RESOURCE AND PATIENT MANAGEMENT SYSTEM

Dental/EDR Interface

(BADE)

User Manual

Version 1.0 Patch 10
February 2026

Office of Information Technology
Division of Information Technology

Table of Contents

Trademark Notice

1.0 Introduction

For over two decades, Indian Health Service (IHS), Tribal and Urban hospitals and health centers have been using a patient information system called the Resource and Patient Management System (RPMS). RPMS is an integrated system consisting of more than 50 healthcare and administrative applications, many directly interacting with one or more of the other RPMS applications.

With the replacement of the RPMS Dental Data System (roll and scroll) application with an Electronic Dental Record (EDR) system, RPMS interacts with the EDR application to meet the needs of both the Dental Department and the local health program.

The EDR software called Dentrix resides on a separate server. The EDR Interface uses IRIS InterSystems software installed on the RPMS server and Health Level Seven (HL7) formatted messages to send patient and provider (Dentist) information to the EDR system and to receive dental procedures and notes from the EDR system. HL7 messages transmitted from Dentrix are processed and stored in RPMS VA FileMan files to create dental visit data in RPMS. Patient and provider (Dentist) additions and updates completed in RPMS are transmitted to the Dentrix application and ensure the systems are in sync so that newly added patients or providers are selectable in the Dentrix application.

This document focuses on the RPMS side of the EDR Interface (BADE assigned namespace) and provides information and details on the options that are available for RPMS administrators and IT staff to resolve issues, provide maintenance functions and support the interface. Additional technical information can be found in the BADE Technical guide located on the IHS website.

This manual provides essential information to understand the Dental/EDR (Electronic Dental Record) Interface application and to assist in the use of the interface. This document contains information about the following three menus:

- Upload Menu
- Dental Interface Management Menu
- Dental Interface Utilities Menu

This manual will be primarily used by OIT personnel, local site managers, and IT specialists after the successful installation of the interface and for updating and maintaining the interface and troubleshooting issues.

2.0 System Navigation

2.1 System Overview

The EDR Interface (BADE) has several different functions. These functions are described starting in Section 3.0.

2.2 Conventions

RPMS has established certain terms and operating procedures (conventions) for EDR. The following is a brief discussion on those conventions, the knowledge of which enables a user to learn how to use the system quickly. While reading the following explanations, refer to the keyboard to ensure correct identification of each key and command function.

2.2.1 The Enter Key

At many points in this manual the user is instructed to type some letters and press the Enter key. The Enter key refers to the key on the keyboard marked with the word "Return" or "Enter."

2.2.2 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), simply type a response and then press Enter. If a prompt has a default response, but you want the response to be blank, you leave the response blank by deleting the default text or typing an "at" sign (@) at the prompt after the default response.

2.2.3 Screenshots

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

```
UPL     Dental Interface Upload Menu ...
MAN     Dental Interface Management ...
UTIL    Dental Interface Utilities ...
```

Figure 2-1: Example screenshot of Dental Interface

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

- After typing an entry, press the Enter key to create the entry.
- If the screenshot shows only the two double slashes (//) without any boldface type, simply press the Enter key without typing anything.

2.2.4 Help 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 he/she wants to know more about the menu choices, type a single question mark (**?**) to display more information.

2.2.5 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 the user 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 "^" character.

2.2.6 The "Select Device:" Prompt

Whenever the software is about to 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 screen, type **HOME** or **0**.
- For help responding to the "Select Device" prompt, contact your site manager.

Some reports also allow the user to type **Q** (for Queue) 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 a search or print. After typing Q, the system displays the "Queue to Print on Device" prompt. At this point, type the name of the printer on which you want to print the report.

