RESOURCE AND PATIENT MANAGEMENT SYSTEM

Master Patient Index

(AGMP)

User Manual

Version 1.0 Patch 3
July 2024

Office of Information Technology
Division of Information Technology

Table of Contents

Document Revision History

Date of Change	Location of Revision	Revision
08/2023	Preface	Corrected menu name
08/2023	Section 2.2	Removed
08/2023	Throughout section 3	Removed MFN and MFE options and other references to MFN/MFK messages and the Treating Facility List
08/2023	Throughout section 3	Updated text to match the figures
08/2023	Section 3.3.4	Corrected description of the background job
08/2023	Throughout section 3.4	Added the UN menu option
08/2023	Sections 3.4.3, 3.4.4, 3.7, 3.8, 3.9	Miscellaneous text correction and cleanup
08/2023	Section 3.6	Added TFL deprecation information
08/2023	Section 3.9.3	Removed reference to VQQ messages
04/2024	Sections 3.0, 3.1, 3.3.2, 3.8, 3.8.1; Acronym List	Removed MRG option and A40 messages
04/2024	Throughout section 3.4	Added the STAT menu option

Table of Figures

Preface

The purpose of this manual is to provide information about the Master Patient Index (MPI) Interface package, and to assist in the use of this interface. The document contains information on the use of the MPI Manager Options menu.

This manual will be primarily used by Office of Information Technology personnel, local site managers, and Information Technology specialists after the successful installation of the interface has been accomplished.

1.0   Introduction

For over 20 years, hospitals and health centers of the Indian Health Service (IHS) and numerous Tribal health programs have used an information system called the Resource and Patient Management System (RPMS). The RPMS is a highly integrated system consisting of some 50 healthcare and administrative applications. Virtually all of these applications directly interact with one or more, and sometimes many, of the other RPMS applications.

RPMS applications are required to interact with the MPI to meet the needs of the IHS MPI initiative. The RPMS/HL7-Optimized (HLO) interface and an Ensemble production is a way to send patient Admission, Discharge, Transfer (ADT) information to the MPI and to receive treating facility information from the MPI and store it in the RPMS database.

When the MPI and the RPMS/AGMPI Interface are complete, the MPI will be the primary data repository for enterprise-wide patient data.

It is the shared vision of IHS national representatives that the RPMS/MPI will be the repository of patient data that can be accessed by outside entities via the National Health Information Network (NHIN). The MPI will also be accessed by the Personal Health Record (PHR) application.

2.0   System Navigation

2.1   System Overview

The AGMP (MPI) interface has many different functions. These functions are described beginning in Section 3.0.

2.2   Conventions in the Software and Manual

The RPMS has established certain terms and operating procedures (conventions) for applications. The following is a brief discussion on those conventions, the knowledge of which enables a new user to quickly navigate through the system. When reading the following explanations, refer to the keyboard to ensure that correct identification of each key and command function.

2.2.1   Double Slash (//)

Prompts in the roll and scroll screens are frequently followed by text and two slashes (//). The text displayed before the two slashes is the default response to the prompt. Pressing Enter selects the default response without retyping it. If you do not want to use the default response (or if no default response is presented before double slashes), type a response and then press Enter. If a prompt has a default response, but you want the response to be blank, you can leave the response blank by deleting the default text or typing an "at" sign (@) at the prompt after the default response.

2.2.2   Screenshots

Figure 2-1 shows an example of a screenshot or screen capture.

```
SM HLO SYSTEM MONITOR
MV HLO MESSAGE VIEWER
APPS HLO APPLICATION REGISTRY
STAT HLO MESSAGE STATISTICS
```

Figure 2-1: Screenshot example

Syntax in screenshots:

- Boldface type in a screenshot indicates text to be typed by the user.

- After typing an entry, press Enter to accept the entry.

- If the screenshot shows only the two double slashes (//) without any boldface type, press Enter without typing anything.

2.2.3   Help at Prompts

Help is available for most menu options and data entry prompts:

- Typing a single question mark (**?**) at the data entry prompt displays instructions for entering the requested data.

- Typing two question marks (**??**) displays a more complete message.

- Typing three question marks (**???**) displays the most complete descriptive help available on the system.

Some prompts display a list of available choices. If at any time you are unsure how to answer a particular question, or if you want to know more about the menu choices, type a single question mark (**?**) to display more information.

2.2.4   The Caret (^)

The caret (^), also known as the up-hat, is a special control character used to exit from a particular activity or data entry sequence. Typing the caret (^) at any prompt usually returns you to the preceding prompt or menu level. It can also be used to exit from long data displays, such as vendor lists, that involve many screens.

Type a caret (^) by simultaneously pressing the **Shift** key and the 6 key at the top of the keyboard. Pressing the Shift key and the 6 key on the numeric keypad does not create a caret (^) character.

2.2.5   The "Select Device:" Prompt

Whenever the software can display a list or report, it displays the "Select Device" prompt:

- To send the report or list to a printer, type the **printer name** or **number**.

- To display the report or list on the monitor, type **HOME** or **0**.

- For help in responding to the "Select Device" prompt, contact your site manager.

- Some reports also allow **Q** (Queue) to be typed at the "Device" prompt. This option sends a report to a printer and then returns immediately to the screen you are using while the report is printing. This option is helpful if the report takes a long time to run (search) or print. After typing **Q**, the system displays the "Queue to Print on Device" prompt. At this prompt, type the name of the printer on which you want to print the report.

3.0   AGMPI Menu Options

The AGMP (MPI) interface includes menu options to create the following HL7 messages:

- A28 (Add a Patient)

- A08 (Update a Patient)

- A01 (Admissions and Check Ins)

- A03 (Discharge and Check Outs)

3.1   Outgoing Patient Data

New patient data, patient updates, and visits/admission data are normally sent using triggers and protocols. When a new patient is registered, edited, and checked in or out, a message is automatically sent. However, it is possible to manually send a message through the interface.

