RESOURCE AND PATIENT MANAGEMENT SYSTEM

Controlled Drug Export System

(BPDM)

User Manual

Version 2.0 Patch 4
May 2019

Office of Information Technology
Division of Information Technology

Table of Contents

Preface

The Controlled Drug Export System is used to identify prescriptions for controlled drugs and other specified drugs dispensed at Indian Health Service (IHS) and tribal health care facilities and create an export file for transmission to state Prescription Drug Monitoring Programs (PDMP). Data is extracted from the Resource and Patient Management System (RPMS) Outpatient Pharmacy Application, in operation at the local facilities. This software creates the export file and saves it in a secure directory as defined by facility's RPMS Site Manager or other IT management personnel. In this patch there is the ability of the file to be automatically transmitted to the PDMP if supported. It is the responsibility of local pharmacy staff or other designated individual to transmit the export file to the PDMP in a timely manner consistent with Health Insurance Portability and Accountability Act (HIPAA) and IHS requirements based on the site's functionality.

This manual provides user instructions on the set up and use of the Controlled Drug Export System.

This version of the software accommodates exports in the following standards which are owned and distributed by the American Society of Automation in Pharmacy (ASAP):

- ASAP Version 4.2a Standard
- ASAP Version 4.2 Standard
- ASAP Version 4.1 Standard
- ASAP Version 4.0 Standard
- ASAP Version 3.0 Standard
- ASAP 1995 Standard

Revision History

Date	Revision	Description	Author
08/02/2012	1.0	User manual v2.0 release	
04/11/2018	1.1	Updated document as a whole to include updates through v2.0 patch 4. Most sections required an update.	Mark Williams

1.0 Introduction

In order to effectively use the Controlled Drug Export System, it is important that the site parameters be set up completely and correctly. There are numerous site parameter values which must be stored in the Prescription Drug Monitoring (PDM) Site Parameters file before data can be extracted for export to the state PDM program.

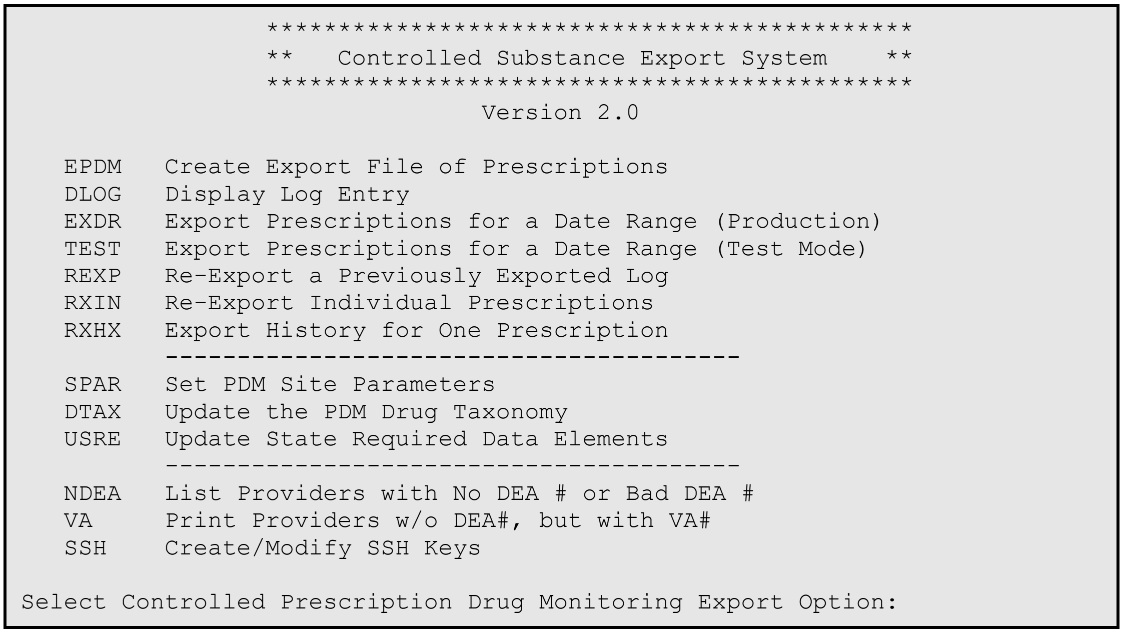
A menu option for editing site parameters is provided in the Controlled Substance Export System. Not all parameters are required by all states. For assistance in learning what is required by your state, contact your state PDM manager or PDM vendor for a description of ASAP message segments used by your state PDM program.

It is the responsibility of each RPMS location to register with their state PDM program and/or PDM vendor. Each RPMS pharmacy division will have a separate entry in the PDM Site Parameters file.

Exports created by this application contain both Personally Identifiable Information (PII) and Protected Health Information (PHI), thus it is imperative that no export files be stored in a public directory. Contact the RPMS Site Manager or other IT specialist to obtain a secure directory in which PDM exports can be stored. When creating the secure directory, permissions must be set correctly such that an RPMS user can write files to the directory. In addition, the individuals responsible for uploading the export file to the state PDM or PDM vendor must be able to navigate or browse to the directory to locate the correct file for upload.

2.0 System Navigation

The Controlled Drug Export System main menu is shown in Figure 2-1. There are 13 items on the primary menu, divided into three sections; Export, Set Up, and Report options. Each menu item is described in detail in a separate section in this manual.



```
                  *********************************************
                  **   Controlled Substance Export System    **
                  *********************************************
                                 Version 2.0

   EPDM   Create Export File of Prescriptions
   DLOG   Display Log Entry
   EXDR   Export Prescriptions for a Date Range (Production)
   TEST   Export Prescriptions for a Date Range (Test Mode)
   REXP   Re-Export a Previously Exported Log
   RXIN   Re-Export Individual Prescriptions
   RXHX   Export History for One Prescription
          ----------------------------------------
   SPAR   Set PDM Site Parameters
   DTAX   Update the PDM Drug Taxonomy
   USRE   Update State Required Data Elements
          ----------------------------------------
   NDEA   List Providers with No DEA # or Bad DEA #
   VA     Print Providers w/o DEA#, but with VA#
   SSH    Create/Modify SSH Keys

Select Controlled Prescription Drug Monitoring Export Option:
```

Figure 2-1: Controlled Drug Export System main menu

2.1 EPDM: Create Export File of Prescriptions

This menu option is used to export a set of prescriptions manually, and is the primary option used to create data files for upload to state PDMPs. A log is kept of all exports so that when this option is run only prescriptions added or edited since the last export are reviewed and exported. This option will export all prescriptions entered or edited since the last export up until the time the export is run.

2.2 DLOG: Display Log Entry

This option will display the information contained in the log for one export. It displays data related to the date range of the export, how many prescriptions were exported, audit information, etc. as well as producing a list of prescriptions in the export file.

2.3 EXDR: Export Prescriptions for a Date Range (Production)

This option is used to export a set of prescriptions in a date range. The only time this option should be used is when you are first starting to use this system and want to send a year's worth of data to "back fill" the database. This option is used to send the data in a production mode. Date Range files will have to be manually uploaded; Auto Upload is not applicable for this option.

2.4 TEST: Export Prescriptions for a Date Range (Test Mode)

This option is used to export a set of prescriptions in a date range in a TEST mode. This option should be used to run test exports of data to the Prescription Monitoring Program (PMP) in order to make sure that the data can be uploaded error free. Date Range files will have to be manually uploaded; Auto Upload is not applicable for this option.

2.5 REXP: Re-Export a Previously Exported Log

This option is used to re-export a set of prescriptions manually. This should only be done if the state rejected an entire file of transactions. Re-exported files will have to be manually uploaded; Auto Upload is not applicable for this option.

2.6 RXIN: Re-Export Individual Prescriptions

This menu option is used to re-export one or more individual prescriptions. This option should be used if the state rejected one or more specific prescriptions due to missing or invalid data. You must specify the record type for each prescription (new, revise, or void).

2.7 RXHX: Export History for One Prescription

This menu option may be used to display the export history for a single prescription.

2.8 SPAR: Set PDM Site Parameters

This menu option is used to display and set up the Site Parameters for each Pharmacy operating on this computer. Each pharmacy that is operational and has an entry in the Outpatient Site file must be entered and site parameters completed.

2.9 DTAX: Update the PDM Drug Taxonomy

When selecting drugs to be exported to the PMP, this application will export all Schedule 2, 3, and 4 drugs, and optionally Schedule 5 drugs. If the site wants to export any other drug, it must enter that drug into the taxonomy called BPDM DRUGS FOR PDM. This menu option allows you to update this drug taxonomy.

2.10 USRE: Update State Required Data Elements

This option is used to update the required data elements for a State Prescription Monitoring Program (PMP). Each pharmacy that is exporting data must use this option to update the State PMP required data elements.

2.11 NDEA: List Providers with No DEA

When exporting prescription data, the prescribing provider's DEA # must be exported. This option allows you to list providers who have prescribed drugs that do not have a DEA # recorded in file 200.

2.12 VA: Print Providers Without DEA# But with VA#

This report option will list all providers on an RPMS database who are authorized to write medication orders, have no DEA # on file, and have data in the VA# field of the New Person File.

2.13 SSH: Create/Modify SSH Keys

This option will allow you to Create/View/Delete Secure Shell (SSH) Keys that are necessary for the Auto Upload feature using Secure File Transfer Protocol (SFTP). You need the BPDMZSSH key to access this option.

3.0 Package Management

This section describes the steps to be followed to set up and use the Controlled Drug Export System.

3.1 Site Parameter Setup

It is imperative that all site parameters are set up for all pharmacies that will be exporting data to the state PMP. Each pharmacy that is operational and is set up in the Outpatient Site must to be entered into the site parameters file. To set up the site parameters:

1. Choose option SPAR – Set PDM Site Parameters. You will be prompted to enter the name of the pharmacy by typing the name as it is entered in the Outpatient Site file.

2. Type a single question mark (**?**) or two question marks (**??**) to display a list of available entries in the Outpatient Site file.

3. Type two more question marks (**??**) to get additional information about what data value should be entered. The parameters displayed may differ depending on which ASAP version is selected.