3.0 EDR Menu Option

The Dental Interface Main menu includes options in support of the EDR Interface, including the initial setup and transmission of HL7 messages. The interface transmits and receives the following HL7 messages:

Transmitted from RPMS to the EDR system:

- A28 (Add a Patient)
- A31 (Update a Patient)
- MFN-M02 (Add or Update a Provider)

Received from the EDR system:

- DFT-P03 (Dental Procedures)
- MDM-T04 (Finalized Dental Progress Notes if enhancement is enabled)

The Dental Interface Main Menu includes the following sub-menus shown in Figure 3-1 below.

```
UPL     Dental Interface Upload Menu ...
MAN     Dental Interface Management ...
UTIL    Dental Interface Utilities ...
```

Figure 3-1: The Dental Interface Main Menu

3.1 Dental Interface Upload Menu (UPL)

Before EDR is implemented, the site works with technical support staff to install the Dentrix application software and set up the EDR interface. On the RPMS system, this consists of installing all the BADE patches, configuring RPMS files and the BADE Production. Review the BADE Installation Manual for more details.

Technical support staff will use the upload options to transmit all patients and providers (Dentists) to the external Dentrix system so that the systems are synchronized. After implementation, these transmissions are done automatically using the BADE protocols (see the BADE Technical manual for more details).

For most RPMS sites, setup and configuration has already been completed. These upload options should only be used once. Do not use these options unless directed and coordinated with Dentrix and IHS technical staff, for instance if the RPMS system crashed and the EDR Interface needs to be re-installed.

From the **Dental Interface Main Menu**, type **UPL** and press the Enter key to display the **Dental Interface Upload Menu**. Most of these options are used for new EDR site implementations. Do not use these options to upload patient or provider data if you are already using the EDR interface. These options should be inactivated after the initial upload of patient and provider data and should not be provided to all users, just the IT staff and Site Manager.

Figure 3-2 shows the **Dental Interface Upload Menu** and includes options to upload, pause, restart and display the transmit process for patients and providers.

```
Select Dental Interface Main Menu <TEST ACCOUNT> Option: upl
pload Menu


   UAP     Load all Patients
              **> Out of order:  Upload completed
   PUP     Pause Patient Load
              **> Out of order:  Upload completed
   RUP     Restart Patient Upload
              **> Out of order:  Upload completed
   UPV     Upload All Providers
              **> Out of order:  Upload completed
   PPV     Pause Provider Upload
              **> Out of order:  Upload completed
   RPV     Restart Provider Upload
              **> Out of order:  Upload completed
   DSP     Display Progress
   MALL    Upload all Merged patients
              **> Out of order:  **ACCESS DISABLED**
   PMRG    Pause Merge Upload
              **> Out of order:  **ACCESS DISABLED**
   RMRG    Restart Merge Upload
              **> Out of order:  **ACCESS DISABLED**
   ASU     Active ASUFAC Display
   PER     EDR Patient File Count Errors
   TCT     Pt Count for Throttle action

                Press 'RETURN' to continue, '^' to stop:
              **> Out of order:  Upload completed
   THR     Throttle Patient Upload
              **> Out of order:  Upload completed
```

Figure 3-2: The Dental Interface Upload Menu

The following options are used to perform patient upload tasks for new EDR sites. For sites that already implemented EDR, most of the options will display **Out of order: upload completed** as shown in Figure 3-2. The Merge options are mentioned in Section 3.1.5 and are disabled in BADE v1.0 p10.

- **Load all Patients (UAP)**: uploads all patients to the EDR (for new sites)
- **Pause Patient Load (PUP)**: pauses the upload if issues arise
- **Restart Patient Upload (RUP)**: restarts the upload after paused
- **EDR Patient File Count Errors (PER)**: identifies which patients could not be uploaded, viewed after the upload is complete

- **Pt Count for Throttle Action (TCT)**: sets the number of patients to process before the upload pauses. If the system is running slow and messages in the queue are backing up, the interface can stop the upload for a few seconds to allow the processing to catch up. This option allows the user to specify how many patients should be processed before the interface checks to see whether the queue is backed up. This value specifies the number of patients processed per throttling interval. The default is 10.
- **Throttle Patient Upload (THR)**: sets a timeframe (in seconds) that throttles the upload. This option allows the user to specify the number of seconds (up to 20) that the system should wait before continuing. The interface processes a certain number of patients, then checks to see if it should pause for the specified number of seconds before continuing. The default is 1.