Use the menus and options shown below to perform the following tasks:

- Add Patient (A28)

- Update Patient (A08)

- Check Ins and Admissions (A01)

- Check Outs and Discharge (A03)

Figure 3-1 shows the MPI Manager Options menu in RPMS.

```
MASTER PATIENT INDEX
2016 DEMO HOSPITAL
MPI Manager Options


EDIT  EDIT AGMP SITE PARAMETERS
ADD   SEND A28 ADD PATIENT
UPD   SEND A08 UPDATE
VST   SEND A01/A03 MESSAGE
RS    RESEND HL7 MESSAGE
RPT   MPI Reports and Debug option ...


You have PENDING ALERTS
Enter  "VA to jump to VIEW ALERTS option
Select MPI Manager Options <TEST ACCOUNT> Option:
```

Figure 3-1: HLO MPI MGR MENU

Refer to the following sections for the details about using the MPI Manager Options.

3.1.1   Edit AGMP Site Parameters

The MPI "Manager Options… Option" EDIT (EDIT AGMP SITE PARAMETERS) is used to opt in or opt out of MPI.

1. At the "Select MPI Manager Options… Option" prompt, type **EDIT (EDIT AGMP SITE PARAMETERS)** and press Enter.

2. At the "MPI Application Status" prompt, type **E** to **Enable** or **D** to **Disable** MPI and press enter (Figure 3-2).

```
Select whether to enable or disable the MPI application:

Select one of the following:
     E        Enabled
     D        Disabled
MPI Application Status: Enabled//D

This option will disable the MPI application. Re-enabling the application
may result in a large number of messages being generated to synchronize
with the central repository.

Are you sure that you want to do this: NO//
```

Figure 3-2: MPI Manager Options

3. At the "Are you sure that you want to do this?" prompt, type **N** for **NO** and **Y** for **YES** and press Enter.

3.2   Add Patient (ADD) in Patient Registration (AG)

The purpose of this message is to establish a patient on the MPI so that the patient record can be viewed across the enterprise. This message allows multiple systems and their respective master patient databases to communicate activity related to a person regardless of whether that person is currently a patient on each system. Each system has an interest in the database activity of the others in order to maintain data integrity across an enterprise. To the enterprise systems, the person may be a current patient, a potential future patient, or never be needed. These events can also be used to maintain another MPI or enterprise database.

This option can be used to create an A28 ADD PATIENT message to add a patient to the MPI. The following steps are for patient registration. Use the Patient Registration option **ADD (ADD a New Patient)**, as shown in Figure 3-3.

```
                       PATIENT REGISTRATION
                       NOT-A-REAL FACILITY
                       Patient Registration
  *** NOTE: IF YOU EDIT A PATIENT AND SEE THEIR NAME IN REVERSE VIDEO ***
  *** WITH '(RHI)' BLINKING NEXT TO IT, IT MEANS THEY HAVE RESTRICTED ***
                       *** HEALTH INFORMATION ***
ADD ADD a new patient
```

```
EPT EDIT a patient's file
FAC Print a FACE SHEET
NON Enter NON-MANDATORY new patient information
NAM CORRECT the patient's NAME
CHR EDIT the patient's CHART NUMBER.
INA INACTIVATE/ACTIVATE a patient's file
RPT REGISTRATION REPORTS ...
VIEW View patient's registration data
DEL DELETE a patient's Health Record Number
REV Review and edit DECEASED or INACTIVE patient files
EMB Print an EMBOSSED CARD
SCA SCAN the patient files ...
THR Third Party Billing Reports ...
IND Print tub-file INDEX cards ...
LBL LABELS menu ...
PAG Edit one of the Patient's PAGEs ...
FIE print Face sheet, Index card, Embossed card
MSP Medicare Secondary Payer Menu ...
Select Master Patient Index Option: ADD
```

Figure 3-3: EDIT AGMPI SITE PARAMETERS option

1. At the "Select Patient Registration Option" prompt, type **ADD (ADD a new patient)**, and press Enter (Figure 3-4).

```
PATIENT REGISTRATION
NOT-A-REAL FACILITY
ADD a new patient
*** NOTE: IF YOU EDIT A PATIENT AND SEE THEIR NAME IN REVERSE VIDEO ***
*** WITH '(RHI)' BLINKING NEXT TO IT, IT MEANS THEY HAVE RESTRICTED ***
*** HEALTH INFORMATION ***

You must first SCAN FOR SIMILAR NAMES or CHART NUMBERS NOW...
Select PATIENT NAME:
Enter the NEW PATIENT'S FULL NAME.....
(EXAMPLE: MORGAN,JAMES PAUL,JR (no space after commas))

Entering NEW Patient for NOT-A-REAL FACILITY

Enter the PATIENT'S NAME: NEW,PATIENT
ARE YOU ADDING 'NEW,PATIENT' AS A NEW PATIENT (THE 9283RD)? No// Y (YES)
```

Figure 3-4: Adding a new patient

2. At the "Select PATIENT NAME" prompt, type the new patient's name and press Enter.

3. At the "ARE YOU ADDING 'NEW,PATIENT' AS A NEW PATIENT (THE 9283RD)?" prompt, type **Y** (Yes) and press Enter.

Follow the steps necessary to enter a new patient into Patient Registration (AG). After registration is complete, a message is displayed indicating that a patient has been added.

After a patient is added in Patient Registration (AG), an A28 is automatically sent to the MPI to determine whether the patient already exists in the MPI database. If an exact match is found, the MPI sends back an Enterprise Unique Identifier (EUID). The RPMS system receives the EUID and places it into the INTEGRATION CONTROL NUMBER (ICN) field in the Veterans Affairs (VA) PATIENT file. Otherwise, if an exact match is not found, the MPI will add the patient to the MPI. When the patient has been successfully added to the system, the MPI returns the EUID, and the EUID is added to the ICN.

3.3 Sending Individual Messages

The options listed below can be used to create a new message that is sent to the MPI. If a message fails, review the error message to debug and recreate a message to send to the MPI after correcting the error.