The first time a site is configured, a mail group will be created for error bulletins. At least one member should be placed in this mail group to receive error bulletins if the export fails. After a site has been configured, the site manager can update members of the mail group.

The mail group will automatically be named BPDM EXPORT MANAGEMENT – XX where XX is the facility's abbreviation in the Location file.

```
Select Controlled Prescription Drug Monitoring Export Option:  SPAR

Select PDM SITE PARAMETERS SITE/LOCATION: DEMO PHARMACY
  Are you adding 'DEMO PHARMACY' as
    a new PDM SITE PARAMETERS (the 1ST)? No// Y  (Yes)

   (Following paragraph displayed on initial installation only)

I am going to set up a mail group so that members of that group.  You can
always update the mail group later using the Mailman options to do so.
Your site manager can also assist in updating a mail group.

Select NEW PERSON NAME: USER,DEMO
Select NEW PERSON NAME:

Your mail group is named:  BPDM EXPORT MANAGEMENT – CIM

SITE/LOCATION: DEMO PHARMACY//

?   Enter pharmacy name from Outpatient Site File
    Answer with OUTPATIENT SITE NAME, or SITE NUMBER, or
```

```
??  This field is a pointer to the Outpatient Site file which is the
primary
    Outpatient Pharmacy Package site parameter file.

INFORMATION SOURCE NAME (IS02): DEMO PHARMACY

?   This is the value that will go into IS02.

??  Value stored in this field is used as the Information Source Entity
    Name, and typically is the name of the pharmacy, eg:DEMO PHARMACY,
    PCHC PHARMACY, etc.  This name does not have to match the PDM Site
    Parameters Site/Location name, although it may.  This field is a
    free-text data type, 1-60 characters

    ASAP Definition:
    IS02 Information Source Entity Name (Required) AN 60
    Entity name of the Information Source.

ASAP VERSION: ASAP 4.2A// ?
     Enter 4.0, 4.1, 4.2, 4.2A, 3.0, or 1995
     Choose from:
       4.0      ASAP 4.0
       4.1      ASAP 4.1
       3.0      ASAP 3.0
       1995     ASAP 1995 (5/95)
       4.2      ASAP 4.2
       4.2A     ASAP 4.2A

??
Enter the version of ASAP (American Society for Automation in Pharmacy)
utilized by your state for PDM submissions.  Acceptable values are 4.0,
4.1, 4.2, 4.2A, 3.0 and 1995.

     Choose from:
       4.0      ASAP 4.0
       4.1      ASAP 4.1
       3.0      ASAP 3.0
       1995     ASAP 1995 (5/95)
       4.2      ASAP 4.2
       4.2A     ASAP 4.2A

STATE: NORTH DAKOTA//

?  Enter the name of the state to receive PDM data.

?? Enter the name of the state to which you are submitting PDM data.  The
   state is usually the same as the state in which the pharmacy is located.

PHONE NUMBER - NUMERIC: 5551231234//

?  Please enter the phone number of the pharmacy, numbers only, 10 digits
   long.  E.g.: 2115551234

?? Enter the Unique Information Source ID as required by your state.
   Typically, this is the telephone number (including area code)
   of the pharmacy ... ten numeric characters only, eg:5051234567.

   This value is used in the IS Segment, data element IS01.

ASAP Definition:
   IS01 Unique Information Source ID (Required) AN 10
   Reference number or identification number as defined
   by the business partners. (Example: Phone number.)

NPI: 6758493022//

?   Please enter your pharmacy's NPI number.

??  Enter your pharmacy's National Provider Identifier (NPI)


ASAP Definition:
    PHA01 National Provider Identifier (NPI) (Situational) AN 10
    Identifier assigned to the pharmacy by CMS.
    Used if required by the PMP.

NCPDP/NABP PROVIDER ID:

?   Answer must be 1-7 characters in length.
NCDPD/NABP Provider ID:

??  Enter the Pharmacy’s NCPDP number. It can be found in the ABSP
    Pharmacies file used by POS.

ASAP Definition:
    PHA02 NCPDP/NABP Provider ID (Situational) AN 7
    Identifier assigned to pharmacy by the National Council
    for Prescription Drug Programs. Used if required by the PMP.

STATE PHARMACY LICENSE NUMBER: ABCD123EFG
 ?   Enter a state license/permit number.  1-20 characters.  This is
intended
     to be the license number for the State listed in the STATE field if
the
     pharmacy is state-licensed.

??   PHA 13 Pharmacy's Permit/License Number (Situational).  This field has
     been added to report the pharmacy's permit number (license number).
It
     is 20 characters AN (alpha numeric).

FACILITY DEA NUMBER: AU1234567//

?   Enter your facility's DEA number

?? The facility DEA number may be used by the state PDM program for
   identification of the pharmacy.  In addition, the facility DEA number
   may be used in lieu of a provider DEA when the provider DEA number field
   in RPMS is not populated.

   ASAP Definition:
   PHA03 DEA Number (Situational) AN 9
   Identifier assigned to the pharmacy by the Drug Enforcement
   Administration.
   Used if required by the PMP.

PHARMACY NAME (PHA04): DEMO PHARMACY

?  Please enter your pharmacy's name (Free text 3-60 characters)

?? If PHA04 segment is required by your PDM state, enter your pharmacy
   name.  Pharmacy name in this field does not need to match the PDM Site
   Parameters Site/Location name, nor does it need to match the name stored
   in the IS02 segment (Information Source Name).

   ASAP Definition:
   PHA04 Pharmacy Name (Situational) AN 60
   Freeform name of the pharmacy.

CONTACT INFORMATON: 3243-2122//

?  Answer must be 1-30 characters in length.

?? When utilized by your state PDM, enter required data, not to exceed 30
   Characters.

   ASAP Definition
   PHA11 Contact name (Situational) AN 30

EXPORT C-5 DRUGS: N - DO NOT EXPORT C-5 DRUGS//

?  Answer yes to include C-5 prescriptions in PDM export

?? If your state requires submission of C-5 prescriptions, answer Yes.

   If your state requires selective C-5 data submission only, use the menu
   option DTAX  Update the PDM Drug Taxonomy, to store the names of C-5
   drugs you wish to have included in your PDM exports.

DEFAULT PHARMACIST: DEMO,PHARMACIST

?  Enter the Pharmacist whose license will be sent to the PMP if a
   technician is the pharmacist of record in the prescription entry.

MAIL FROUP FOR BULLETINS: BPDM EXPORT MANAGEMENT – CIM PHARM

?   Answer with MAIL GROUP NAME

SECURE DIRECTORY FOR FILE: C:\FTP\//

?   Enter secure directory path information, eg: U:\PDM\, /secure/exports/,
    etc.

??  PDM exports contain PII and PHI, and should not be stored in a public
    directory.  Enter the name of the secure directory provided for PDM
    export files.

IS03 SEGMENT DATA VALUE:

?   Answer must be 1-60 characters in length.

??  If IS03 is required by your state, enter the value here.

    IS Information Source Segment - To convey the name and identification
    numbers of the entity supplying the information.

    IS03 is Message (Situational)
    Freeform text message.  Used for more detailed information
 if required by the PDMP.

FILE NAME DESCRIPTOR: PMP_NV_AB1234567//

?    Answer must be 1-30 characters in length.

??   Please enter what you would like the filename to be for the export
```

```
     files.  It cannot contain any spaces.  This will be used as the first
     part of the filename.

     For example, if you are required to use the Pharmacy DEA # in the
     filename, please enter the Pharmacy DEA # in this field, and the
     filename will be pharmdea#_log entry.ext (either .txt or .dat).

    If you want the filename to be descriptive you can enter something like
   "FT.TOTTEN" into this field. The filename would become ft.totten_12.txt
    where the 1st part is the value entered into this field, an underscore,
    the log entry # and the extension as defined in field "Default file
    extension."

DEFAULT FILE EXTENSION: .dat//

?   Please enter T if your PDM vendor requires a .txt file, and D for .dat

??  Enter the extension that is required by the PDM vendor receiving and
    processing your files.

    Allowed values in this field are "T" or "D". If left blank, a .dat file
    will be created.

PDMP PROCESSOR:

?      Answer with PDMP PROCESSORS, or ABBRV
     Choose from:
     ATLANTIC ASSOCIATES, INC
     GOOLD HEALTH SYSTEMS
     HEALTH INFORMATION DESIGNS
     OPTIMUM TECHNOLOGY, INC
     RELAYHEALTH
     STATE SYSTEM

??   Choose from:
     ATLANTIC ASSOCIATES, INC
     GOOLD HEALTH SYSTEMS
     HEALTH INFORMATION DESIGNS
     OPTIMUM TECHNOLOGY, INC
     RELAYHEALTH
     STATE SYSTEM

Select COMPOUND DRUGS: MORPHINE GEL CMPD

?    You may enter a new COMPOUND DRUGS, if you wish
     Enter compounded prescription's controlled substance from Drug File.

  If your pharmacy compounds prescriptions which contain controlled
substances,
  enter the controlled substance from the drug file here.  In addition, you
will
  need to provide the controlled substance ingredient amount per dispense
unit
    (EA, ML or GM).

COMPOUND INGREDIENT QUANTITY: 3.75

?   Enter the amount of controlled substance contained in the compounded
drug per dispense unit (EA, ML or GM).

COMPOUND DRUG DOSAGE UNIT: ML
```

```
?   Enter one of the following: EA, ML or GM

    The above is an example of an extemporaneous compound in which 10ml of
morphine
    15mg/ml was added to 30ml of a gel producing a morphine concentration
of
    3.75mg/ml.

GENERATE ZERO REPORT?: YES
  ?   Should a Zero report be generated and sent to the PDMP?
     Choose from:
       0        NO
       1        YES

  ??    A zero report is a transaction that is sent to the PDMP when there
were
        no controlled substances dispensed during the previous day.

        The usefulness of a Zero Report is to let a state know that no
        controlled substances were dispensed during the required reporting
        period.  The Zero Report would be sent when you normally send a
        batch file for the reporting period.

        In RPMS, a Zero Report reporting period is one full day.

AUTO UPLOAD EXPORT?: ?
     Enter Yes to enable Auto Uploading of the PDM Export
     Choose from:
       0        NO
       1        YES

THE FOLLOWING SETUP IS NEEDED IF YOU ARE USING THE AUTOMATED SECURE FTP
PROCESS.

OPENSSH FOLDER (WINDOWS):
        This is the folder location on Windows where the OpenSSH folder is
located.  Leave this blank for AIX systems.

SFTP SSH KEY FORMAT: OpenSSH Format// ??
        This is the format of the SSH public and private key used

     Choose from:
       OSSH     OpenSSH Format
       SSH2     SSH2 Format
SFTP SSH KEY FORMAT: OpenSSH Format//

SFTP SSH KEY ENCRYPTION: Rivest, Shamir & Adleman
         // ??
        This is the type of encryption algorithm of the SSH

     Choose from:
       DSA      Digital Signature Algorithm
       RSA      Rivest, Shamir & Adleman
SFTP SSH KEY ENCRYPTION: Rivest, Shamir & Adleman
         //

SFTP SERVER IP ADDRESS: 54.175.203.159// ??
        This is the secure FTP IP address of the PDMP processor

SFTP SERVER IP ADDRESS: 54.175.203.159//
SFTP SERVER PORT: ??    THIS CAN BE LEFT BLANK IF THERE IS NOT A SPECIAL
PORT SETUP
        This is the secure FTP port number used by the PDMP processor

SFTP SERVER PORT:

SFTP SERVER DIRECTORY: ME// ??
        This is the directory on the PDMP server that the export file gets
sent to.

SFTP SERVER DIRECTORY: ME//
SFTP USER: xxxxx1234567890@prodpmpSFTP  Replace ??
        This is the name of the userid login to the PDMP processor.

SFTP USER: xxxxx1234567890@prodpmpSFTP  Replace

SFTP RENAME EXPORT FILE: YES// ??
        This field determines whether a backup copy of the export will be
made and reside in the local export directory.

     Choose from:
       0        NO
       1        YES
SFTP RENAME EXPORT FILE: YES//

SFTP KEY FILE: authorized_keys// ??
This is the name of the key file needed for secure FTP and SSH to function
properly.  If this is left blank it will default to authorized_keys.
```