3.1.1 Load All Patients (UAP)

This task should be done only once during the initial setup and configuration of EDR. This option should be run by IT Support staff and the task, once initiated, should be monitored regularly until completed.

Use the option to upload all living patients to the EDR. This option should be run after the Provider Upload has been completed. This option loops through the entire patient file and is a tasked job that could take considerable amount of time to complete, depending on the size of the patient file. You can select specific locations or all locations.

When selecting this option, the user is prompted to provide a start time so the upload can be set to start and run after hours. You can select **Now** to run the task immediately. A task number is displayed after the start time is entered. Expect the upload process to take about one hour for each 5000-8000 patients depending on system performance.

Use the **Pause Patient Load** option to stop the load (Figure 3-4). Use the **Restart Patient Upload (RUP)** to restart the upload process (Figure 3-5).

While an upload job is running, the **Restart Patient Upload** option may not be used. If the restart option is selected while the upload is running, a message indicating that the upload is already running will be displayed.

After the upload, new patient data, patient updates, and provider information are transmitted to Dentrix using triggers set up in RPMS BADE protocols. When a patient is registered or edited, an HL7 message is automatically transmitted to Dentrix. Likewise, editing dentist data transmits a message when using the **AVA Add/Edit Providers** option.

It is possible to manually send a message through the interface or to reprocess a message that has already been sent. These options are described in the **Dental Interface Management** menu in Section 3.2.

```
This option transmits patient data to a Dentrix server

This is for new sites only, do not use if you already implemented EDR!!


Do you want to push specific locations in RPMS to Dentrix?? Y// ES

Enter the total number of locations you wish to transmit for this Patient Push
 select "^" to exit:  1
Enter Location Name or ASUFAC code:
Select LOCATION NAME: 232101  2016 GOLD           HEADQUARTERS WEST       ALBUQ
ERQUE       01                     HC        8213
You entered the following location(s):

DEMO

Do you wish to continue with the patient push? (Y/N)
YY

Continuing with the Patient Upload Process by Location

Requested Start Time: NOW//
```

Figure 3-3: The Load All Patients Option (UAP)

The number of patients at a site can be quite large, so the initial patient upload is the most time consuming. Users can remain on the system during the upload, but the preference is to run the patient upload during off peak hours. The **Display Progress** option (Section 3.1.4) shows the progress of the upload and tracks the last patient uploaded.

3.1.2 Pause and Restart Patient Load

Use the **Pause Patient Load (PUP)** option to stop the load (Figure 3-4). This option is used if there are issues and the upload does not appear to be working. If the value is already set to YES, changing the value to NO does not restart the upload, but it does prevent the restart from occurring. The program behaves as if the upload is already running and does not start again. This option is only to be used to STOP the load.

```
2016 GOLD                      RPMS-Dentrix Upload                      Version 1
                                Pause Patient Load

--------- Setting Stop Dental Patient Load  for System: DEMO.IHS.GOV ---------
Pause Dental Patient Load: NO// YES
```

Figure 3-4: Pause Patient Load Option

Use the **Restart Patient Upload (RUP)** option to restart the Patient load process (Figure 3-5) after pausing.

```
Select Dental Interface Upload Menu <TEST ACCOUNT> Option: rest
    1    Restart Patient Upload
    2    Restart Provider Upload
CHOOSE 1-2: 1  Restart Patient Upload
Requested Start Time: NOW//  (NOV 05, 2025@10:33:40)
Task number 2419087
```

Figure 3-5: Restart Patient Upload Option

3.1.3 Provider Upload (UPV)

The number of dentists at any one site is usually not large, so this upload should take less than ten minutes to complete. Only providers belonging to the PROVIDER CLASS of DENTIST (CODE 52) and have a National Provider Identification number (NPI) established before his/her data is transmitted. It's a good idea to review the Dentist list prior to starting the upload (see Management menu in Section 3.2) to ensure these fields are populated.