3.3.1 Send A28 Add Patient (ADD)

```
Use the ADD (SEND A28 ADD PATIENT) option to create an A28 Add A Patient
message to add a patient to the MPI. Use a FileMan patient lookup to select
any patient in the PATIENT file, as shown in Figure 3 5. An acknowledgment
that the message was sent is contained within the message file.ENTER
PATIENT YOU WISH TO ADD TO THE MPI:
Select PATIENT NAME:
DEMO, DELORES M                    F 03-28-1982 XXX-XX-2882  WE 123456789
```

Figure 3-5: Send a single A28 Message option (ADD option)

3.3.2 Send A08 Update (UPD)

Use the **UPD (SEND A08 UPDATE)** option to send an Update Patient message, as shown in Figure 3-6. A background job runs every five minutes to send A08 messages; however, if a message needs to be sent immediately, use this option. An acknowledgment that the message was sent is contained within the message file.

```
Select MPI Manager Options Option: UPD SEND A08 UPDATE
EXAMPLE OF AN A08 UPDATE
Select PATIENT NAME:
NEW,PATIENT                        F 05-04-2010 605050410P   WE 12323

A08 Message 12345 has been sent to update patient NEW,PATIENT on the MPI.
```

Figure 3-6: Update a patient option (UPD option)

3.3.3   Send A01/A03 Message (VST)

Use the **VST (SEND A01/A03 MESSAGE)** option to send a check-in or admission message, as shown in Figure 3-7. The admission date can be entered manually at the "ENTER MOVEMENT DATE" prompt. The check-in date can be entered manually at the "ENTER CHECK-IN DATE" prompt. An acknowledgment that the message was sent is within the message file.

An A03 event signals the end of a patient's stay in a healthcare facility. It signals that the patient's status has changed to "discharged" and that a discharge date has been recorded. It is also captured when the patient checks out.

Use the **VST (A03)** option to send a checkout or discharge message. The discharge date can be entered manually at the "ENTER MOVEMENT DATE" prompt. The check-out date can be entered manually at the "CHECK-OUT DATE" prompt. An acknowledgment that the message was sent is contained within the message file.

```
Select MPI Manager Options Option: VST SEND A01/A03 MESSAGE
CREATE A VISIT HL7 MESSAGE
Select PATIENT NAME:
NEW,PATIENT                       F 05-04-2010 605050410P    WE 12323

Select one of the following:

A       ADMISSION
D       DISCHARGE
CIN        CHECK-IN
COUT   CHECK-OUT

ENTER MOVEMENT DATE:T@12

A01 Message IEN 123456 has been sent to update patient NEW,PATIENT last
treated date on the MPI.
```

Figure 3-7: Send A01/A03 Message (VST option)

3.3.4   Resend HL7 Message (RS)

To resend (RS) a message, use the **RS RESEND HL7 MESSAGE** option, as shown in Figure 3-8.

1. At the "Select MPI Manager Options Option" prompt, type **RS** and press Enter.

2. At the "SELECT FROM MESSAGE" prompt, type the message ID or a single question mark (**?**) to get a list of messages and press Enter.

3. Each site will have a different number of messages to choose from, depending on the number of messages sent.

4. At the "SELECT FROM MESSAGE" prompt, type a message ID and press Enter.

5. At the "OK" prompt type **Y** (Yes) and press Enter.

6. At the "SELECT TO MESSAGE" prompt, type a message ID and press Enter.

7. At the "OK" prompt type **Y** (Yes) and press Enter. The message(s) are resent and the new message number(s) are provided.

```
Select SELECT MPI MANAGER OPTIONS OPTION: RS RESEND HL7 MESSAGE

SELECT FROM MESSAGE: ?
Answer with HLO MESSAGES MESSAGE ID, or MESSAGE BODY

Choose from:
   14752 1
   14752 10
   14752 11
   14752 12
   14752 13
   14752 14
   14752 15
   14752 16
   14752 17
   14752 18
   14752 19
   14752 2
   14752 20
   14752 21
   14752 22
   14752 3
   14752 4
   14752 5
   14752 6
   14752 7
   14752 8
   14752 9
SELECT FROM MESSAGE: 14752 9
...OK? Yes// Y (Yes)
SELECT TO MESSAGE: 14752 9
...OK? Yes// Y (Yes)

MESSAGE RESENT, NEW NUMBER: 23
               OLD NUMBER: 9
SENT AT DATE@TIME

TOTAL MESSAGES PROCESSED: 1
Enter RETURN to continue or '^' to exit:
```

Figure 3-8: Message resend (RS option)

In Figure 3-8, message number **14752 9** was selected and when it was resent the system assigned a new number which displays after the "MESSAGE RESENT, NEW NUMBER" prompt.

3.4   MPI Reports and Debug Option (RPT)

The **MPI Reports and Debug** option menu contains the following items, as shown in Figure 3-9:

- MFE: MPI Unsuccessful MFE Report

- DAT: MPI Messages by Date

- TOT: MPI Queue and msg Totals

- ICN: MPI Report of ICNs populated

- UN: MPI Print Unsuccessful Messages

- STAT: Display the MPI application status report

```
MASTER PATIENT INDEX
NOT-A-REAL FACILITY
MPI  Reports and Debug option


   DAT    MPI Messages by Date
   TOT    MPI Queue and msg Totals
   ICN    MPI Missing ICN Report
   UN     MPI Print Unsuccessful Messages
   STAT   Display the MPI application status report


Select MPI Reports and Debug option Option:
```

Figure 3-9: MPI Reports and Debug option menu

3.4.1   MPI Messages by Date Option (DAT)

The **MPI Messages by Date** option compares the number of messages for the following groups of message types, as shown in Figure 3-10:

- ADT and ACK messages

    - There should be twice as many ACK messages as ADT messages.

```
   DAT    MPI Messages by Date
   TOT    MPI Queue and msg Totals
   ICN    MPI Missing ICN Report
   UN     MPI Print Unsuccessful Messages
   STAT   Display the MPI application status report

Select MPI Reports and Debug option Option: DAT MPI Messages by Date

MASTER PATIENT INDEX
NOT-A-REAL FACILITY
MPI Messages by Date
Enter from Date: T// (AUG 26, 2010)
Enter to Date: T// (AUG 26, 2010)


MESSAGE REPORT BY DATE PAGE 1
DATE PRINTED: AUG 26,2010@12:50:51
PRINTED BY: LASTNAME,USER
FOR MESSAGES FROM AUG 26,2010 TO AUG 26,2010


EVENT^TYPE TOTAL % OF TOTAL

A01^ACK 3997 66.69
A01^ADT 1996 33.30
```

```
TOTAL MSGS: 5993
Enter RETURN to continue or '^' to exit:
```

Figure 3-10: MPI Messages by Date Report (DAT option)

1. At the "Select MPI Reports and Debug option" prompt, type **DAT** and press Enter.

2. At the "Enter from Date" prompt, type the **date** and press Enter.

3.4.2   MPI Queue and Msg Totals Option (TOT)

The TOT report shows the total number of messages in the IN and OUT queues and the number of messages in the HLO Globals, as shown in Figure 3-11.