Figure 3-1: Site parameter set up

4.0 Package Operation

This section provides detailed examples of the menu options used by Controlled Drug Export System.

4.1 EPDM: Create Export File of Prescriptions

Use this menu option to manually create PDM export file. A log is kept of all exports so that when this option is run only prescriptions added or edited since the last export are reviewed and exported.

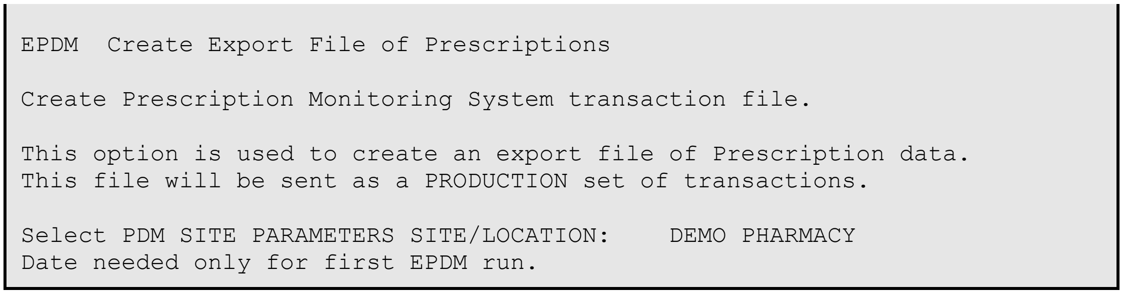
This option describes the following actions:

- Evaluates all prescriptions in the export period checking for prescriptions qualifying for export (DEA Special Handling field of the Drug File contains 2, 3, 4, and possibly 5 or drug is listed in PDM drug taxonomy).
- Checks qualifying prescriptions for errors which would cause a fatal error on upload to PDM processor and generates MailMan bulletin if errors exist.
- If no errors are identified, the PDM export file containing PDM data for qualifying prescriptions dispensed up to COB previous day is created and deposited in the secure directory identified in PDM Site Parameter file.

Once the PDM export file is created, it is the responsibility of facility pharmacy personnel to transmit the file to the state PDM processor in a HIPAA compliant manner.

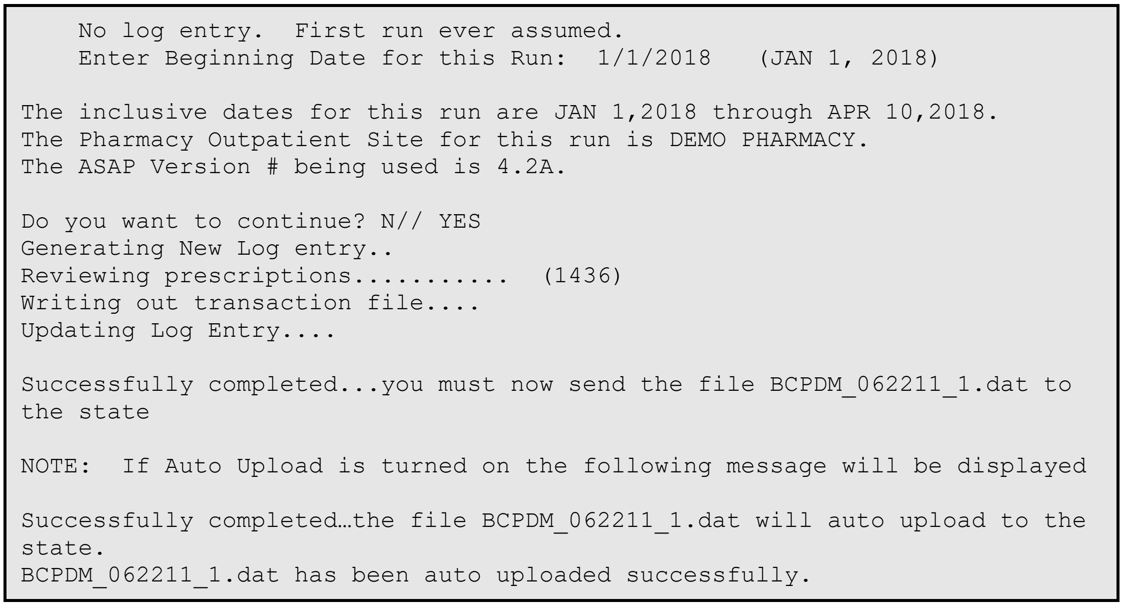
In the example that follows, you are prompted for a beginning date for the export. This will occur only on the initial PDM export, and subsequent exports will use the log of PDM exports to obtain starting date.

```
                  *********************************************
                  **   Controlled Substance Export System    **
                  *********************************************
   EPDM   Create Export File of Prescriptions
   DLOG   Display Log Entry
   EXDR   Export Prescriptions for a Date Range (Production)
   TEST   Export Prescriptions for a Date Range (Test Mode)
   REXP   Re-Export a Previously Exported Log
   RXIN   Re-Export Individual Prescriptions
   RXHX   Export History for One Prescription
           ----------------------------------------
   SPAR   Set PDM Site Parameters
   DTAX   Update the PDM Drug Taxonomy
   USRE   Update State Required Data Elements
           ----------------------------------------
   NDEA   List Providers with No DEA # or Bad DEA #
   VA     Print Providers w/o DEA#, but with VA#
   SSH    Create/Modify SSH Keys

Select Controlled Prescription Drug Monitoring Export Option:  EPDM <enter>
```



```
EPDM  Create Export File of Prescriptions

Create Prescription Monitoring System transaction file.

This option is used to create an export file of Prescription data.
This file will be sent as a PRODUCTION set of transactions.

Select PDM SITE PARAMETERS SITE/LOCATION:    DEMO PHARMACY
Date needed only for first EPDM run.
```

Figure 4-1: Date needed only for the first EPDM run.



```
    No log entry.  First run ever assumed.
    Enter Beginning Date for this Run:  1/1/2018   (JAN 1, 2018)

The inclusive dates for this run are JAN 1,2018 through APR 10,2018.
The Pharmacy Outpatient Site for this run is DEMO PHARMACY.
The ASAP Version # being used is 4.2A.

Do you want to continue? N// YES
Generating New Log entry..
Reviewing prescriptions...........  (1436)
Writing out transaction file....
Updating Log Entry....

Successfully completed...you must now send the file BCPDM_062211_1.dat to
the state

NOTE:  If Auto Upload is turned on the following message will be displayed

Successfully completed…the file BCPDM_062211_1.dat will auto upload to the
state.
BCPDM_062211_1.dat has been auto uploaded successfully.
```

Figure 4-2: PDM export file creation

After creation of a sufficient number of error free reports, the PDM export may be scheduled to run automatically by TaskMan. The following is an example of the TaskMan schedule setup screen.

Note: The name of the pharmacy from the Outpatient Site file must be stored in the Task Parameter field in order for the export to complete properly.