The following options can be used when uploading Provider (Dentist) data. For sites already using EDR, the following options will be disabled. These options are like the Patient Upload options: the user is prompted to provide a start time, and a task number is displayed after the start time is entered. You can select **Now** to run the task immediately.

- **Upload All Providers (UPV)**: uploads all Dentists to the EDR
- **Pause Provider Load (PPV)**: pauses the upload if issues arise
- **Restart Provider Upload (RPV)**: restarts the upload after paused

This option can be run while users are on the system, and the pause and restart options are usually not needed since it takes just a few minutes to complete.

```
Select Dental Interface Upload Menu <TEST ACCOUNT> Option: upv  Upload All Provi
ders
Requested Start Time: NOW//  (NOV 06, 2025@09:15:55)
Task number 6955268
```

Figure 3-6: Upload All Providers Option

If the Dentist does not have an NPI number, you will receive an RPMS alert (Figure 3-7), but you must be a member of the "RPMS Dental" Mailman group (see Section 6.1).

```
Provider: DENTAL,PROVIDERTWO [3150]. No NPI.  Can't create STF.
```

Figure 3-7: Provider Alert Message

For this issue, using the **AVA** option, add the NPI number then use the **AVA Add/Edit Providers** option to trigger the transmission of the Dentist to Dentrix, see Figure 3-8.

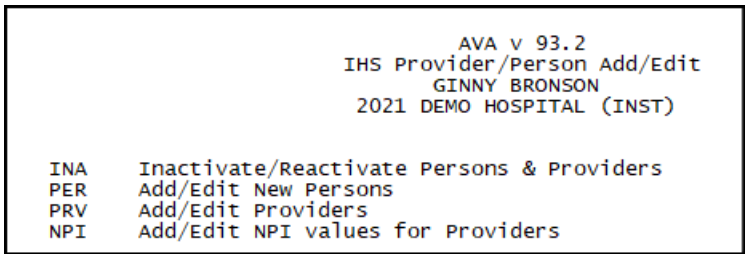


Figure 3-8: AVA Menu

3.1.4 Display Progress

Figure 3-9 shows the status of the upload, either currently running or completed using the **Display Progress (DSP)** option. This option is used to determine the progress of the patient and provider upload to display how many were processed (uploaded) and if the upload is complete.

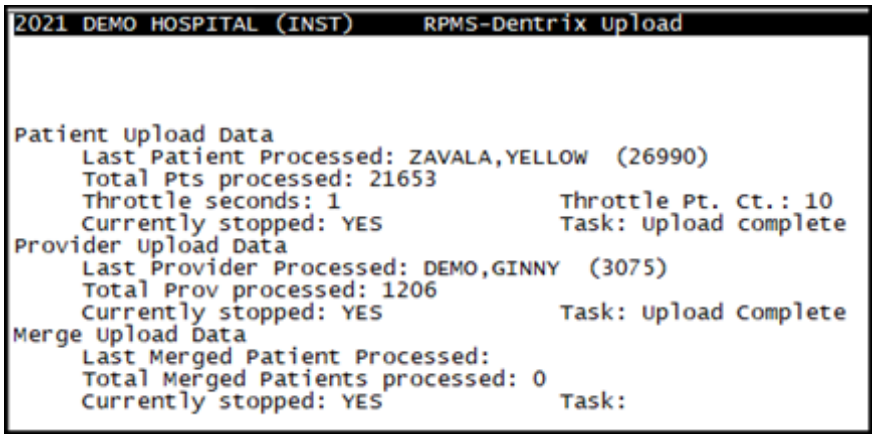


Figure 3-9: Display Progress Option

Last Patient Processed: displays the last patient uploaded and IEN number

Total Pts processed: total number of patients processed (uploaded)

