit Event	Authentication Result, Success
BUSA Audit Entry	Authentication Result
Type	S – Service
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS53

Audit Event	Authentication Result, Success
Name Space	BEH
Option	N/A
Additional Information	N/A
MailMan Alert	No

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.

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

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

Audit Event	Create Provider Profile, Fail
Name Space	BEH
Option	N/A
MailMan Alert	No

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

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

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

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

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

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

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

Audit Event	Provider Profile-Revoke, Success
Event Code	EPCS38
Additional Information	IEN of Provider
Name Space	BEH
Option	N/A
MailMan Alert	No

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

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

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

Audit Event	Verify Provider Profile, Fail
MailMan Alert	No

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

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 to allow a Daily Incident Report to be accurately recreated at a later date.

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
Additional Information	IEN of Division
Name Space	BEH
Option	N/A

Audit Event	EPCS-Enabled division, added
MailMan Alert	No

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

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

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

Audit Event	Count of EPCS Pharmacists
BUSA Audit Entry	Count of EPCS Pharmacists
Type	G – General

Audit Event	Count of EPCS Pharmacists
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

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

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

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

Audit Event	Attempt to Order
Event Code	EPCS95
Additional Information	N/A
Name Space	OR
Option	N/A
MailMan Alert	No

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
MailMan Alert	No

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

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

Audit Event	Delete an Order
MailMan Alert	No

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
Option	N/A
MailMan Alert	No

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

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

Audit Event	Authenticate an Order (Electronic signature), Success
BUSA Audit Entry	OR(<Order IEN>;Action: Elec Sig Code Success <Drug>

Audit Event	Authenticate an Order (Electronic signature), Success
Type	X – Prescribing
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS64
Additional Information	N/A
Name Space	OR
Option	N/A
MailMan Alert	No

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

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

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

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

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

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

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

Audit Event	Transmit an Order, Internal Pharmacy
MailMan Alert	No

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

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

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

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

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

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

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

Audit Event	Digitally Signed, Fail
Event Code	EPCS83
Additional Information	N/A
Name Space	APSP
Option	N/A
MailMan Alert	No

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

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

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

Audit Event	Discontinue due to hash failure
MailMan Alert	No

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

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

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

Audit Event	Verify Pharmacy Hash
BUSA Audit Entry	OR(<Order IEN>;Action: Verify Pharmacy Hash <Drug>

Audit Event	Verify Pharmacy Hash
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

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

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

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

Audit Event	Changed accepted
Additional Information	N/A
Name Space	APSP
Option	N/A
MailMan Alert	No

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

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

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

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

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

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
Additional Information	N/A
Name Space	BEH
Option	N/A
MailMan Alert	No

Audit Event	BEHO AUDIT SUMMARY TASK Complete
BUSA Audit Entry	Completed BEHO AUDIT SUMMARY TASK for date: <Date>

Audit Event	BEHO AUDIT SUMMARY TASK Complete
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

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

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
Event Domain	E – EPCS Ordering
Event Code	EPCS103
Additional Information	N/A
Name Space	BEH
Option	N/A
MailMan Alert	No

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

Audit Event	CS Order Integrity Check Results
Additional Information	N/A
Name Space	BEH
Option	N/A
MailMan Alert	No

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

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

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.

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
MailMan Alert	No

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

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

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
Event Domain	E – EPCS Ordering
Event Code	EPCS123
Additional Information	IEN of User
Name Space	XU
Option	N/A
MailMan Alert	No

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

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

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

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

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
Additional Information	IEN of Provider
Name Space	XU
Option	N/A
MailMan Alert	No

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

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

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

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

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
Option	N/A
MailMan Alert	No

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

Audit Event	Remove Pharmacy Key (PSDRPH, PSORPH) from User, Success
BUSA Audit Entry	XU: Deallocated key PSDRPH from <Pharmacist Name>

Audit Event	Remove Pharmacy Key (PSDRPH, PSORPH) from User, Success
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

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

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

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

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

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

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
Option	N/A
MailMan Alert	No

A.12 Logical Access Control – Access Pharmacy Menus

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

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

Audit Event	Login Success
BUSA Audit Entry	XU: Successful System Login
Type	L – Login
Status	S – Success
Event Domain	E – EPCS Ordering
Event Code	EPCS140
Additional Information	N/A
Name Space	XU
Option	N/A
MailMan Alert	No

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

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

Audit Event	Login Attempt Fail
BUSA Audit Entry	XU: Failed System Login Attempt - Invalid Verify Code Attempt <#>

Audit Event	Login Attempt Fail
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

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

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
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 web site: http://security.ihs.gov/.

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 ROBs 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 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, 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
DEA	Drug Enforcement Administration
EH	Eligible Hospital
EHR	Electronic Health Record
EP	Eligible Provider
EPCS	Electronic Prescribing of Controlled Substances
HHS	Department of Health and Human Services
ID	Identification
IHS	Indian Health Service
IP	Internet Protocol
ISSO	Information System Security Officer
IT	Information Technology
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 OIT Help Desk (IHS).

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

Web: http://www.ihs.gov/helpdesk/

Email: support@ihs.gov