RESOURCE AND PATIENT MANAGEMENT SYSTEM

IHS Pharmacy-Automated Dispensing Interface System

(BOP)

User Manual

Version 1.0 Patch 4
September 2025

Office of Information Technology
Division of Information Technology

Table of Contents

Preface

This manual provides information regarding the use of the IHS Pharmacy-Automated Dispensing Interface System (BOP).

1.0 Introduction

The IHS Pharmacy Automated Dispensing Interface System sends RPMS patient data and medication orders to the Automated Dispensing System in real-time, as transactions occur.

The network administrator determines the **TCP/IP** addresses, an **IP** address for each Automated Dispensing System automated medication dispensing system, and an **IP** address for each RPMS IHS facility.

When an Automated Dispensing System is installed, Automated Dispensing System site engineers and local RPMS staff determine which medications will be stored and dispensed from the Automated Dispensing System. Users then map the Automated Dispensing System medication formulary to the **RPMS Drug** file, using the **Internal Entry Number (IEN)** of the records from the **RPMS Drug** file.

RPMS staff determines the types of medications that will be dispensed by the Automated Dispensing System automated medication dispensing system as well as the types of patients (**Inpatients**, **Outpatients**).

The next step is to initialize the Automated Dispensing System automated medication dispensing system database with RPMS patients and orders.

The final step to beginning live interface activity is started by initializing the **BOP Monitor**. This process makes sure that a sender and receiver are always ready to receive and transmit **HL7** messages across the interface.

2.0 Functionality

- Data in the **BOP QUEUE** file is placed into HL7 messages and transmitted to the Automated Dispensing System via **TCP/IP** protocol. The RPMS system always acts as the client and initiates a connection to the Automated Dispensing System.
- RPMS provides the ability to toggle the interface transmissions **On** or **Off** for Inpatient or Outpatient activity. These toggles are located in the RPMS **BOP Site Parameter** file.
- There is a list of **Outpatient Admitting Areas**. This list may be used to filter patient information that will be sent to the Automated Dispensing System. If the list is empty and the field **Send All Outpatients** is set to **No**, no Outpatients whose registration activity activates an interface call will be transmitted to the Automated Dispensing System. If there are any entries, no patient will be sent across the interface unless its **Admitting Area** is in the list. Since the **Admitting Area** is only asked if the **ADT ACTIVE** flag is set to **YES** in the **Record Tracking System Parameters** file, the interface operations instructions will discuss this in detail and give examples.
- If Outpatient data is to be sent, and the RPMS facility would like to have an RPMS visit file record created when the Outpatient is admitted through the **SD IHS WALK-INS** option, then the field **Create Visit At Check In** (in the **Hospital Location** file) should be set to **YES**.
- Uses **TCP/IP**[i] to transmit and receive data.
- Monitors itself and reliably keeps itself running.
- Transmits **ADT** to the Automated Dispensing System automated medication dispensing system real-time.
- Transmits patient orders to the Automated Dispensing System automated medication dispensing system real-time.
- Can be used to transmit patient information in a batch mode to initialize the Automated Dispensing System automated medication dispensing system.
- Reports on queues into which data is put for transmission. The **Queue** file (**90355.1**) will now store the actual transmission data in the **O** node. It will retain the actual HL7 data message that is transmitted.
- Can be started and stopped by users using easy to access options on their menu.

[i] Makes socket to socket connection, Send and receives HL7 Messages. HL7 messages are structured as followed: $C(11) = first byte == HL7 Message (each segment ends with $C(13)) == and each HL7 message ends with $C(28,13). Each message is followed by an exchange of HL7 Acknowledgements. The TCP/IP process keeps channel opened constantly.

- Can be parameterized to meet specific site needs.
- Can work with multiple room/bed coding combinations for patient locations.
- Self maintains its file with its purge routine.

2.1 Data Transmitted from RPMS

- **ADT:** When a patient is admitted, discharged, or transferred an ADT transaction may be sent to the interface for transmission to the Automated Dispensing System
  - Dependent on patient's location being configured as an Automated Dispensing System location.
- **Outpatient Demographic Data:** Transmitted to the Automated Dispensing System if Outpatient locations are included in the site parameters or if the field **Send All Outpatients** in the parameter file is set to **YES**.
- **Orders:** When the order type has been set to **YES** for sending to the Automated Dispensing System.
  - Types of orders that can be configured for transmission: PRN, Continuous, One-Time, Fill-On-Request, On-Call, New Orders, Renewed Orders, Other Orders, Inpatient Meds for Outpatient (IMO), and IV Orders

3.0 Menu

The Interface menus provide control over the interface. Two menus are released with the interface, **BOP USER MENU** and **BOP IRM MENU**. Below are the option names descriptions:

3.1 Option List for the BOP User Menu [BOPMENU]

Users require the security key **BOPZUSER** to use this menu (Figure 3-1). The following options can be accessed through this menu:

```
PAT Display Queue for a patient
SEND Send One Patient ADT/Orders to Interface
SHOW Show Ready Queue
SITE Site Parameter Edit
TRB Interface Trouble Shooting . . .
```

Figure 3-1: BOP User Menu

- **Display Queue for a Patient (PAT) [BOP PATIENT DISPLAY]**. Abbreviation **PAT**. This option is used to display the transactions in the sending queue for a particular patient.
- **Send one patient (DFN) ADT & orders to Automated Dispensing System (SEND) [BOP TRANSMIT ONE PATIENT]**. Abbreviation **SEND**. This option is often used to force ADT and Order transactions across the interface. If an ADT or order did not make it to the interface, this option allows the sending of all of that patient’s current orders to the Automated Dispensing System. The patient **IEN (DFN)** is entered and if the patient’s location is a sending location the patients ADT information and all orders for that patient are sent.
- **Show Ready Queue (SHOW) [BOP SHOW]**. Abbreviation: **SHOW**. This option displays the status of the sending queue. The display shows the total number of items in the queue file, how many are ADT, how many are Orders, and how many timing transactions from Automated Dispensing System.
- **BOP Site Parameters (SITE) [BOP SITE]**. Abbreviation: **SITE**. This option allows users to edit the **BOP SITE** parameters.
- **Interface Trouble Shooting… (TRB) [BOP TROUBLE MENU]**. Abbreviation: TRB. Within this Menu, there are **3** options:
  - Check the Automated Dispensing System log file **(CHK) [BOP CHECK TRANSACTIONS]**.
  - Display future **Automated Dispensing System Monitor** tasks **(FUT) [BOP FUTURE TASK LIST]**.
  - Display running task and job ID **(RUN) [BOP RUN TASK LIST]**.

There are times when the interface will have nothing to send. At that time, it will create a future **Automated Dispensing System Monitor** task scheduled for **5** to **15** minutes in the future. If you see **a Future Task**, it means the interface is running but completed its processing and will check for more processing at the time listed in TaskMan.

The **CHK** option will show the actual numbers in the **Queue** file that are waiting to be sent. If there are entries in that file and the numbers do not change, contact IRM and let them know.

3.2 Option List for the BOP IRM Menu

The following options (Figure 3-2) can be accessed through this menu.

```
MON Start the Monitor
PAT Display Queue for a patient
PURG Purge Queue File
SEND Send One Patient ADT/Orders to Interface
SHOW Show Ready Queue
SITE Site Parameter Edit
STOP Stop the Interface
TRB Interface Trouble Shooting ...
```

Figure 3-2: BOP IRM Menu options

- **Start the Monitor (MON) [BOP MONITOR]**. Abbreviation **MON**. This option starts the **BOP interface monitor**. The monitor constantly checks the system to see if the appropriate jobs are running. If it finds that a necessary process is not running, it schedules it to run using the RPMS Task Manager. The monitor process reschedules itself using the RPMS background task scheduler, TaskMan. It will run **'X'** seconds in the future, (determined by the field **Reschedule Frequency** in the **IHS BOP Site Parameters** file, **#90355** –Recommend 300 to 900 seconds). When it runs it checks to see if the transmitter to Automated Dispensing System and receiver from Automated Dispensing System are running and attempts to start them if they are not running.
- **Display Queue for a patient (PAT) [BOP PATIENT DISPLAY]**. Abbreviation **PAT**. This option is used to display the transactions in the sending queue for a particular patient.
- **Purge BOP Queue (PUR) [BOP PURGE]**. Abbreviation **PUR**. This option removes old data from the **Automated Dispensing System Queue**. Entries that are less than **7** days old are ignored. Purging old transmissions from the queue file is an important item and controls the amount of space on the system that the interface uses.

- **Send one patient (DFN) ADT & orders to Automated Dispensing System (SEND) [BOP TRANSMIT ONE PATIENT]**. Abbreviation **SEND**. This option is often used to force **ADT** and **Order** transactions across the interface. If an ADT or order did not make it to the interface, this option allows the sending of all of that patient's current orders to the Automated Dispensing System. The patient **IEN (DFN)** is entered and if the patient's location is a sending location the patients ADT information and all orders for that patient are sent.
- **Show Ready Queue (SHOW) [BOP SHOW]**. Abbreviation: **SHOW**. This option displays the status of the sending queue. The display shows the total number of items in the queue file, how many are ADT, how many are Orders, and how many timing transactions from Automated Dispensing System.
- **BOP Site Parameters (SITE) [BOP SITE]**. Abbreviation: **SITE**. This option allows users to edit the **BOP SITE** parameters.
- **Stop the BOP interface (STOP) [BOP STOP]**. Abbreviation: **STOP**. The interface can be stopped in two ways. The first is to edit the setup file and change the monitor active field (file **90355**) from **ON** to **OFF**. This will stop the monitor so that the monitor will not reschedule itself in TaskMan. This does not stop the current running transmitter or receiver. The second way to stop the interface is to use the Stop the BOP Interface option. This option will halt the current running transmitter and receiver but does not interfere with the interface monitor. Use this option if the interface needs to be stopped for a short while but not permanently.
- **BOP TROUBLESHOOT MENU (TRB) [BOP TROUBLESHOOT MENU]**. Abbreviation: **TRB**. Within this Menu, there are **3** options:
  - **CHK Check the Log File [BOP CHECK TRANSACTIONS]**
  - **FUT Display Future Monitor tasks [BOP FUTURE TASK LIST]**
  - **RUN Display Running Tasks and job ID [BOP RUN TASK LIST]**