Throttle seconds: timeframe (in seconds) that throttles the upload, default is 1; the interface processes a certain number of patients, then checks to determine if it should pause for the specified number of seconds before continuing

Throttle Pt. Ct.: the number of patients to process before the interface pauses, default is 10 (processes 10 patients per throttle timeframe)

Currently stopped: it should display “Yes”, unless it is running

Task: if the upload is running the task number will be displayed, otherwise it should state “Upload complete” or blank

Last Provider Processed: displays the last uploaded Dentist

Total Prov processed: total number of Dentists processed

Currently stopped: it should display “Yes”, unless it’s running

3.1.5 Patient Merge

The patient merge options have been disabled since the RPMS Merge application is not supported and no longer being used.

3.1.6 Active ASUFAC Display (ASU)

This option is used to find out how many patients are active for each ASUFAC location. This information is used to determine how many patients will be transmitted to Dentrix as well as verification with Dentrix after the upload.

```
    A S U F A C  D I S P L A Y


Active  Count  Facility                                ASUFAC
Active:  137   2016 GOLD                               232101

Inactive Count Facility                                ASUFAC
Press ENTER to continue...
```

Figure 3-10: Active ASUFAC Display Option

3.1.7 EDR Patient File Count Errors (PER)

This option displays the total number of patient errors including those missing Health Record Numbers. This data is stored in the parameters file for BADE EDR ERROR PTS and can be retrieved using the option shown in 25 3.3.1

```
Patient Counts
-------------------------------------------------------
VA PATIENT (DPT) COUNT:  137
PATIENT (AUPNPAT) COUNT:  137
AUPNPAT ENTRY MISSING DPT COUNT:  0
DPT ENTRY MISSING AUPNPAT COUNT:  0
AUPNPAT ENTRY MISSING A DIVISION/HRCN (A41) COUNT:  0
DPT MISSING "B" XREF COUNT:  0


Press ENTER to continue...
```

Figure 3-11: EDR Patient File Count Errors option

Below is a brief explanation of each line in the Patient File Counts report:

VA PATIENT (DPT) COUNT: total patient count in the VA Patient file

PATIENT (AUPNPAT) COUNT: total patient count in the Patient file

AUPNPAT ENTRY MISSING DPT COUNT: patients that exist in the AUPNPAT file, but not the VA PATIENT file

DPT ENTRY MISSING AUPNPAT COUNT: patients that exist in the VA PATIENT file, but are missing in the AUPNPAT file

AUPNPAT ENTRY MISSING A DIVISION/HRCN (A41) COUNT: patients that are missing a division and/or a health record number for that division

DPT MISSING "B" X REF COUNT: patients that are missing the B x-reference that is required for certain patient lookups and should be present

3.2 Dental Interface Management Menu (MAN)

Below is the standard **Dental Interface Management Menu**.

```
A28     Send a Single A28 Message
A31     Send a Single A31 Message
MFN     Send a Single MFN Message
REP     Reprocess an Inbound HL7 Message
RES     Resend an Outbound HL7 Message
CLN     Set Default Clinic
DTI     Set Default Time for Dental Visit
DUSR    Default User for Interface
DPR     Set Default Days for Message Purge Retention
PRO     Dentist List
PUR     Manual Purge EDR HL7 Messages
RPC     EDR Dental Notes Menu ...
```

Figure 3-12: Dental Interface Management Menu

The **Dental Interface Management** menu provides the following options for sending messages and maintaining the interface.