The number of messages listed in the IN and OUT queues should diminish on a regular basis. The IN queue may grow during any five-minute period, but when the background job runs, the queue should go to zero or near zero. A continued growth in the number of messages in these two queues over a long period of time (10 or 20 minutes) may indicate a problem.

- If messages back up in the IN queue, the problem is on the RPMS side, and there may be errors listed in the Error log. In addition, check to make sure the AGMPI ACK BCKGRND TSK task is scheduled in TaskMan and that TaskMan is running.

- If messages back up in the OUT queue, the problem is in Ensemble. Make sure the Ensemble AGMPI production is running. If the production is not running, start it back up.

- If the production is running and either queue has a backup of messages, contact the IHS IT Service Desk.

```
   DAT     MPI Messages by Date
   TOT     MPI Queue and msg Totals
   ICN     MPI Missing ICN Report
   UN      MPI Print Unsuccessful Messages
   STAT    Display the MPI application status report

You have 6 PENDING ALERTS

Enter "VA to jump to VIEW ALERTS option

Select MPI Reports and Debug option Option: TOT MPI Queue and msg Totals

MASTER PATIENT INDEX
NOT-A-REAL FACILITY
MPI Queue and msg Totals

   MESSAGES IN THE IN QUEUE:  5,827
   MESSAGES IN OUT QUEUE: 1
   TOTAL MESSAGES IN HLO GLOBALS:    8,004
```

```
     Enter RETURN to continue or '^' to exit:
```

Figure 3-11: MPI Queue and Msg Totals report (TOT option)

1. At the "Select MPI Reports and Debug option" prompt, type **TOT** and press
   Enter.

Figure 3-11 shows that messages are backing up in the IN queue, which indicates a
problem on the RPMS side. If a TOT report shows this kind of discrepancy, call the
IHS IT Service Desk.

3.4.3   MPI Missing ICN report (ICN)

The ICN report shows the number of patients whose ICN have been populated or not,
as shown in Figure 3-12.

The value in the NUMBER NOT POPULATED field should stay close to zero. A
value above zero that stays for more than a day indicates a possible network issue or
message processing problem. A large number in this field can also indicate the
AGMPI MPI MISSING ICN TSK option is not scheduled in TaskMan, or that
TaskMan is not running.

If the ICN report shows a value significantly above zero for more than a day, contact
the IHS IT Service Desk.

```
    DAT     MPI Messages by Date
    TOT     MPI Queue and msg Totals
    ICN     MPI Missing ICN Report
    UN      MPI Print Unsuccessful Messages
    STAT    Display the MPI application status report

You have 6 PENDING ALERTS
Enter "VA to jump to VIEW ALERTS option
Select MPI Reports and Debug option Option: ICN MPI Report of ICNs
populated

MASTER PATIENT INDEX
NOT-A-REAL FACILITY
MPI Report of ICNs populated
NUMBER OF ICNs POPULATED: 0
NUMBER NOT POPULATED: 9282

Enter RETURN to continue or '^' to exit:
```

Figure 3-12: MPI Report of ICNs populated (ICN option)

1. At the "Select MPI Reports and Debug option Option" prompt, type **ICN** and
   press Enter.

3.4.4   Display the MPI application status report (STAT)

The STAT report summarizes information about the state of the MPI application, as well as header information for the most recent outbound and inbound messages and oldest unsuccessful outbound messages. The intent of the report is to provide support personnel with a snapshot of the application. It is not intended to be used by site managers, and no information is provided to assist site managers with interpreting the report. The report does not contain personally identifiable information (PII) or protected health information (PHI).