There are times when the interface will have nothing to send. At that time, it will create a future **BOP Monitor** task scheduled for **3** to **15** minutes in the future. If you see a **Future Task**, it means the interface is running but completed its processing and will check for more processing at the time listed in TaskMan.

The **CHK** option will show the actual numbers in the **Queue** file that are waiting to be sent. If there are entries in that file and the numbers do not change, contact user support.

4.0 Site Parameters

The **BOP Site Parameter File (90355)** is used to define how the interface will work. The user may determine:

- If ADT should go to the Automated Dispensing System.
- Which divisions will be allowed.
- If Outpatients' data should be sent.
- Which orders are active.
- Which order types should be sent.
- If the interface is active.
- IP addresses and their respective sockets (ports) for each hospital division.
    - Each division goes to a different **pro-car**.
    - The **pro-car** is the Automated Dispensing System interface receiver. It then sends the transmission to the appropriate Automated Dispensing System console.

4.1 BOP Site Parameters

- **Name:** Your **Site Name** from the institution **file #4**.
- **Facility ID:** Your **Site Number** from the institution **file #4**.
- **Receiving Application:** Which vendor are you interfacing to. Options are **Omnicell** or **Pyxis**.
- **Acknowledgment Time Out:** Number of seconds between **5** and **180**.
- **Number of Retries:** Number of tries between **5** and **10**.
- **ADT Active:** Enter **YES** if sending admission information. Enter **NO** if not sending admission information.
- **ADT Send Inpatient:** Enter **YES** if sending **Inpatient ADT** information.
- **ADT Send Outpatient:** Enter **YES** if sending **Outpatient ADT** information.
- **INPATIENT MEDS FOR OUTPATIENT**: Enter **YES** if you want to send IMO to Automated Dispensing Interface or **NO** otherwise
- **SEND IV ORDERS:** Enter **YES** to transmit IV Orders or **NO** otherwise
- **Admit Diagnosis:** Enter **YES** if sending the free text **short admit diagnosis**.
- **Send PRN:** Enter **YES** if sending **PRN** orders.
- **Send Continuous:** Enter **YES** if sending continuous orders.
- **Send One-Time:** Enter **YES** if one-time orders are to be sent.

- **Send Fill-On-Request:** Enter **YES** if sending fill on request orders.
- **Send On-Call:** Enter **YES** if sending on call orders.
- **New Orders Active:** Enter **YES** if sending new orders.
- **Renew Orders Active:** Enter **YES** if sending re-new orders.
- **Other Orders Active:** Enter **YES** if sending other orders.
- **Send Formulary:** Enter **YES** if updates to the drug file are to go to the remote system.
- **Processing ID: P** The processing id is always set to **P**.
- **Version ID: 2.3** The **Version ID** is for the version of the HL7 standard interface document followed.
- **P-O Interface Domain:** Enter the domain name for your site. From **^XMB("NETNAME")**.

> **Important:** This will be different in test versus live. Remember when you put the data into live to change this field!

- **Interface Vendor:** Enter **O** for **OmniCell** or **P** for **Pyxis**.
- **Base Allergy:** Leave blank or select **Other Allergy/Adverse Reaction**.
- **Location Decoding Type:** Enter the appropriate style for room bed to be sent to the Automated Dispensing System.
- **Send All Outpatients:** If **YES**, all Outpatient transactions will be sent regardless of location.

> **Note:** If this field is set to **YES**, but the **Location** is not found in the **Outpatient Location multiple** (below), the **Outpatient ADT** information will be sent, but the **Location** associated with it will be the **Default OP Send Location** (above).

- **Default Outpatient Location:** If Outpatients are to be sent what is the default location.
- **Default OP Send Location:** Default map value agreed with Automated Dispensing System. Used when **Location** cannot be found in the **Outpatient Location multiple** (below).
- **Default OP Location Pointer:** Pointer to **Hospital Location file (44)**.

4.1.1 Multiple For Outpatient Areas

To ensure best data, enter all **Outpatient** locations that will send ADT information.