In this patch the export can be run “near real time” instead of once daily. If this is scheduled, the export will run at the time entered and prescriptions from the last successful export until the task runs will be exported. This will run based on the RESCHEDULING FREQUENCY set in the task. The site has the responsibility of determining whether they would like to run a “near real time” export or once daily as is the functionality now. Real time exports can be run as frequently as five minutes if needed.

```
                          Edit Option Schedule
    Option Name: BPDM QUEUE PDM EXPORT
    Menu Text: Queueable Prescription Drug Moni          TASK ID:

__________________________________________________________________________

  QUEUED TO RUN AT WHAT TIME: APR 13,2018@22:00

DEVICE FOR QUEUED JOB OUTPUT:

 QUEUED TO RUN ON VOLUME SET:

      RESCHEDULING FREQUENCY: 1D

             TASK PARAMETERS: DEMO PHARMACY

            SPECIAL QUEUEING:
___________________________________________________________________________
```

Figure 4-3: Example of TaskMan setup for daily PDM export

4.2 DLOG: Display Log Entry

This option will display the information contained in the log for one export. It displays data related to the date range of the export, how many prescriptions were exported, etc. as well as a list of prescriptions exported.

```
         Controlled Prescription Drug Monitoring Export Log Report
2018
                                  Number:   311
                                 Run Date:   Nov 27, 2018@12:23:32
                           Beginning Date:   Oct 28, 2018@00:00:01
                              Ending Date:   Nov 27, 2018@23:59:59
                          Outpatient Site:   PARKER INDIAN HOSP
                              Export Type:   DATE RANGE
                      Transmission Status:   SUCCESSFULLY COMPLETED

   Total Number of Prescriptions Reviewed:   13
          Number of Prescriptions Exported:   7
                          Export Filename:   PARKER_112718_311.dat
                                File Type:   PRODUCTION

AUDIT:
Date: Nov 27, 2018@12:23  User: UESR,DEMO      Option: BPDM EXPORT DATE
RANG
PRESCRIPTIONS EXPORTED:
859937        FT 99999     2       Nov 04, 2018        DOKTOR,IMA MD
      DRUG: TRAMADOL 50MG TAB               PHARMACIST: DEMO,PHARMACIST
861928        FT 99999     2       Nov 01, 2018        DOKTOR,IMA MD
   DRUG: HYDROCODONE & APAP 7.5/500        PHARMACIST: DEMO, PHARMACIST
```

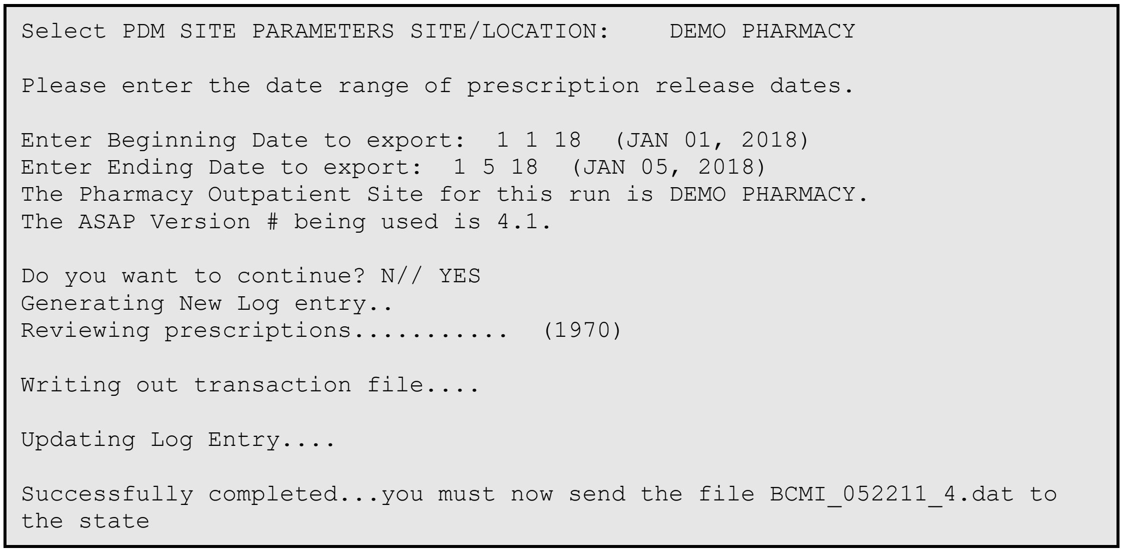
Figure 4-4: Display PDM export log

4.3 EXDR: Export Prescriptions for a Date Range (Production)

Use this option to export a set of prescriptions in a date range. The only time this option should be used is when you first start to use this system and want to “back fill” the database. This option is used to send the data in a production mode. Use the option in Section 4.4 for test file submissions. Date Range files will have to be manually uploaded; Auto Upload is not applicable for this option.

4.4 TEST: Export Prescriptions for a Date Range (Test Mode)

Use this option to export a set of prescriptions in a date range in a TEST mode. This option should be used to run test exports of data to the PDM program in order to make sure that the data can be uploaded error free, or when initiating PDM activities and testing is desired. This option and the previous option, EXDR, export prescriptions for a date range, except the TEST option populates the TH07 file segment with a “T” flag. Date Range files will have to be manually uploaded; Auto Upload is not applicable for this option.

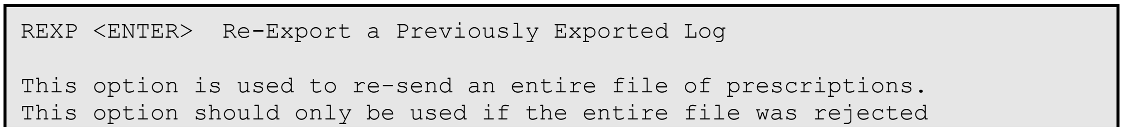


```
Select PDM SITE PARAMETERS SITE/LOCATION:    DEMO PHARMACY

Please enter the date range of prescription release dates.

Enter Beginning Date to export:  1 1 18  (JAN 01, 2018)
Enter Ending Date to export:  1 5 18  (JAN 05, 2018)
The Pharmacy Outpatient Site for this run is DEMO PHARMACY.
The ASAP Version # being used is 4.1.

Do you want to continue? N// YES
Generating New Log entry..
Reviewing prescriptions...........  (1970)

Writing out transaction file....

Updating Log Entry....

Successfully completed...you must now send the file BCMI_052211_4.dat to
the state
```

Figure 4-5: Creation of test file for PDM upload

4.5 REXP: Re-Export a Previously Exported Log

Use this option to re-export a set of prescriptions manually. This should only be done if the state rejected an entire file of transactions. Re-exported files will have to be manually uploaded; Auto Upload is not applicable for this option.



```
REXP <ENTER>  Re-Export a Previously Exported Log

This option is used to re-send an entire file of prescriptions.
This option should only be used if the entire file was rejected
```

```
with a fatal error.  If only some of the prescriptions sent in the
file failed then you should use the option to re-send individual
prescriptions.

Do you wish to continue? N// y  YES
Select PDM SITE PARAMETERS SITE/LOCATION:    DEMO PHARMACY
Select PDM EXPORT LOG DATE RUN: 4/11/18   APR 11, 2018       Jan 1,2018
Apr10,2018

Information for Log Entry 1 Run Date: APR 11,2018

NUMBER: 1                                DATE RUN: APR 11, 2018
  BEGINNING FILL DATE: JAN 01, 2008      ENDING FILL DATE: APR 10, 2018
  # PRESCRIPTIONS REVIEWED: 1843           TOTAL # RECORDS EXPORTED: 642
  FILENAMES CREATED: BCMI34654_1.dat     STATUS: SUCCESSFULLY COMPLETED
  EXPORT TYPE: REGULAR                   FILE TYPE: PRODUCTION
  OUTPATIENT SITE: DEMO PHARMACY

Is this the log you want to re-run? Y// YES
Generating transactions.  Counting records.  (1)

Writing out transaction file....

Updating Log Entry....

Successfully completed...you must now send the file BCMI_063011_1.dat to
the state
```

Figure 4-6: Re-export of entire batch of prescriptions

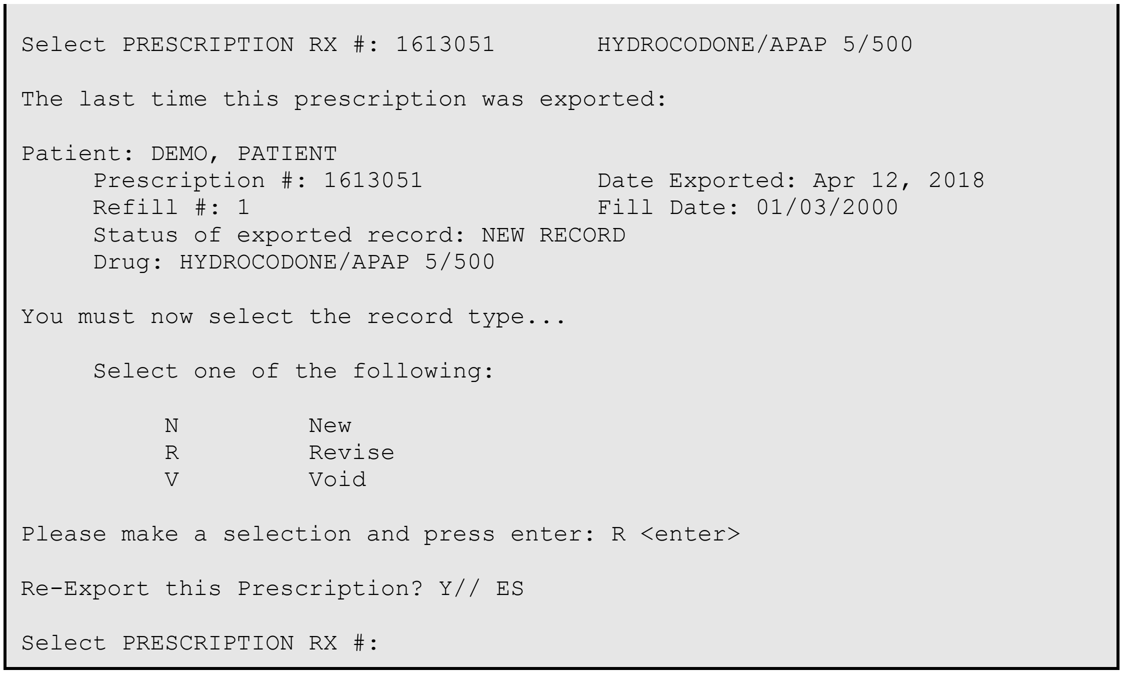
4.6 RXIN: Re-Export Individual Prescriptions

Use this option to re-export one or more individual prescriptions. This option should be used if the state rejected one or more specific prescriptions due to missing or invalid data. Users of the option are expected to specify the record type for the resubmission:

- **New** – if entire record was rejected (aka fatal error)
- **Revise** – if record was accepted, but contained non-fatal error
- **Void** – to expunge a previously accepted prescription transaction from the PDM processor database

Certain RPMS Pharmacy Package actions (Delete Prescription, Return to Stock) will automatically cause a void transaction to be generated and submitted with the next regular export.

```
RXIN  <ENTER>    Re-Export Individual Prescriptions

This option is used to re-send a selected set of prescriptions that
encountered an error when originally transmitted.

Do you wish to continue? N// YES
Select PDM SITE PARAMETERS SITE/LOCATION:    DEMO PHARMACY

Please enter all of the prescriptions that you wish to re-export.
```