When the user runs the report, it will ask whether to display the report with page breaks. If the user intends to view the report on the screen, it is recommended that page breaks be used. If the user is running the report in order to copy and paste information for the support team, then not using page breaks may be preferred.

```
--------------------------- MPI SUMMARY START ---------------------------
Report time: 2024-04-12 14:44:21
Site: 8992 (2019 DEMO HOSPITAL (INST))
Patches installed: v1 {1,2,3}
$ZV=Cache for Windows (x86-64) 2017.2.2 (Build 865_3_20793U) Thu Apr 15 2021 16:
04:37 EDT
MPI is enabled.
MPI production is running.
Upload type: INCLUDE ALL
Task status: MICN not scheduled
Missing ICN time:
SiteId: BS=8992, BO=8992
Central MPI: 10.155.137.42:5222
Listener port: 5203

Ensemble queue counts:
 AGMPI.MPIMessageRouting: 0          AGMPI.RPMSMessageRouting: 0
             BadMessage: 0                        EmailAlert: 1
              Ens.Actor: 0                         Ens.Alarm: 0
              Ens.Alert: 0               Ens.ScheduleHandler: 0
  EnsLib.Testing.Process: 0                      MPIOutBound: 1
           RPMSOutBound: 0

Site list:
Num     StaNm   ORF     AGMPCHK    Name
---     -----   ---     -------    ----
2869    -       NO      -          -
2872    -       NO      -          -
2906    8992    YES     VALID      2019 DEMO HOSPITAL (DIV)
2907    8992A   NO      -          2019 DEMO CLINIC TIN A
2914    8992C   YES     VALID      2019 DEMO-2 CLINIC TIN B
12651   8992E   YES     VALID      NEIGHBORHOOD PHYSICIANS PRACTICE
12652   8992F   YES     VALID      COMMUNITY HEALTH AND HOSPITALS

HLO queue information:
^HLC("FILE777","IN","TCP")=694995
^HLC("FILE777","OUT")=527878
^HLC("FILE778","IN","TCP")=694996
^HLC("FILE778","OUT","TCP")=527883
^HLC("QUEUECOUNT","OUT","MPI:5200","MPI RPMS")=81450
Size of outbound MPI queue: 0
Size of inbound MPI queue: 0
```

```
Last 5 outbound messages:
HLB IEN=Message ID^HLA IEN^Transmission D/T^Completion Status^Error Text

527883=8992 527883^527878^3240412.1144^^
MSH^~|\&^RPMS-MPI^8992~HL7.2013-DEMO.NA.IHS.GOV:5201~DNS^MPI^8990~:5200~DNS^2024
0412114410-0700^^ADT~A28~^8992 527883^P~^2.4^^^AL^NE^ + EVN + PID + ZPD

527881=8992 527881^527876^3240412.0555^^
MSH^~|\&^RPMS-MPI^8992~HL7.2013-DEMO.NA.IHS.GOV:5201~DNS^MPI^8990~:5200~DNS^2024
04120555-0700^^ADT~A28~^8992 527881^P~^2.4^^^AL^NE^ + EVN + PID + ZPD

527861=8992 527861^527856^3240402.0844^^~26891~~Error code: 301 Detail
MSH^~|\&^RPMS-MPI^8992~HL7.2013-DEMO.NA.IHS.GOV:5201~DNS^MPI^8990~:5200~DNS^2024
0402084445-0700^^ADT~A28~^8992 527861^P~^2.4^^^AL^NE^ + EVN + PID + ZPD

527860=8992 527860^527855^3240402.0816^^~26891~~Error code: 301 Detail
MSH^~|\&^RPMS-MPI^8992~HL7.2013-DEMO.NA.IHS.GOV:5201~DNS^MPI^8990~:5200~DNS^2024
0402081609-0700^^ADT~A28~^8992 527860^P~^2.4^^^AL^NE^ + EVN + PID + ZPD

527786=8992 527786^527781^3240314.0711^^
MSH^~|\&^RPMS-MPI^8992~HL7.2013-DEMO.NA.IHS.GOV:5201~DNS^MPI^8990~:5200~DNS^2024
0314071148-0700^^ADT~A28~^8992 527786^P~^2.4^^^AL^NE^ + EVN + PID + ZPD

Last 5 inbound messages:
HLB IEN=Message ID^HLA IEN^Transmission D/T^Completion Status^Error Text

200000694996=8992 200000694996^100000694995^3240411.12^SU^
MSH^~|\&^MPI^8990^^8992A^20240411120029-0600^^MFN~M05^882619^D^2.4^^^AL^NE + MFI
+ MFE + MFE + MFE + MFE

200000694995=8992 200000694995^100000694994^3240411.12^SU^
MSH^~|\&^MPI^8990^^8992^20240411120029-0600^^MFN~M05^882618^D^2.4^^^AL^NE + MFI
+ MFE + MFE + MFE + MFE

200000694994=8992 200000694994^100000694993^3240411.1159^SU^
MSH^~|\&^MPI^8990^^8992A^20240411115948-0600^^MFN~M05^882596^D^2.4^^^AL^NE + MFI
+ MFE + MFE + MFE + MFE + MFE

200000694993=8992 200000694993^100000694992^3240411.1159^SU^
MSH^~|\&^MPI^8990^^8992A^20240411115943-0600^^MFN~M05^882580^D^2.4^^^AL^NE + MFI
+ MFE + MFE + MFE + MFE + MFE

200000694992=8992 200000694992^100000694991^3240411.1138^SU^
MSH^~|\&^MPI^8990^RPMS-MPI^8992^20240411113817-0600^^ACK~A08^3181137-se^P^2.4^^^
AL^NE + MSA

First 5 unsuccessful outbound messages:
HLB IEN=Message ID^HLA IEN^Transmission D/T^Completion Status^Error Text

426512=8992 426512^426512^3161229.113^AE^~~~Error code: 400 Details: MD
MSH^~|\&^RPMS-MPI^8992~HL7.2013-DEMO.NA.IHS.GOV:5201~DNS^MPI^8990~:5200~DNS^2016
1229091734-0700^^VQQ~Q02~^8992 426512^P~^2.4^^^AL^NE^ + EVN + PID + ZPD

426765=8992 426765^426765^3170427.0939^AE^~~~Error code: 400 Details: MD
MSH^~|\&^RPMS-MPI^8992~HL7.2013-DEMO.NA.IHS.GOV:5201~DNS^MPI^8990~:5200~DNS^2017
0427093916-0700^^ADT~A08~^8992 426765^P~^2.4^^^AL^NE^ + EVN + PID + ZPD

494581=8992 494581^494579^^SE^INTERFACE ENGINE LOGICAL LINK PROVIDED BUT NOT FOU
ND
MSH^~|\&^RPMS-MPI^8992~HL7.2013-DEMO.NA.IHS.GOV:5201~DNS^MPI^8990~:~DNS^20210413
063550-0700^^ADT~A28~^8992 494581^P~^2.4^^^AL^NE^ + EVN + PID + ZPD
```

```
494582=8992 494582^494580^^SE^INTERFACE ENGINE LOGICAL LINK PROVIDED BUT NOT FOU
ND
MSH^~|\&^RPMS-MPI^8992~HL7.2013-DEMO.NA.IHS.GOV:5201~DNS^MPI^8990~:~DNS^20210413
064034-0700^^ADT~A28~^8992 494582^P~^2.4^^^AL^NE^ + EVN + PID + ZPD

494583=8992 494583^494581^^SE^INTERFACE ENGINE LOGICAL LINK PROVIDED BUT NOT FOU
ND
MSH^~|\&^RPMS-MPI^8992~HL7.2013-DEMO.NA.IHS.GOV:5201~DNS^MPI^8990~:~DNS^20210413
065304-0700^^ADT~A28~^8992 494583^P~^2.4^^^AL^NE^ + EVN + PID + ZPD
----------------------------- MPI SUMMARY END -------------------------------
Enter RETURN to continue or '^' to exit:
```

Figure 3-13: MPI Application Status report (STAT)

3.4.5   Viewing Alerts

If there is a messaging issue on the RPMS side, the "Enter VA to jump to VIEW ALERTS" option message will display. If you see this prompt, type **VA** to view alerts. When the list displays, take a screen capture and send it to the IHS IT Service Desk.