> **Note:** If **Send All Outpatients** is set to **YES**, but the location is not defined below, the transaction will be sent using the **Default OP Send Location**.

- **Outpatient Location:** The free-text partial match to the **.01** field in **file 44 Outpatient Location** that can send to the Automated Dispensing System.
- **OP Send Location:** Enter the **map value** for the **Outpatient Location** that will be sent to the Automated Dispensing System.
- **OP Location Pointer:** The pointer to **file 44** for the **Outpatient Location** that can send to Automated Dispensing System. Externally the user will see the full name of the location from **file 44**.
- **Monitor Active:** This field controls whether the **BOP** interface continues to run.
  - Set this to **OFF**. When ready to begin testing or go-live, complete the following:
    1. Perform **Connectivity Check (CALL^%ZISTCP)** refer to Section 6.0, Troubleshooting.
    2. If you have connectivity, change **Monitor Active** to **ON**.
    3. Use **BOP MONITOR** to start up interface.
    4. Run **Pre-seed ^BOPTSD**. This has to be run from the mumps level.
- **Monitor Rescheduling Frequency:** Frequency to check the interface monitor. Select frequency between **120** to **3600** seconds.
- **Stop:** Used to stop the interface.

4.1.2 Multiple Receiving Facilities

- **Receiving Facility:** Enter the **name** for the receiving facility (from **Medical Center Division file #40.8**)
- **Channel Active:** Enter **YES** if sending to the Automated Dispensing System.
- **Accept Transactions:** Enter **YES** if accepting transactions for sending to the Automated Dispensing System.
- **Client or Server:**
  - Enter **CLIENT** if your side is to initiate contact with the Automated Dispensing System.
  - Enter **SERVER** if your side is to listen to the Automated Dispensing System.
- **IP Address:** Enter the **IP address** of the Automated Dispensing System. (determined by information systems).

- **Send Socket:** Enter the **socket number** that will be used to send to the Automated Dispensing System.
- **Receive Socket:** Enter the socket number that will be used to receive from the Automated Dispensing System.

4.2 Sample BOP Site Parameters

```
OUTPUT FROM WHAT FILE: 90355 BOP SITE PARAMETERS
NAME: IHS DEMO HOSPITAL                 FACILITY ID: 100
  ACKNOWLEDGEMENT TIME OUT: 5           NUMBER OF RETRIES: 5
  SEND PRN: YES                         SEND CONTINUOUS: YES
  SEND ONE-TIME: YES                    SEND FILL-ON-REQUEST: YES
  SEND ON-CALL: YES                     PROCESSING ID: P
  VERSION ID: 2.3                       SEND FORMULARY: YES
  ADMIT DIAGNOSIS: YES                  SEND DISCHARGE ICD9 DIAGNOSIS: YES
  ADT ACTIVE: YES                       NEW ORDERS ACTIVE: YES
  RENEW ORDERS ACTIVE: YES              OTHER ORDERS ACTIVE: YES
  INTERFACE VENDOR: AUTOMATED DISPENSING SYSTEM
  ADT SEND OUTPATIENT: YES              ADT SEND INPATIENT: YES
  INPATIENT MEDS FOR OUTPATIENT: YES    SEND IV ORDERS: YES

RECEIVING FACILITY: HOSPITAL DEMO       CHANNEL ACTIVE: YES
  IP ADDRESS: EXAMPLE IP ADDRESS
  SEND SOCKET: EXAMPLE                  RECEIVE SOCKET: EXAMPLE
  ACCEPT TRANSACTIONS: YES              CLIENT OR SERVER: CLIENT
  PHARMACY OUTPATIENT SITE: DEMO RX
  MONITOR ACTIVE: ON                    MONITOR RESCHEDULING FREQUENCY: 180
  MONITOR CURRENT TASK: 1               BASE ALLERGY:
  DAYS TO KEEP IN QUEUE: 7              STOP: INTERFACE ACTIVE

OUTPATIENT LOCATION: DEMO CLINIC        OP SEND LOCATION: DEMO OP CLINIC
  OP LOCATION POINTER: DEMO OP CLINIC
  ILC P-O INTERFACE DOMAIN: your.domain.gov
  LOCATION DECODING TYPE: DEFAULT
  DEFAULT OUTPATIENT LOCATION: DEMO CLINIC
  DEFAULT OP SEND LOCATION: DEMO CLINIC
  SEND ALL OUTPATIENTS: YES
  DEFAULT OP LOCATION POINTER: DEMO CLINIC
  DEFAULT CLERK: DEMO,DOC TWO
```