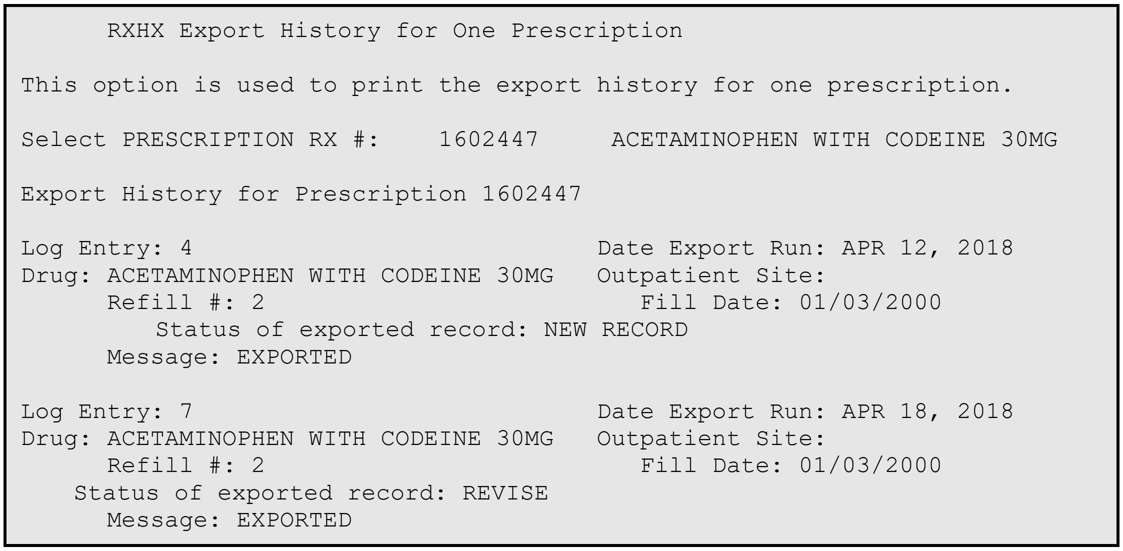


```
Select PRESCRIPTION RX #: 1613051       HYDROCODONE/APAP 5/500

The last time this prescription was exported:

Patient: DEMO, PATIENT
     Prescription #: 1613051            Date Exported: Apr 12, 2018
     Refill #: 1                        Fill Date: 01/03/2000
     Status of exported record: NEW RECORD
     Drug: HYDROCODONE/APAP 5/500

You must now select the record type...

     Select one of the following:

          N         New
          R         Revise
          V         Void

Please make a selection and press enter: R <enter>

Re-Export this Prescription? Y// ES

Select PRESCRIPTION RX #:
```

Figure 4-7: Re-export of individual prescription

4.7 RXHX: Export History for One Prescription

Use this option to display all export activity for an individual prescription.



```
      RXHX Export History for One Prescription

This option is used to print the export history for one prescription.

Select PRESCRIPTION RX #:    1602447     ACETAMINOPHEN WITH CODEINE 30MG

Export History for Prescription 1602447

Log Entry: 4                            Date Export Run: APR 12, 2018
Drug: ACETAMINOPHEN WITH CODEINE 30MG   Outpatient Site:
      Refill #: 2                          Fill Date: 01/03/2000
         Status of exported record: NEW RECORD
      Message: EXPORTED

Log Entry: 7                            Date Export Run: APR 18, 2018
Drug: ACETAMINOPHEN WITH CODEINE 30MG   Outpatient Site:
      Refill #: 2                          Fill Date: 01/03/2000
    Status of exported record: REVISE
      Message: EXPORTED
```

Figure 4-8: Export History for one prescription

4.8 SPAR: Set PDM Site Parameters

Use this option to display set up of the Site Parameters for each Pharmacy operating on this computer. It is described in significant detail in Section 5.1.

When selecting drugs to be exported to the PMP, this application will export all Schedule 1, 2, 3, and 4 drugs, and optionally Schedule 5 drugs. If the site wants to export any other drug, it must enter that drug into the taxonomy called BPDM DRUGS FOR PDM. This menu option allows you to update this drug taxonomy. If your state’s PDM program does not accept C-5 prescriptions, but the state classifies certain C-5 drugs as C-3, they should be included in this taxonomy. See #5 in the taxonomy screen in Figure 4-9.

```
PDM DRUG TAXONOMY UDPATE      Apr 12, 2018 09:21:11   Page:    1 of    1
Updating the BPDM DRUGS FOR PDM taxonomy

________________________________________________________________________
1)  TRAMADOL 50MG TAB
2)  TRAMADOL/ACETAMINOPHEN 37.5MG/325MG TAB
3)  CARISOPRODOL
4)  CARISOPRODOL 350MG TAB
5)  GUAIFENSIN & CODEINE 100/10MG/5ML SYRUP

-          Enter ?? for more actions                                    -

A    Add a Drug           R    Remove a Drug        Q    Quit
Select Action:+//
```

Figure 4-9: Editing BPDM Drugs for PDM taxonomy

4.9 USRE: Update State Required Data Elements

Use this option to update the required data elements for the state PDMP. Any pharmacy that has not exported data using this application must use this option to identify data elements required by their state PDM program.

```
USRE <ENTER>

This option is used to review and update the data elements
that are required by your State when transmitting Controlled Prescription
Drug information to the State.

You should only update those elements that are required by your
State.  If an item is required by ASAP it cannot be changed.

You must have the Site Parameters set up for your site before
using this option.

Select PDM SITE PARAMETERS SITE/LOCATION:    DEMO PHARMACY

BPDM UPDATE STATE REQ ELEMENTS Apr 12, 2018 10:18:47 Page: 3 of 6
Review/Update Required Elements for WISCONSIN
 #    ID        Element Description         Required?
38)    PAT14    PATIENT CITY                 REQUIRED BY ASAP
39)    PAT15    PATIENT STATE                REQUIRED BY STATE
40)    PAT16    PATIENT ZIP                  REQUIRED BY ASAP
41)    PAT17    PATIENT PHONE NUMBER         NOT REQUIRED
42)    PAT18    DOB                          REQUIRED BY ASAP
43)    PAT19    GENDER                       REQUIRED BY STATE
44)    PAT20    SPECIES                      NOT REQUIRED
```

```
45)     PAT21    PATIENT LOCATION CODE        NOT REQUIRED
46)     PAT22    COUNTRY OF NON US RESIDEN    NOT REQUIRED
47)     PAT23    NAME OF ANIMAL               NOT REQUIRED
48)     DSP01    STATUS                       REQUIRED BY ASAP
+         Enter ?? for more actions
E     Edit Required Status     +   Next Screen          Q    Quit
Select Action: +// E   Update Required Status

Edit Which Item:  (1-91): 41
REQUIRED?: NOT REQUIRED// ?
     Choose from:
       R        REQUIRED BY ASAP
       RR       REQUIRED BY STATE
       RWA      REQUIRED WHEN AVAILABLE
       N        NOT REQUIRED
REQUIRED?: NOT REQUIRED// RR <ENTER>
```

Figure 4-10: Changing patient phone number to RR - Required by State

4.10 NDEA: List Providers with No DEA

When exporting prescription data, the prescribing provider’s DEA # is required to be exported. If a provider does not have a DEA#, the facility’s DEA # will be used in addition to the VA # if present. This option allows you to list providers who have prescribed drugs that do not have a DEA # recorded in the New Person File (File 200).

```
          Prescription Providers Without DEA # On File
     Provider Name                      Provider Class           IEN
----------------------------------------------------------------------------
     DEMO,ONE                                                   1725
     DEMO,TWO                                                   1779
     DEMO,THREE                        PHYSICIAN                196
     DEMO,FOUR                                                  1663
     DEMO,FIVE                         OB/GYN                   1017
     DEMO,SIX                          OPHTHALMOLOGIST          974
```

Figure 4-11: Report of providers with no DEA # on file

4.11 VA: Print Providers Without DEA# but with VA#

Most providers authorized to write medication orders will possess a DEA number which will be used in the prescription export record. If a provider does not have a DEA number, the facility’s DEA number will be transmitted with the prescription record, and, if available, the provider’s VA number will be included in the export record. The VA # must be 3 to 10 characters, be unique and not previously used.

```
Select Controlled Prescription Drug Monitoring Export Option: VA

Print Providers w/o DEA#, but with VA#

DEVICE:   Virtual    Right Margin: 80//

Providers w/o DEA # but with a VA #            MAY  5,2018  08:02    PAGE 1
```

```
Provider Name                        VA #
--------------------------------------------------------------------

DEMO,H,                              HA7XXX
DEMO,B.                              BK4XXX
```

Figure 4-12: Report of providers with a VA # number but no DEA #

4.12 SSH: Create/Modify SSH Keys

See Section 5.0 for Auto Upload using Secure FTP. You need the BPDMZSSH key to access this option.

5.0 Auto Upload using Secure File Transfer Protocol

This section provides detailed setup and logging examples for Auto Uploading the export file via SFTP to the PDM processor.

> **Note:** Secure FTP Setup with the PDMP Processor must be accomplished before setting up the RPMS PDM application for Secure FTP (SFTP). This is most likely in the State Processor Guide or you may need to contact them directly.

5.1 SPAR: Set PDM Site Parameters

Use this menu option to setup the SFTP site parameters needed before you can create SSH keys and Auto Upload the PDM Export via SFTP.