1. At the "Select MPI Reports and Debug option" prompt, type **VA** and press Enter.

In this example (Figure 3-14), there are nine messages that have an error. Choose a message to view more details.

```
   DAT     MPI Messages by Date
   TOT     MPI Queue and msg Totals
   ICN     MPI Missing ICN Report
   UN      MPI Print Unsuccessful Messages
   STAT    Display the MPI application status report

MPI MSG MFN:204: POSSIBLE GARBLED MESSAGE
MPI MSG MFN:204: POSSIBLE GARBLED MESSAGE
MPI MSG MFN:204: POSSIBLE GARBLED MESSAGE
Enter "VA to jump to VIEW ALERTS option

Select MPI Reports and Debug option Option: va View Alerts
1.I MPI MSG MFN:204: POSSIBLE GARBLED MESSAGE
2.I MPI MSG MFN:204: POSSIBLE GARBLED MESSAGE
3.I MPI MSG MFN:204: POSSIBLE GARBLED MESSAGE
4.I MPI MSG MFN:204: POSSIBLE GARBLED MESSAGE
5.I MPI MSG MFN:204: POSSIBLE GARBLED MESSAGE
6.I MPI MSG MFN:204: POSSIBLE GARBLED MESSAGE
7.I MPI MSG MFN:204: POSSIBLE GARBLED MESSAGE
8.I MPI MSG MFN:204: POSSIBLE GARBLED MESSAGE
9.I MPI MSG MFN:204: POSSIBLE GARBLED MESSAGE
       Select from 1 to 9
       or enter ?, A, I, D, F, S, P, M, R, or ^ to exit: 1

Processed Alert Number 1
MPI MSG MFN:204: POSSIBLE GARBLED MESSAGE

Continue (Y/N) or F(orward) or R(enew) YES//
```

Figure 3-14: Issue with garbled messages (VA option)

3.5   HL7 ACK Codes

The HL7 table of ACK codes contains three automated items: CA, CE, and CR. The Acknowledgement Accept (AA) message is sent when the application successfully processed and executed the requested function. The AE message is sent if the application was unsuccessful in executing the requested MPI function due to an internal application error.

Table 3-1: HL7 Table 0008—Acknowledgement Code

Value	Description
AA	Original mode: Application Accept–Enhanced mode: Application Acknowledgement: Accept
AE	Original mode: Application Error–Enhanced mode: Application Acknowledgement: Error
AR	Original mode: Application Reject–Enhanced mode: Application Acknowledgement: Reject
CA	Enhanced mode: Accept Acknowledgement: Commit Accept
CE	Enhanced mode: Accept Acknowledgement: Commit Error
CR	Enhanced mode: Accept Acknowledgement: Commit Reject

3.6   Receiving MPI Data

When an A28 (Add a Patient) message is successfully processed, the MPI composes an MFN message containing a list of all treating facilities that the patient is linked to in the MPI. This MFN is sent to all the linked facilities in the MFN message. This message was used to update the TREATING FACILITY LIST (#391.71) file in RPMS. Beginning in p2, this file has been deprecated, and the AGMPI application marks the MFN message complete with no further processing.

3.7   Updates to the MPI

When a patient record is edited using the Patient Registration (AG) edit screens, certain fields contain triggers that create records in the ADT/HL7 PIVOT file that are then processed by a background job. This creates A08 (Patient Update) messages to send the updated or edited fields to the MPI.

3.8   Errors on Outbound Messages

RPMS outbound ADT-A28, ADT-A08, ADT-A01, and ADT-A03 messages that cannot send data to the MPI send an alert to individuals in the mail group AGMPI MPI. Along with the messages, patient information is stored in the parameters. If a general error occurs, more information is provided in the alert, which allows the user to debug.

Message errors for outbound messages are displayed in Section 3.8 and for inbound messages in Section 3.9.

3.8.1   Unable to Build HL7 Message – HLO Message Could Not be Created

All outbound messages contain a Message Header (MSH) and Event (EVT) segment. If HLO is able to open and build the MSH segment for a message, but cannot create the EVT segment, the "Unable to build HL7 message. HLO message could not be created" error alert is generated. This is a fatal error and indicates a problem associated with the HLO HL7 application, not the AGMPI application. The most likely cause is an error installing a new HL7 patch.

3.8.2   EVT Segment Could Not be Created

All outbound messages contain a MSH and EVT segment. If HLO is able to open and build the MSH segment for a message, but cannot create the EVT segment, the "EVT segment could not be created" error alert is generated. This is a fatal error and indicates a problem associated with the HLO HL7 application and not the AGMPI application. The most likely cause is an error in installing a new HL7 patch.

3.8.3   MSA Segment Could Not be Created

All outbound messages contain a MSH and EVT segment. If HLO is able to open and build the MSH segment for a message, but cannot create the EVT segment, the "MSA segment could not be created" error alert is generated. This is a fatal error and indicates a problem associated with the HLO HL7 application, not the AGMPI application. The most likely cause is an error in installing a new HL7 patch.

3.9   Errors on Inbound Messages

Errors can be generated for a variety of reasons. Inbound messages that cannot be filed in RPMS from MPI send an alert to people in the mail group RPMS MPI. RPMS Inbound message errors and descriptions are displayed below:

3.9.1   MPI General ACK Error

```
"MPI ERR ACK IEN "_ACKIEN_" – MSG IEN "_HLMSGIEN_" :: "_ERROR
```

Figure 3-15: MPI ACK Error

In Figure 3-15, the ACK message ID is returned along with the ID of the acknowledgement message and the error message.