Figure 4-1: BOP Site Parameters example

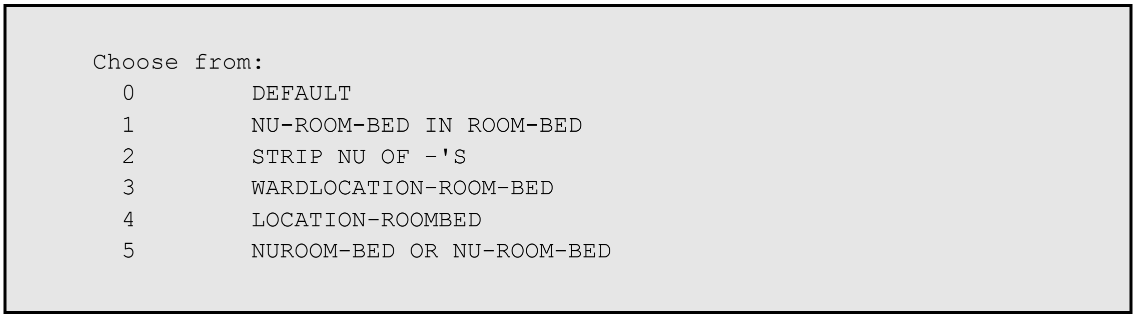
5.0 Wards, Beds, and Facilities

There are fields in the **BOP Site Parameter** file to control how the interface will send ward, bed and facility data. If these parameters are not set up by the installing staff, the system will set them up automatically according to defaults as below:

- A **Type** field determines how ward, bed, and facility are extracted from **VADPT** information. There are currently **5** types. The default type uses the standard **3** fields from **VADPT** information.
- Another field, **Automated Dispensing System domain** was added so that code can be written in the interface that is specific to one site, using a name that will probably be the same as the site’s Internet domain name–and is used as the default by looking at **^XMB(“NETNAME”)**.

The field may be described in more detail as below:

The **LOCATION DECODING TYPE** is necessary because different facilities use **Room-Bed** and **Nursing Unit** in different formats (Figure 5-1).



```
     Choose from:
       0        DEFAULT
       1        NU-ROOM-BED IN ROOM-BED
       2        STRIP NU OF -'S
       3        WARDLOCATION-ROOM-BED
       4        LOCATION-ROOMBED
       5        NUROOM-BED OR NU-ROOM-BED
```

Figure 5-1: Location Decoding Type example

6.0 Troubleshooting

The first steps taken to determine if the interface is running should be to use the **BOP TROUBLESHOOT MENU**. Check **FUT** for future tasks to determine if future jobs are being built. Check **RUN** for running tasks. You should see a **BOPRNEW** task, a **BOPRNEW1** task, and a **BOPT1** task.

The main transmission file (**90355.1**) should be checked to determine if the transactions are current.

Review **^BOP(90355.1,0**. Piece 3 is the last record created. Review **^BOP(90355.1,#,0)**. Piece 1 is a date/time stamp in the format of **3040625.111111** to correspond to 06/25/04 at 11:11:11.

The **AS** cross reference is used to determine the records that need to be sent. Review **^BOP(90355.1,"AS",0<ret>** to determine what records are in the queue to be transmitted. If there are no records in the **"AS",0** cross reference and the last record in **^BOP(90355.1** is current, then the interface is running.

Review the RPMS error monitor. If there is a problem with the first record ready to be transmitted, remaining transactions will not transmit. In addition, the error will be created for that first record each time the future job is rescheduled, so you will see the same error every 3 to 5 minutes.

To get the interface past the **bad** first record, either a user or an IRM member may go into the troubleshoot menu and select **CHK**. If the same number repeats (through at least one iteration of a new future job being created), then when the system offers to remove the **AS** cross reference, the user may answer **YES**. That should allow the interface to get past the **bad** record and process all other records.

It may be appropriate to stop both sides of the interface, restart the vendor system, then restart the RPMS system to reset both systems and restart transmissions. Follow the process below:

1. Stop the job that is transmitting. Stop the monitor by setting the **MONITOR ACTIVE** field to **OFF**. The transmitter needs to be stopped by a programmer in programmer mode. You may have to wait a few minutes to ensure that all jobs have completed (you should have some experience at your site and know how long it may take for this process).
2. If the background jobs are still running, a programmer must go into the system and stop the jobs manually. The mumps utility to check the system status is **%SS** to determine if a job is running.

3. Contact the **Automated Dispensing System Support Center**. Have your **Automated Dispensing System Customer ID** available. The Automated Dispensing System representative will dial in to stop the interface and will reboot the Automated Dispensing System if necessary. Ask the Automated Dispensing System representative to remain on-line until you complete **Step 4**.

4. Before restarting the interface on the RPMS system, it is recommended to utilize the **CALL^%ZISTCP** process described below to clear out the **ip/socket combo** used for the interface. If there are ghost jobs left on RPMS, use the **call^%zistcp** to clear them out.

5. Restart the **monitor** on the RPMS system.

The following can help analyze the issue:

- The transmission job is not running.