Skip through the prompts until you get to the SFTP SSH KEY FORMAT prompt. Follow the prompts and enter the necessary information as shown in Figure 5-1.

```
THE FOLLOWING SETUP IS NEEDED IF YOU ARE USING THE AUTOMATED SECURE FTP
PROCESS.

OPENSSH FOLDER (WINDOWS):
       This is the folder location on Windows where the OpenSSH folder is
located.  Leave this blank for AIX systems.

SFTP SSH KEY FORMAT: OpenSSH Format// ??
        This is the format of the SSH public and private key used

     Choose from:
       OSSH     OpenSSH Format    used for WINDOWS systems
       SSH2     SSH2 Format   used for AIX systems
SFTP SSH KEY FORMAT: OpenSSH Format//

SFTP SSH KEY ENCRYPTION: Rivest, Shamir & Adleman
         // ??
        This is the type of encryption algorithm of the SSH

     Choose from:
       DSA      Digital Signature Algorithm
       RSA      Rivest, Shamir & Adleman    Always use RSA at this time
SFTP SSH KEY ENCRYPTION: Rivest, Shamir & Adleman
         //

SFTP SERVER IP ADDRESS: 54.175.203.159// ??
        This is the secure FTP IP address of the PDMP processor

SFTP SERVER IP ADDRESS: 54.175.203.159//

SFTP SERVER PORT: ??    THIS CAN BE LEFT BLANK IF THERE IS NOT A SPECIAL
PORT SETUP
        This is the secure FTP port number used by the PDMP processor
```

```
SFTP SERVER PORT:

SFTP SERVER DIRECTORY: ME// ??
        This is the directory on the PDMP server that the export file gets
sent
to.

SFTP SERVER DIRECTORY: ME//
SFTP USER: xxxxx1234567890@prodpmpSFTP  Replace ??
        This is the name of the userid login to the PDMP processor.

SFTP USER: xxxxx1234567890@prodpmpSFTP  Replace

SFTP RENAME EXPORT FILE: YES// ??
     This field determines whether a backup copy of the export will be made
and reside in the local export directory.

     Choose from:
       0        NO
       1        YES
SFTP RENAME EXPORT FILE: YES//

SFTP KEY FILE: authorized_keys// ??
        This is the name of the key file needed for secure FTP and SSH to
function properly.  If this is left blank it will default to
authorized_keys.
```

Figure 5-1: Set PDM Site Parameters

5.2 SSH: Create or Modify SSH Keys

Use this menu option to create the SSH private and public key needed for the secure FTP process.

Notes: If your Operating System is Advanced Interactive eXecutive (AIX), you MUST be logged in as the user that will be running the EPDM option or the BPDM QUEUE PDM EXPORT TaskMan option.
You need the BPDMZSSH key to access this option.

This option performs the following actions:

- Checks for the existence of OpenSSH in the folder location that is entered in the OPENSSH FOLDER (WINDOWS) field. If it cannot find the OpenSSH software or the folder is incorrect, it will display a message indicating such and exit the option. ***This is for Windows only.***
- Creates both the private and public SSH keys and stores them in the SECURE DIRECTORY FOR FILE field of the PDM SITE PARAMETER file.
- Displays the key file names stored in the SECURE DIRECTORY FOR FILE location.
- Allows deletion of the SSH keys (if you have OS permissions to do so).

In the example that follows, the deletion, creation, and viewing of the SSH keys is shown.

```
                 *********************************************
                 **   Controlled Substance Export System     **
                 *********************************************
   EPDM   Create Export File of Prescriptions
   DLOG   Display Log Entry
   EXDR   Export Prescriptions for a Date Range (Production)
   TEST   Export Prescriptions for a Date Range (Test Mode)
   REXP   Re-Export a Previously Exported Log
   RXIN   Re-Export Individual Prescriptions
   RXHX   Export History for One Prescription
           ----------------------------------------
   SPAR   Set PDM Site Parameters
   DTAX   Update the PDM Drug Taxonomy
   USRE   Update State Required Data Elements
           ----------------------------------------
   NDEA   List Providers with No DEA # or Bad DEA #
   VA     Print Providers w/o DEA#, but with VA#
   SSH    Create/Modify SSH Keys

Select Controlled Prescription Drug Monitoring Export Option: ssh
Create/Modify
 SSH Keys

Select PDM SITE PARAMETERS SITE/LOCATION:    PARKER INDIAN HOSP

     Select one of the following:

          V         View Public SSH Key
          N         Create New SSH Key Pair
          D         Delete SSH Key Pair

DELETION OF SSH KEYS

     Select one of the following:

          V         View Public SSH Key
          N         Create New SSH Key Pair
          D         Delete SSH Key Pair

Action: V// Delete SSH Key Pair

Confirm Deletion of PARKER INDIAN HOSP's SSH Keys? NO// YES

Deleting SSH Keys...Done

CREATION OF SSH KEYS

     Select one of the following:

          V         View Public SSH Key
          N         Create New SSH Key Pair
          D         Delete SSH Key Pair

Action: V// N  Create New SSH Key Pair

     Select one of the following:
          RSA       Rivest, Shamir & Adleman (RSA)    RSA will always be
used at this time

SSH Key Encryption Type: RSA//   Rivest, Shamir & Adleman (RSA)

Confirm Creation of SSH Keys for PARKER INDIAN HOSP? NO// YES

Creating New SSH Keys, please wait...done

VIEWING OF SSH KEYS

     Select one of the following:

          V         View Public SSH Key
          N         Create New SSH Key Pair
          D         Delete SSH Key Pair

Action: V// iew Public SSH Key

authorized_keys
authorized_keys.pub

Press Return to continue:
```

Figure 5-2: Create or Modify SSH Keys

5.3 Setup Secure FTP on an AIX system

This section describes the process of initial setup of Secure FTP on an AIX system. This includes manually logging into the PDM processor with user credentials, moving the public key to the processor, renaming the public key to the correct name, and modifying the private key ownership and permissions to the appropriate user and permissions.

The following task is most likely done by a site manager or someone with "root" level access to the AIX operating system.

> **Note:** If you have multiple Outpatient Sites using the same credentials to log into your PDM Processor you will to ensure that they SSH Keys are copied to each appropriate folder for that Outpatient Site setup in the SPAR option and that permissions at the AIX level are identical in each folder.

Log on to AIX and change directories to the folder defined in the SECURE DIRECTORY FOR FILE field of the PDM SITE PARAMETERS file. Follow the sequence in Table 5-1 to perform the necessary actions.

Table 5-1: Display Initial Secure FTP Setup in AIX

Sequence	Expected Result
`$ cd /home/BPDM`	Change directories to the folder defined in the SECURE DIRECTORY FOR FILE field of the BPDM SITE PARAMETERS file
`$ SFTP xxxxx1234567890@prodpmpSFTP@54.175.203.159`	Initiate the Secure FTP process using the user stored in the SFTP USER with the IP address stored in the SFTP SERVER IP ADDRESS field of the PDM SITE PARAMETERS file, the SFTP SERVER IP ADDRESS may be a domain name as well

`PAM Authentication`
`Password:`
	Enter the password assigned to this user ID

`Connected to 54.175.203.159.`	This shows you are connected successfully
`SFTP> cd .ssh`	Change directories on the PDM server to .ssh or other defined folder as described in the state user guide
`SFTP> put authorized_keys.pub`	Use the put command to move the public key to the PDM server

`Uploading authorized_keys.pub to /homedir/.ssh/authorized_keys.pub`
`authorized_keys.pub  100%  382 0.4KB/s   00:00`
	This shows the file was uploaded successfully

`SFTP> rename authorized_keys.pub authorized_keys`	Rename the public key to the name of the key required by the PDM processor, in this example we are renaming the key from authorized_keys.pub to authorized_keys
`SFTP> quit`	Use the quit command to exit the PDM processor server
`$ su`	Use root credentials or someone that has full access and credentials for the directory stored in the SECURE DIRECTORY FOR FILE field of the BPDM SITE PARAMETERS file

`root's Password:`
`# chown EPCS authorized_keys`
	Use the chown command to change the file owner to the user that will be logging into the system and will be scheduling the tasked job. NOTE: This step is critical as the Auto Upload will give Permission Denied errors if the owner is not correct.

`# chmod 600 authorized_keys`	Use the chmod command to change permissions to read/write only for the owner of the file

5.4 Set up Secure FTP on a Windows System

This section describes the process of initial setup of Secure FTP on a Windows system. This includes manually logging into the PDM Processor with user credentials, moving the public key to the processor, renaming the public key to the correct name, and modifying the private key ownership and permissions to the appropriate user and permissions.

> **Note:** If you have multiple Outpatient Sites using the same credentials to log into your PDM Processor you will to ensure that they SSH Keys are copied to each appropriate folder for that Outpatient Site setup in the SPAR option and that permissions at the Windows level are identical in each folder.

The following task is most likely done by a site manager or someone with administrator level access to the Windows operating system.

1. Log on to Windows.
2. Open a command prompt.
3. Change directories to the folder defined in the SECURE DIRECTORY FOR FILE field of the PDM SITE PARAMETERS file. Follow the sequence in Table 5-2 to perform the necessary actions.

Table 5-2: Display Initial Secure FTP Setup in AIX

Sequence	**Expected Result**
C:\Users\mwilliams2>cd \pub\BPDM	Use the CD command to change directories to the folder defined in the SECURE DIRECTORY FOR FILE field of the PDM SITE PARAMETERS file
C:\PUB\BPDM>SFTP xxxxx1234567890@prodpmpSFTP@54.175.203.1 59	Initiate the Secure FTP process using the user stored in the SFTP USER with the IP address stored in the SFTP SERVER IP ADDRESS field of the PDM SITE PARAMETERS file, the SFTP SERVER IP ADDRESS may be a domain name as well
PAM Authentication Password: Connected to xxxxx1234567890@prodpmpSFTP@54.175.203.1 59.	
PAM Authentication Password:	Enter the password assigned to this user ID
Connected to 54.175.203.159.	This shows you are connected successfully
SFTP> cd .ssh	Change directories on the PDM server to .ssh or other defined folder as described in the state user guide
SFTP> put authorized_keys.pub	Use the put command to move the public key to the PDM server
Uploading authorized_keys.pub to /homedir/.ssh/authorized_keys.pub authorized_keys.pub 100% 382 0.4KB/s 00:00	This shows the file was uploaded successfully