4.0   Debugging

4.1   Testing Whether Ensemble is Running via Cache System Status

Follow these steps to determine if Ensemble is running:

1.   At the programmer prompt, type **D ^%SS** and press Enter.

The bold type in Figure 4-1 indicates that the Ensemble production is running. Refer to the lines with Ens.Queue.

```
HLOMPI>D ^%SS
Cache System Status: 1:09 pm 04 May 2010
Process  Device Namespace Routine   CPU,Glob  Pr User/Location
1236         CONTROL   0,0 7
1372         WRTDMN 42405,1942148
652          GARCOL 0,0 7
1460         JRNDMN 216108,0
1528         EXPDMN 0,0 7
3132 //./nul   EDR %ZTMS1 15868650,3117048 7   %System
3072 //./nul   %SYS   MONITOR   510765,33 7
3360 //./nul   %SYS   CLNDMN 14535,669    7
3528 //./nul   %SYS   RECEIVE   1120980,1546077
3560 //./nul   %SYS   ECPWork   0,0    7   ECPWORK
3572 //./nul   %SYS   ECPWork   0,0    7   ECPWORK
2152 localhost HLOMPI %SYS.cspServer2 14166525,3242444 7   UnknownUser
3584 //./nul   %SYS   ECPWork   0,0    7   ECPWORK
3596 //./nul   %SYS   ECPWork   0,0    7   ECPWORK
3608 //./nul   %SYS   ECPWork   0,0    7   ECPWORK
3620 //./nul   %SYS   ECPWork   0,0    7   ECPWORK
3632 //./nul   %SYS   ECPWork   0,0    7   ECPWORK
3672 //./nul   %SYS   ECPWork   0,0    7   ECPWORK
1132 |TCP|56773   %SYS   %SYS.SERVER   0,0 7
1360 //./nul   %SYS   LMFMON 634440,822    7
3156*    |TNT|localhost:1895|3156   %SYS   SYS.Process   16806897,8537637    HLOMPI
2816 //./nul   HLOMPI %ZTM   14046165,1926971 7   %System
2852 //./nul      %ZTM   14450085,1922222 7   %System
2412 //./nul   %SYS   %MONAPP   11641770,4080817
2424 //./nul   %SYS   %SYS.Task 2507415,2058687      TASKMGR
3276 //./nul      %ZTMS1 15866355,3116597 7   %System
2512 //./nul   EDR %ZTM   14450340,1922253 7   %System
6064 //./nul   %SYS   %CSP.Daemon   439365,46162 7
5848 localhost %SYS   %SYS.cspServer2
5324 localhost DOCBOOK   %SYS.cspServer2 1020510,424831   7   UnknownUser
4308 NPA24-530 HLOMPI %SYS.BINDSRV 781830,136034 7   UnknownUser
3928 //./nul   HLOMPI Ens.Queue 29835,3067    7   HLOMPI
2564 //./nul   HLOMPI Ens.Queue 67320,4671    7   HLOMPI
4360 //./nul   HLOMPI Ens.Queue 6885,962  7   HLOMPI
692  //./nul   HLOMPI Ens.Queue 36720,2252    7   HLOMPI
4972 //./nul   HLOMPI Ens.Queue 19635,1634    7   HLOMPI
1180 //./nul   HLOMPI Ens.Queue 14790,1246    7   HLOMPI
4204 //./nul   HLOMPI Ens.Queue 255,57 7   HLOMPI
716  //./nul   HLOMPI Ens.Queue 990420,276952 7   HLOMPI
3516 //./nul   HLOMPI Ens.Queue 30090,6653    7   HLOMPI
5900 //./nul   HLOMPI Ens.Queue 255,53 7   HLOMPI
```

```
5868  //./nul   HLOMPI Ens.Queue 3315,411  7   HLOMPI
5204  //./nul   HLOMPI Ens.Queue 14280,1260   7   HLOMPI
5072  |TCP|5026 HLOMPI EnsLib.HL7.Adapter.TCPInboundAdapter 2204985,5218097    HLOMPI
2072  |TCP|8899 HLOMPI Ens.Queue 1017705,155258   7   HLOMPI
1164  //./nul   HLOMPI Ens.Queue 306765,36576 7   HLOMPI
6116  //./nul   HLOMPI Ens.Queue 61965,6773   7   HLOMPI
240   //./nul   HLOMPI %ZTMS1 3578160,7013467     %System
1824  NPA24-530 HLOMPI %SYS.BINDSRV 687225,1509537  UnknownUser
132   localhost DOCBOOK  %SYS.cspServer   23315,348 7  UnknownUser
```

Figure 4-1: Cache system status to determine if Ensemble is running

4.2   Debugging Tools

FileMan or HLO menu can be used to debug or to view messages from the RPMS side of the AGMPI application.

Figure 4-2 shows a message header. The message header shows where a message came from, its status, the direction it is going, its port, HLO application, and header segments.

```
MESSAGE ID: 14752 7        MESSAGE BODY: MAY 04, 2010@11:18:49
DIRECTION: OUTGOING        LINK: MPI
QUEUE: MPI RPMS           REMOTE PORT: 8899
SCHEDULED PURGE DATE/TIME: MAY 11, 2010@11:18
APPLICATION ACK RSPNS TAG: AACK      APPLICATION ACK RSPNS RTN: AGMPIHLO
ACCEPT ACK RSPNS TAG: CACK        ACCEPT ACK RESPNS RTN: AGMPIHLO
TRANSMISSION DATE/TIME: MAY 04, 2010@11:18
ACCEPT ACK'D: YES       COMPLETION STATUS: SUCCESSFUL
HDR SEGMENT,COMPONENTS 1-6: MSH^~|\&^RPMS-
MPI^14752~161.223.91.63:5026~DNS^MPI
^00001~:8899~DNS

HDR SEGMENT,COMPONENTS 7-END: ^20100504111849-0600^^VTQ~Q02^14752
7^T~^2.4^^^A
L^NE^

   DATE/TIME OF ACCEPT ACK: MAY 04, 2010@11:18
   ACCEPT ACK MESSAGE ID: 14752 7 ACCEPT ACK MSA SEGMENT: MSA
```

Figure 4-2: Viewing a message header using FileMan

Use the Inquiry option in FileMan to view an HLO message body. The message body contains facility information, such as station number. If debugging is required due to a missing segment, the station number may be missing or may be an incorrect number.