If the interface does not seem to be transmitting data to the vendor system, it may be due to the monitor not running. Check to see if the monitor has been scheduled. Use the **BOP TROUBLESHOOT MENU** to determine if the Future job exists and if the Running jobs exist. If the Troubleshoot options says that there are no future jobs and no running jobs, then use the option **BOP MONITOR** to restart the interface.

> **Important:** Only use the **BOP MONITOR** option if no future or running jobs exist.

- Check **TCP/IP** connections

  If the interface does not seem to be transmitting data to the vendor system, it may be a **TCP/IP** connectivity issue. Symptoms that indicate this kind of problem usually can be seen in the transmission files. Records will not be marked or acknowledged. The vendor system will not have the patients or orders on file that should have been transmitted.

1. Stop the **job** that is transmitting. Stop the **monitor** by setting the **MONITOR ACTIVE** field to **OFF** in the BOP SITE PARAMETERS. The transmitter needs to be stopped by a programmer.

2. Contact the **Automated Dispensing System Support Center**. Have your **Automated Dispensing System Customer ID** available. The Automated Dispensing System representative will dial in to stop the interface and will reboot the Automated Dispensing System if necessary. Ask the Automated Dispensing System representative to remain on-line until you complete **Step 4**.

3. In **RPMS** programmer mode enter the following code (Figure 6-1):

```
(Example: vendor IP address = 111.22.33.44, port = 6000)
      D CALL^%ZISTCP("111.22.33.44",6000) W POP
```

Figure 6-1: RPMS Machine code

4. If **POP = 0** a successful connection was made. Restart the **RPMS Monitor**. The systems should start communicating again. Have the Automated Dispensing System representative verify that data is being received from the RPMS system and is being passed to the **Automated Dispensing System Console**.

5. If you get **POP = 0**, which is a successful connection, you must close that connection when you are finished before you can try to restart the interface. Type the following (Figure 6-2) to close the connection:

```
D CLOSE^%ZISTCP
```

Figure 6-2: Closing the Connection code

6. If **POP=1** there is no connectivity. At this point, advanced troubleshooting will be required to identify the exact cause of the communication problem.

Appendix A Rules of Behavior

The Resource and Patient Management (RPMS) system is a United States Department of Health and Human Services (HHS), Indian Health Service (IHS) information system that is ***FOR OFFICIAL USE ONLY***. The RPMS system is subject to monitoring; therefore, no expectation of privacy shall be assumed. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution.

All users (Contractors and IHS Employees) of RPMS will be provided a copy of the Rules of Behavior (ROB) and must acknowledge that they have received and read them prior to being granted access to a RPMS system, in accordance with IHS policy.

- For a listing of general ROB for all users, see the most recent edition of *IHS General User Security Handbook* (SOP 06-11a).
- For a listing of system administrators/managers rules, see the most recent edition of the *IHS Technical and Managerial Handbook* (SOP 06-11b).

Both documents are available at this IHS website: https://home.ihs.gov/security/index.cfm.

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

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

A.1 All RPMS Users

In addition to these rules, each application may include additional ROBs that may be defined within the documentation of that application (e.g., Dental, Pharmacy).

A.1.1 Access

RPMS users shall:

- Only use data for which you have been granted authorization.
- Only give information to personnel who have access authority and have a need to know.
- Always verify a caller's identification and job purpose with your supervisor or the entity provided as employer before providing any type of information system access, sensitive information, or nonpublic agency information.
- Be aware that personal use of information resources is authorized on a limited basis within the provisions *Indian Health Manual* Part 8, "Information Resources Management," Chapter 6, "Limited Personal Use of Information Technology Resources."

RPMS users shall not:

- Retrieve information for someone who does not have authority to access the information.
- Access, research, or change any user account, file, directory, table, or record not required to perform their *official* duties.
- Store sensitive files on a PC hard drive, or portable devices or media, if access to the PC or files cannot be physically or technically limited.
- Exceed their authorized access limits in RPMS by changing information or searching databases beyond the responsibilities of their jobs or by divulging information to anyone not authorized to know that information.

A.1.2 Information Accessibility

RPMS shall restrict access to information based on the type and identity of the user. However, regardless of the type of user, access shall be restricted to the minimum level necessary to perform the job.

RPMS users shall:

- Access only those documents they created and those other documents to which they have a valid need-to-know and to which they have specifically granted access through an RPMS application based on their menus (job roles), keys, and FileMan access codes. Some users may be afforded additional privileges based on the functions they perform, such as system administrator or application administrator.
- Acquire a written preauthorization in accordance with IHS policies and procedures prior to interconnection to or transferring data from RPMS.