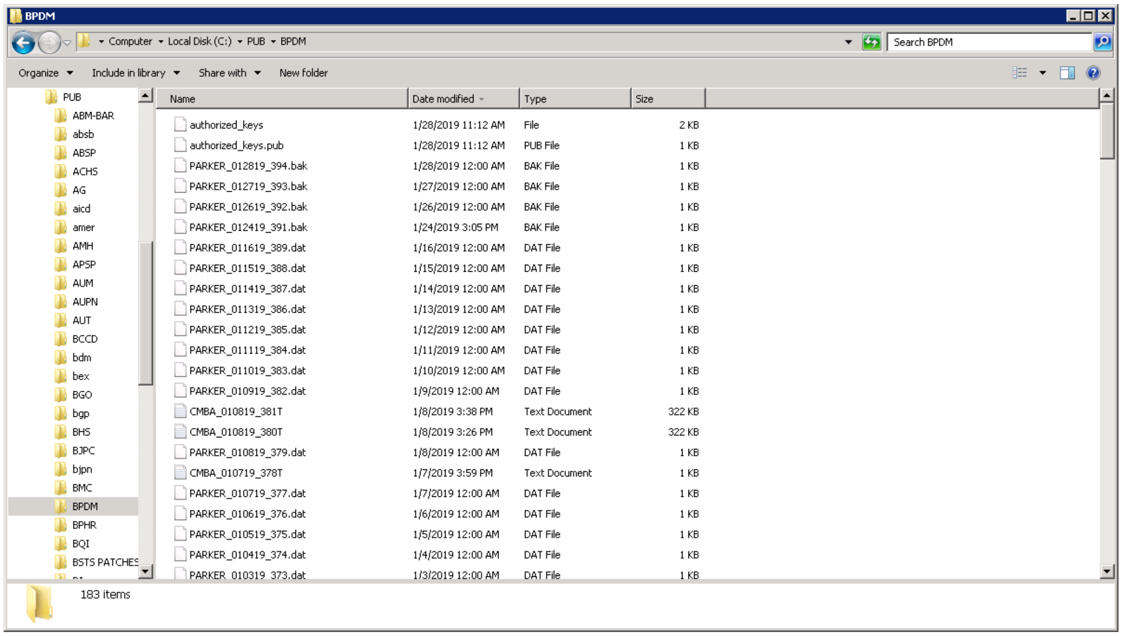
Sequence	Expected Result
`SFTP> rename authorized_keys.pub authorized_keys`	Rename the public key to the name of the key required by the PDM processor, in this example we are renaming the key from authorized_keys.pub to authorized_keys
`SFTP> quit`	Use the quit command to exit the PDM processor server

5.5 Configuring Windows Permissions for the SSH Private Key File

Windows permissions for the private key file need to be changed so that only the user that starts up Ensemble has access to the private key file. Every other user will need to be removed from having access. The user that starts up Ensemble should have Full Control of the private key file. Refer to the figures that follow to accomplish this. In this example we are assuming the user SYSTEM starts Ensemble:

1. Use Windows Explorer to open the folder defined in the SECURE DIRECTORY FOR FILE field of the PDM SITE PARAMETERS file.

2. Locate the private key file as defined in the SFTP KEY FILE field of the PDM SITE PARAMETERS file. In this example the private key is authorized_keys.

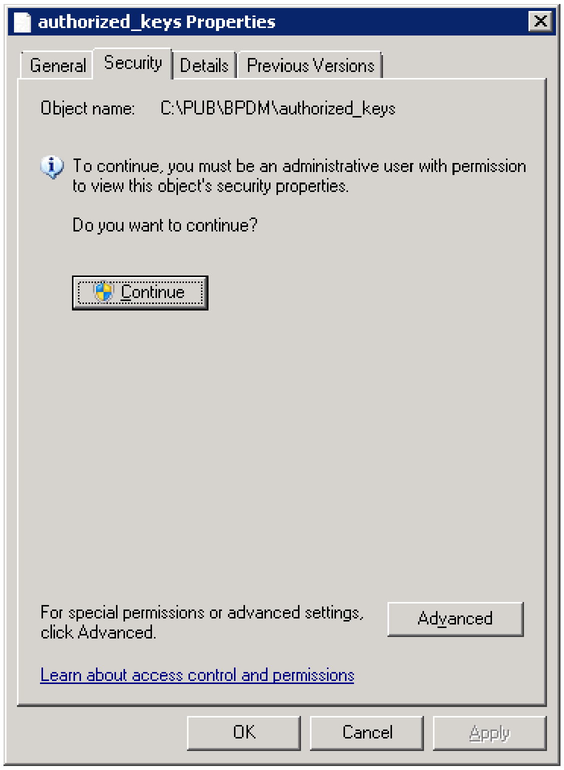


Name	Date modified	Type	Size
authorized_keys	1/28/2019 11:12 AM	File	2 KB
authorized_keys.pub	1/28/2019 11:12 AM	PUB File	1 KB
PARKER_012819_394.bak	1/28/2019 12:00 AM	BAK File	1 KB
PARKER_012719_393.bak	1/27/2019 12:00 AM	BAK File	1 KB
PARKER_012619_392.bak	1/26/2019 12:00 AM	BAK File	1 KB
PARKER_012419_391.bak	1/24/2019 3:05 PM	BAK File	1 KB
PARKER_011619_389.dat	1/16/2019 12:00 AM	DAT File	1 KB
PARKER_011519_388.dat	1/15/2019 12:00 AM	DAT File	1 KB
PARKER_011419_387.dat	1/14/2019 12:00 AM	DAT File	1 KB
PARKER_011319_386.dat	1/13/2019 12:00 AM	DAT File	1 KB
PARKER_011219_385.dat	1/12/2019 12:00 AM	DAT File	1 KB
PARKER_011119_384.dat	1/11/2019 12:00 AM	DAT File	1 KB
PARKER_011019_383.dat	1/10/2019 12:00 AM	DAT File	1 KB
PARKER_010919_382.dat	1/9/2019 12:00 AM	DAT File	1 KB
CMBA_010819_381T	1/8/2019 3:38 PM	Text Document	322 KB
CMBA_010819_380T	1/8/2019 3:26 PM	Text Document	322 KB
PARKER_010819_379.dat	1/8/2019 12:00 AM	DAT File	1 KB
CMBA_010719_378T	1/7/2019 3:59 PM	Text Document	1 KB
PARKER_010719_377.dat	1/7/2019 12:00 AM	DAT File	1 KB
PARKER_010619_376.dat	1/6/2019 12:00 AM	DAT File	1 KB
PARKER_010519_375.dat	1/5/2019 12:00 AM	DAT File	1 KB
PARKER_010419_374.dat	1/4/2019 12:00 AM	DAT File	1 KB
PARKER_010319_373.dat	1/3/2019 12:00 AM	DAT File	1 KB

Figure 5-3: Windows Explorer Window displaying the location of the sample private keys

3. Right-click the private key file and select **Properties**.

4. Select the **Security** tab. If prompted with the following, click **Continue** to proceed.



Object name: C:\PUB\BPDM\authorized_keys

To continue, you must be an administrative user with permission to view this object's security properties.

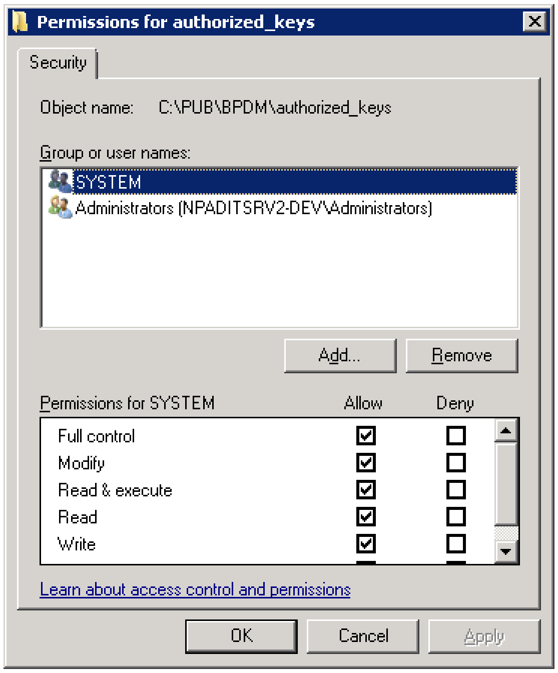
Do you want to continue?

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

Figure 5-4: Private key properties Security tab

The permissions for the private key file are displayed similar to the following:



Object name: C:\PUB\BPDM\authorized_keys

Group or user names:

- SYSTEM
- Administrators (NPADITSRV2-DEV\Administrators)

Permissions for SYSTEM	Allow	Deny
Full control	☑	□
Modify	☑	□
Read & execute	☑	□
Read	☑	□
Write	☑	□

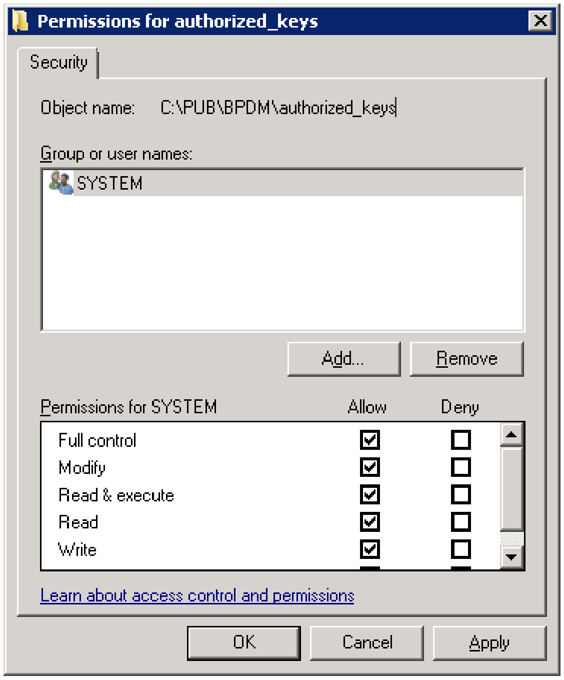
Learn about access control and permissions

Figure 5-5: Private key properties Security Permissions

5. Click any user except for the one that starts Ensemble. In this example, SYSTEM starts Ensemble. So we want to remove Administrators from having access to this file.