In Figure 4-3, the station number (14752) is an example of what must be double checked for accuracy. The ZPD (Figure 4-3, bold at the bottom) contains RPMS-specific information such as Tribe, blood quantum, and chart numbers, and can be used for reference.

```
VA FileMan 22.0
Select OPTION: INQUIRE TO FILE ENTRIES
OUTPUT FROM WHAT FILE: MAIL GROUP// 1 HLO MESSAGE BODY
Select HLO MESSAGE BODY DATE/TIME ENTERED: T MAY 04, 2010
1 5-4-2010@11:18:00 ACK Q02
2 5-4-2010@11:18:49 VTQ Q02
3 5-4-2010@12:16:00 ACK Q02
4 5-4-2010@12:16:00 ACK A28
5 5-4-2010@12:16:00 ACK A28
Press <RETURN> to see more, '^' to exit this list, OR
CHOOSE 1-5: 2 5-4-2010@11:18:49 VTQ Q02
ANOTHER ONE:

STANDARD CAPTIONED OUTPUT? Yes// Y (Yes)
```

```
Include COMPUTED fields: (N/Y/R/B): NO// - No record number (IEN), no Computed
Fields
DATE/TIME ENTERED: MAY 04, 2010@11:18:49
BATCH: NO MESSAGE TYPE: VTQ
EVENT: Q02 HL7 VERSION: 2.4
SEGMENTS:
EVN^VTQ^^^^398~SENDER NAME~~~~~~USIHS&&0363~L~~~NI~IHS FACILITY ID -NOT-A-REAL
FACILITY&14752&L^^14752
PID^1^V^V~~~USIHS&&0363~NI~IHS FACILITY ID – NOT-A-REAL FACILITY&14752&L|605050
410P~~~USSSA&&0363~SS~IHS FACILITY ID – NOT-A-REAL FACILITY&14752&L|9290~~~USIHS
&&0363~PI~IHS FACILITY ID – NOT-A-REAL FACILITY&14752&L|V~~~USIHS&&0363~NI~IHS F
ACILITY ID – NOT-A-REAL FACILITY&14752&L~~200910205571-0700^^NEW~PATIENT~~~~~L^~
~~~~~M^20100504^F^^^~~~~~~P~|~~~~~~N^^~~|~~|~~|~~^^^8^^^^^^^^^^^Y^^|
ZPD^1^084^D^01^FULL^9290~0000012323~516~19316~17000000
Select HLO MESSAGE BODY DATE/TIME ENTERED:
```

Figure 4-3: Message Body using FileMan

1. At the "Select OPTION" prompt, type **INQUIRE TO FILE ENTRIES** and press Enter.

2. At the "OUTPUT FROM WHAT FILE: MAIL GROUP" prompt, type **1 HLO MESSAGE BODY** and press Enter.

3. At the "Select HLO MESSAGE BODY DATE/TIME ENTERED" prompt, either enter the **date and time or Enter the message ID** number and press Enter.

4. At the "CHOOSE" prompt**, choose the message number** and press Enter.

5. At the "ANOTHER ONE" prompt, press Enter or choose another message.

6. At the "STANDARD CAPTIONED OUTPUT" prompt, type **Y** (Yes) and press Enter. The message body displays.

Figure 4-4 shows an alternate method of viewing message bodies and headers.

Figure 4-4: HLO Main menu for viewing a message body

Appendix A   Rules of Behavior

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

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

- For a listing of general ROB for all users, see the most recent edition of *IHS General User Security Handbook* (SOP 06-11a).

- For a listing of system administrators/managers rules, see the most recent edition of the *IHS Technical and Managerial Handbook* (SOP 06-11b).

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

Glossary

Archiving

The storing of historical or little-used data off-line (often on tape).

Configuration Diagram

A graphical representation of the business hosts in a production.

Entry Point

Entry point within a routine that is referenced by a "DO" or "GOTO" command from a routine internal to a package.

File

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

FileMan

The database management system for RPMS.

Flowsheet

A tabular format for organizing and displaying data in a special section of the health summary.

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).

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 menu-type options are displayed, the prompt includes the name of the menu preceded by the word "Select" and followed by the word "option," as in "Select Menu Management option" (the menu's "Select" prompt).

Namespace

A unique set of two to four alpha characters assigned by the database administrator to a software application.

Option

An entry in the Option file. As an item on 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, non-interactively, by TaskMan.

Production

The unit of delivery for Ensemble-based development projects.

Production Table

Contains information about the currently running production.

Panel

A tabular format for presenting a series of clinical measurements or results in the health summary.

Queuing

Requesting 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.

Utility

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

Acronym List

Acronym	Term Meaning
A01	Patient check-in
A03	Checkout and discharge
A08	Patient update
A28	Add patient
AA	Acknowledgement Accept
ACK	Acknowledgement codes
ADT	Admission, Discharge, Transfer
AE	Acknowledgement Error
AG	Patient Registration
AR	Acknowledgement Reject
CA	Commit Accept
CE	Commit Error
CISO	Chief Information Security Officer
CR	Commit Reject
DAT	Date
ERR	Error
EUID	Enterprise Unique Identifier
EVT	Event
HIE	Health Index Exchange
HIPAA	Health Insurance Portability and Accountability Act
HLO	HL7 Optimized
ICN	Integration Control Number
IHS	Indian Health Service
ISSO	Information System Security Officer
IT	Information Technology
MFN	Master File Update
MPI	Master Patient Index
MSH	Message Header
NHIN	National Health Information Network
PC	Personal Computers
PHR	Personal Health Record
ROB	Rules of Behavior
RPMS	Resource and Patient Management System
RPT	Report

Acronym	Term Meaning
RS	Resend
SAC	Standards and Conventions
TOT	Total
UN	Unsuccessful print
UPD	Update
VA	Veterans Affairs
VPN	Virtual Private Network
VST	Visit

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