A.1.3 Accountability

RPMS users shall:

- Behave in an ethical, technically proficient, informed, and trustworthy manner.
- Log out of the system whenever they leave the vicinity of their personal computers (PCs).
- Be alert to threats and vulnerabilities in the security of the system.
- Report all security incidents to their local Information System Security Officer (ISSO)
- Differentiate tasks and functions to ensure that no one person has sole access to or control over important resources.
- Protect all sensitive data entrusted to them as part of their government employment.
- Abide by all Department and Agency policies and procedures and guidelines related to ethics, conduct, behavior, and information technology (IT) information processes.

A.1.4 Confidentiality

RPMS users shall:

- Be aware of the sensitivity of electronic and hard copy information and protect it accordingly.
- Store hard copy reports/storage media containing confidential information in a locked room or cabinet.
- Erase sensitive data on storage media prior to reusing or disposing of the media.
- Protect all RPMS terminals from public viewing at all times.
- Abide by all Health Insurance Portability and Accountability Act (HIPAA) regulations to ensure patient confidentiality.

RPMS users shall not

- Allow confidential information to remain on the PC screen when someone who is not authorized to that data is in the vicinity.
- Store sensitive files on a portable device or media without encrypting.

A.1.5 Integrity

RPMS users shall:

- Protect their systems against viruses and similar malicious programs.
- Observe all software license agreements.

- Follow industry standard procedures for maintaining and managing RPMS hardware, operating system software, application software, and/or database software and database tables.
- Comply with all copyright regulations and license agreements associated with RPMS software.

RPMS users shall not:

- Violate federal copyright laws.
- Install or use unauthorized software within the system libraries or folders.
- Use freeware, shareware, or public domain software on/with the system without their manager's written permission and without scanning it for viruses first.

A.1.6 System Logon

RPMS users shall:

- Have a unique User Identification/Account name and password.
- Be granted access based on authenticating the account name and password entered.
- Be locked out of an account after five successive failed login attempts within a specified time period (e.g., one hour).

A.1.7 Passwords

RPMS users shall:

- Change passwords a minimum of every 90 days.
- Create passwords with a minimum of eight characters.
- If the system allows, use a combination of alpha-numeric characters for passwords, with at least one uppercase letter, one lower case letter, and one number. It is recommended, if possible, that a special character also be used in the password.
- Change vendor-supplied passwords immediately.
- Protect passwords by committing them to memory or store them in a safe place (do not store passwords in login scripts or batch files).
- Change passwords immediately if password has been seen, guessed, or otherwise compromised, and report the compromise or suspected compromise to their ISSO.
- Keep user identifications (IDs) and passwords confidential.

RPMS users shall not:

- Use common words found in any dictionary as a password.

- Use obvious readable passwords or passwords that incorporate personal data elements (e.g., user's name, date of birth, address, telephone number, or social security number; names of children or spouses; favorite band, sports team, or automobile; or other personal attributes).
- Share passwords/IDs with anyone or accept the use of another's password/ID, even if offered.
- Reuse passwords. A new password must contain no more than five characters per eight characters from the previous password.
- Post passwords.
- Keep a password list in an obvious place, such as under keyboards, in desk drawers, or in any other location where it might be disclosed.
- Give a password out over the phone.

A.1.8 Backups

RPMS users shall:

- Plan for contingencies such as physical disasters, loss of processing, and disclosure of information by preparing alternate work strategies and system recovery mechanisms.
- Make backups of systems and files on a regular, defined basis.
- If possible, store backups away from the system in a secure environment.

A.1.9 Reporting

RPMS users shall:

- Contact and inform their ISSO that they have identified an IT security incident and begin the reporting process by providing an IT Incident Reporting Form regarding this incident.
- Report security incidents as detailed in the *IHS Incident Handling Guide* (SOP 05-03).

RPMS users shall not:

- Assume that someone else has already reported an incident. The risk of an incident going unreported far outweighs the possibility that an incident gets reported more than once.

A.1.10 Session Timeouts

RPMS system implements system-based timeouts that back users out of a prompt after no more than 5 minutes of inactivity.

RPMS users shall:

- Utilize a screen saver with password protection set to suspend operations at no greater than 10 minutes of inactivity. This will prevent inappropriate access and viewing of any material displayed on the screen after some period of inactivity.

A.1.11 Hardware

RPMS users shall:

- Avoid placing system equipment near obvious environmental hazards (e.g., water pipes).
- Keep an inventory of all system equipment.
- Keep records of maintenance/repairs performed on system equipment.

RPMS users shall not:

- Eat or drink near system equipment.

A.1.12 Awareness

RPMS users shall:

- Participate in organization-wide security training as required.
- Read and adhere to security information pertaining to system hardware and software.
- Take the annual information security awareness.
- Read all applicable RPMS manuals for the applications used in their jobs.