6. Select the **Administrators** user.

7. Click **Remove**. The permissions screen should now look like Figure 5-6.



Permissions for authorized_keys

Object name: C:\PUB\BPDM\authorized_keys

Group or user names:
SYSTEM

Permissions for SYSTEM	Allow	Deny
Full control	☑	□
Modify	☑	□
Read & execute	☑	□
Read	☑	□
Write	☑	□

Figure 5-6: Private key properties Security Permissions after modifications

8. Click **OK** to save the permissions.

9. Click **OK** at the following private key properties window.

You are now ready to begin using the Auto Upload Secure FTP process.

5.6 Testing the Auto Upload Secure FTP process

Confirm the following steps have been accomplished:

- Secure FTP parameters have been setup in the PDM SITE PARAMETERS file.
- The AUTO UPLOAD EXPORT field in the PDM SITE PARAMETERS file is set to YES.
- OpenSSH has been installed (***Windows only***) and the folder where it is installed is in the OPENSSH FOLDER (WINDOWS) field via the SPAR option.
- SSH Keys have been generated and are located in the folder defined in the SECURE DIRECTORY FOR FILE field of the PDM SITE PARAMETERS file.

- The private SSH key has been manually uploaded to the PDM processor and named correctly as defined by the PDM processor.
- Permissions have been set correctly as described in Section 5.3 for AIX systems and in Sections 5.4 and 5.5 for Windows systems.

From the Controlled Prescription Drug Monitoring Export menu, use the EPDM option as described in Section 4.1. You may need to enter a sample prescription before running this option.

The following is a sample session:

```
Select PDM SITE PARAMETERS SITE/LOCATION:    DEMO PHARMACY

Create Export File of Prescriptions

Create Prescription Monitoring System transaction file.

This option is used to create an export file of Prescription data.
This file will be sent as a PRODUCTION set of transactions.

Select PDM SITE PARAMETERS SITE/LOCATION:    PARKER INDIAN HOSP

Last run was for JAN 27,2019@00:00:01 through JAN 27,2019@23:59:59.

The inclusive dates for this run are JAN 27,2019@23:59:59 through JAN
28,2019@11:44:16.
The Pharmacy Outpatient Site for this run is PARKER INDIAN HOSP.
The ASAP Version # being used is 4.2A.

Do you want to continue? N// YES

Generating New Log entry..
Reviewing prescriptions...........  (1)

Writing out transaction file....

Updating Log Entry....

Successfully completed...the file PARKER_012819_395.dat will auto upload to
the state.

PARKER_012819_395.dat has been auto uploaded successfully
```

Figure 5-7: Creation of test file for PDM upload

> **Note:** The last line indicates that the file has been auto uploaded successfully.

The following message is displayed if the file is not uploaded successfully:

> PARKER_012819_396.dat was NOT uploaded successfully, see log entry 395 for details (file name and log entry will be different based on your system and settings.

Use the DLOG – Display Log Entry option to display the log. See the log entry for the example in Figure 5-8.

```
Select Controlled Prescription Drug Monitoring Export Option: DLOG  Display
Log

Display Controlled Prescription Drug Monitoring Export Log Entry

Select PDM SITE PARAMETERS SITE/LOCATION:    PARKER INDIAN HOSP
Select PDM EXPORT LOG DATE RUN: `395  1-28-2019@11:48:22     Jan
27,2019@23:59:5
9     Jan 28,2019@11:43:13

     Select one of the following:

          B         BROWSE Output on Screen
          P         PRINT Output to Printer

Do you want to: B// PRINT Output to Printer
DEVICE: HOME// 0;80;9999999  Virtual

Controlled Prescription Drug Monitoring Export Log Report
       Information for Log Entry 395 Beginning Date:  Jan 28, 2019@11:48:22

                                   Number:   395
                                 Run Date:   Jan 28, 2019@11:48:22
                           Beginning Date:   Jan 27, 2019@23:59:59

                              Ending Date:   Jan 28, 2019@11:43:13
                          Outpatient Site:   PARKER INDIAN HOSP
                              Export Type:   REGULAR
                      Transmission Status:   SUCCESSFULLY COMPLETED

   Total Number of Prescriptions Reviewed:   1
          Number of Prescriptions Exported:   1
                          Export Filename:   PARKER_012819_395.dat
                                File Type:   PRODUCTION

AUDIT:
Date: Jan 28, 2019@11:48  User: DEMO,USER      Option: BPDM EXPORT
TRANSACTI

SFTP LOG:
```

Figure 5-8: Display Log Entry

> **Note:** This section is a capture of the Secure FTP process. If you do not see any errors indicating that the process failed then the process completed successfully. Figure 5-9 shows a successful transmission.

```
SFTP> cd ME
SFTP> put c:\pub\bpdm\PARKER_012819_395.dat

PRESCRIPTIONS EXPORTED:
1486289       TST 103193   4       Jan 28, 2019        DEMO, USER
```

```
   DRUG: ALPRAZOLAM 0.25MG TAB            PHARMACIST: DEMO, PHARMACIST
```

Figure 5-9: Display Log Entry (continued)

Appendix A: PDM Setup Checklist

In order to perform the PDM application setup, numerous codes and other data must be available including:

- RPMS name of pharmacy: This is the pharmacy application name in the Outpatient Site file (File #59). It does not have to match the RPMS location file entry, and multiple pharmacy names may exist on one RPMS computer.
- ASAP version (4.0, 4.1, 4.2, 4.2A, 3.0 or 1995) used by the state to which PDM transactions are being submitted.
- Pharmacy phone number.
- Pharmacy NPI number.
- Pharmacy DEA number.
- Pharmacy NCPDP number.
- Pharmacy state license number (when applicable).
- Secure directory in which to save PDM files.
- Export file name descriptor. This is the name of the export file to which a date, log number, and file extension will be appended.
- File extension required by PDM vendor, usually .dat or .txt.
- DEA #: Prior to creation of the facility's first PDM export, provider DEA numbers should be reviewed. Use the PDM packages option to list providers without DEA numbers as well as checking existing DEA numbers for compliance with the DEA number algorithm.
- VA #: If a provider does not have a DEA number, a VA number should be created and entered into the New Person File (File 200). You may need assistance from your site manager or other RPMS support person in order to edit the VA number field. It is up to the facility to create the VA number, which must be unique, 3-10 characters and not previously used for another provider. Many sites concatenate the provider's SSN "last four" to the provider's initials. For example, Dr Vinnie Boombah's VA number might be VB7343.
- The PDM export file may contain a patient identifier which uses the Health Record Number (HRN). It is important that the value in your pharmacy's entry in the Outpatient Site file's Related Institution field match the RPMS division you selected at login.

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 (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

- Use 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

Browser

An interactive application that displays ASCII text on a terminal that supports a scroll region. The text can be in the form of a word-processing field or sequential local or global array. The user is allowed to navigate freely within the document.

Callable

Entry Points in a routine that can be called from an application program.

Default Response

Many of the prompts in the Controlled Drug Export System contain responses that can be activated simply by pressing the Enter key. For example: “Do you really want to quit? No.” Pressing the Enter key tells the system you do not want to quit. “No” is considered the default response.

Device

The name of the printer to use when printing information. Home means the computer screen.

Entry Point

A point within a routine that is referenced by a “DO” or “GOTO” command from a routine internal to a package.

Fields

Fields are a collection of related information that comprises a record. Fields on a display screen function like blanks on a form. For each field, the application displays a prompt requesting specific types of data.

File

A set of related records or entries treated as a single unit.

FileMan

The database management system for RPMS.

Free Text Field

This field type will accept numbers, letter, and most of the symbols on the keyboard. There may be restrictions on the number of characters that are allowed.

Global

In MUMPS, global refers to a variable stored on disk (global variable) or the array to which the global variable may belong (global array).

INDEX (%INDEX)

A kernel utility used to verify routines and other MUMPS code associated with a package. Checking is done according to current ANSI MUMPS standards and RPMS programming standards. This tool can be invoked through an option or from direct mode (>D ^%INDEX).

Information Resource Management

The IHS personnel responsible for information systems management and security.

Kernel

The set of MUMPS software utilities that function as an intermediary between the host operating system and application packages, such as Laboratory and Pharmacy. The kernel provides a standard and consistent user and programmer interface between application packages and the underlying MUMPS implementation. These utilities provide the foundation for RPMS.

Menu

A list of choices for computing activity. A menu is a type of option designed to identify a series of items (other options) for presentation to the user for selection. When displayed, menu-type options are preceded by the word “Select” and followed by the word “option,” as in “Select Menu Management option:” (the menu’s select prompt).

Mnemonic

A short cut designated to access a particular party, name, or facility.

National Drug Code

A medical code set maintained by the Food and Drug Administration, which contains codes for drugs that are FDA-approved. The Secretary of HHS adopted this code set as the standard for reporting drugs and biologics on standard transactions.

Option

An entry in the Option file. As an item in a menu, an option provides an opportunity for users to select it, thereby invoking the associated computing activity. Options may also be scheduled to run in the background, noninteractively, by TaskMan.

Queuing

A request that a job be processed at a later time rather than within the current session.

Routine

A program or sequence of instructions called by a program that may have some general or frequent use. MUMPS routines are groups of program lines that are saved, loaded, and called as a single unit via a specific name.

Taxonomy

Taxonomies are groupings of functionally related data elements, such as specific codes, code ranges, or terms, that are used by various RPMS applications to find data items.

User Class Identification

A computing area.

Utility

A callable routine line tag or function. A universal routine usable by anyone.

Variable

A character or group of characters that refers to a value. MUMPS recognizes three types of variables: local variables, global variables, and special variables. Local variables exist in a partition of the main memory and disappear at signoff. A global variable is stored on disk, potentially available to any user. Global variables usually exist as parts of global arrays.

Acronym List

Acronym	Meaning
AIX	Advanced Interactive eXecutive
ASAP	American Society for Automation in Pharmacy
DEA	U.S. Drug Enforcement Administration
HIPAA	Health Insurance Portability and Accountability Act
IHS	Indian Health Service
PDM	Prescription Drug Monitoring
PDMP	Prescription Drug Monitoring Program
PHI	Protected Health Information
PII	Personally Identifiable Information
PMP	Prescription Monitoring Program
RPMS	Resource and Patient Management System
SFTP	Secure File Transfer Protocol
SSH	Secure Shell

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