A.1.13 Remote Access

Each subscriber organization establishes its own policies for determining which employees may work at home or in other remote workplace locations. Any remote work arrangement should include policies that:

- Are in writing.
- Provide authentication of the remote user through the use of ID and password or other acceptable technical means.
- Outline the work requirements and the security safeguards and procedures the employee is expected to follow.
- Ensure adequate storage of files, removal, and nonrecovery of temporary files created in processing sensitive data, virus protection, and intrusion detection, and provide physical security for government equipment and sensitive data.

- Establish mechanisms to back up data created and/or stored at alternate work locations.

Remote RPMS users shall:

- Remotely access RPMS through a virtual private network (VPN) whenever possible. Use of direct dial in access must be justified and approved in writing and its use secured in accordance with industry best practices or government procedures.

Remote RPMS users shall not:

- Disable any encryption established for network, internet, and Web browser communications.

A.2 RPMS Developers

RPMS developers shall:

- Always be mindful of protecting the confidentiality, availability, and integrity of RPMS when writing or revising code.
- Always follow the IHS RPMS Programming Standards and Conventions (SAC) when developing for RPMS.
- Only access information or code within the namespaces for which they have been assigned as part of their duties.
- Remember that all RPMS code is the property of the U.S. Government, not the developer.
- Not access live production systems without obtaining appropriate written access and shall only retain that access for the shortest period possible to accomplish the task that requires the access.
- Observe separation of duties policies and procedures to the fullest extent possible.
- Document or comment all changes to any RPMS software at the time the change or update is made. Documentation shall include the programmer’s initials, date of change, and reason for the change.
- Use checksums or other integrity mechanism when releasing their certified applications to assure the integrity of the routines within their RPMS applications.
- Follow industry best standards for systems they are assigned to develop or maintain and abide by all Department and Agency policies and procedures.
- Document and implement security processes whenever available.

RPMS developers shall not:

- Write any code that adversely impacts RPMS, such as backdoor access, “Easter eggs,” time bombs, or any other malicious code or make inappropriate comments within the code, manuals, or help frames.

- Grant any user or system administrator access to RPMS unless proper documentation is provided.
- Release any sensitive agency or patient information.

A.3 Privileged Users

Personnel who have significant access to processes and data in RPMS, such as, system security administrators, systems administrators, and database administrators, have added responsibilities to ensure the secure operation of RPMS.

Privileged RPMS users shall:

- Verify that any user requesting access to any RPMS system has completed the appropriate access request forms.
- Ensure that government personnel and contractor personnel understand and comply with license requirements. End users, supervisors, and functional managers are ultimately responsible for this compliance.
- Advise the system owner on matters concerning information technology security.
- Assist the system owner in developing security plans, risk assessments, and supporting documentation for the certification and accreditation process.
- Ensure that any changes to RPMS that affect contingency and disaster recovery plans are conveyed to the person responsible for maintaining continuity of operations plans.
- Ensure that adequate physical and administrative safeguards are operational within their areas of responsibility and that access to information and data is restricted to authorized personnel on a need-to-know basis.
- Verify that users have received appropriate security training before allowing access to RPMS.
- Implement applicable security access procedures and mechanisms, incorporate appropriate levels of system auditing, and review audit logs.
- Document and investigate known or suspected security incidents or violations and report them to the ISSO, Chief Information Security Officer (CISO), and systems owner.
- Protect the supervisor, superuser, or system administrator passwords.
- Avoid instances where the same individual has responsibility for several functions (i.e., transaction entry and transaction approval).
- Watch for unscheduled, unusual, and unauthorized programs.
- Help train system users on the appropriate use and security of the system.

- Establish protective controls to ensure the accountability, integrity, confidentiality, and availability of the system.
- Replace passwords when a compromise is suspected. Delete user accounts as quickly as possible from the time that the user is no longer authorized system. Passwords forgotten by their owner should be replaced, not reissued.
- Terminate user accounts when a user transfers or has been terminated. If the user has authority to grant authorizations to others, review these other authorizations. Retrieve any devices used to gain access to the system or equipment. Cancel logon IDs and passwords and delete or reassign related active and backup files.
- Use a suspend program to prevent an unauthorized user from logging on with the current user's ID if the system is left on and unattended.
- Verify the identity of the user when resetting passwords. This can be done either in person or having the user answer a question that can be compared to one in the administrator's database.
- Shall follow industry best standards for systems they are assigned to and abide by all Department and Agency policies and procedures.

Privileged RPMS users shall not:

- Access any files, records, systems, etc., that are not explicitly needed to perform their duties.
- Grant any user or system administrator access to RPMS unless proper documentation is provided.
- Release any sensitive agency or patient information.

Acronym List

Acronym	Meaning
BOP	IHS Pharmacy-Automated Dispensing Interface System
EHR	Electronic Health Record
IEN	Internal Entry Number
IHS	Indian Health Service
IRM	Information Resource Management

Contact Information

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

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

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

Email: itsupport@ihs.gov