- **A28 Send a single A28 Message.** This option sends a Patient Registration message for one patient.
- **A31 Send a single A31 Message**. This option sends a Patient Update message for one patient.
- **MFN Send an MFN Message.** This option sends a Master File Update message to add or update a provider record. The user can select anyone in the new person file, but messages are only sent for dentists.
- **REP Reprocess an Inbound HL7 Message**. This option will allow the user to reprocess an inbound message received from Dentrix.
- **RES Resend Outbound HL7 Message**. This option allows the user to reprocess an outbound HL7 message which will transmit to Dentrix (patient/provider updates).
- **CLN Default Clinic for Interface.** This option allows the user to specify the default clinic for creating visit records.
- **DTI Default Time for Dental Visit.** This option allows the user to specify the default time when creating visits in RPMS.
- **DUSR Default User for Interfaces.** This option assigns a user to an ASUFAC Clinic, records a user who created the visit, and records a user who last updates the visit.
- **DPR Set Default Days for Message Purge Retention**. This option sets the number of days to keep EDR HL7 messages from being purged by the nightly purge process. The default is 7 days if no value is set.
- **PRO Dentist list**. This option displays the dentists in RPMS. You may select all dentists or just active dentists.
- **PUR Manual Purge EDR HL7 Messages**. This option will purge all Dentrix messages which are older than a certain date.
- **RPC EDR Dental Notes Menu**. This menu provides options to print, purge and reprocess failed dental notes created and transmitted from Dentrix.

3.2.1 Outgoing Patient and Provider Data

After the initial upload, patient and provider additions and updates are normally sent using triggers and protocols. When a new patient is registered or edited using Patient Registration, a message is automatically sent. The **AVA Add/Edit Provider** option is used to transmit Dentist provider data and are automatically sent. However, it is possible to manually send a message using an option in the management menu.

The **Dental Interface Management** options in Sections 3.2.2 through 3.2.6 are used to transmit data to the Dentrix system.

3.2.2 Send a Single A28 Message (A28)

Use this option to transmit a new patient message to Dentrix. This option is used if the patient addition did not transmit after adding a patient in Patient Registration and exiting from the option or saving in the BPRM application.

```
Select Dental Interface Management <TEST ACCOUNT> Option: a28  Send a Single A28
 Message
 Select Patient:  demo,april
                                      F 03-13-1977 XXX-XX-7201   TST 113
Message was sent
Press ENTER to continue...
```

Figure 3-13: Send a Single A28 Message

3.2.3 Send a Single A31 Message (A31)

Use this option to transmit a patient update message. This option is used if the patient update did not transmit after editing a patient in Patient Registration and exiting from the option or saving in the BPRM application.

```
Select Dental Interface Management <TEST ACCOUNT> Option: a31  Send a Single A31
 Message
 Select Patient:  demo,abigail
                                     F 12-23-2021 XXX-XX-3468   TST 235
Message was sent
Press ENTER to continue...
```

Figure 3-14: Send a Single A31 Message

3.2.4 Send a Single MFN Message (MFN)

Use this option to transmit a provider message. This option is used if the provider (Dentist) addition or update did not transmit when using the **AVA Add/Edit Provider** option.

```
Select Dental Interface Management <TEST ACCOUNT> Option: mfn  Send a Single MFN
 Message
Select DENTIST: demo,dentistwo DDS  DEMO,DENTISTWO DDS     DD2          DENTIST
Message was sent...
Press ENTER to continue...
```

Figure 3-15: Send a Single MFN Message

3.2.5 Reprocessing an Inbound HL7 Message (REP)

This option is used to reprocess incoming HL7 messages (dental procedures). The HLB message number included in the alert is used when selecting these options. The issue must be fixed before trying to reprocess or you will get another alert. For example, if there was an issue with an incoming message and an alert was created it will include the HLB message number then you can use the option to reprocess the message.

When using this option, type in two question marks (**??**) to find what is used before the message number-sites can use their domain name or location or just "Dental" shown below. If there are quite a few messages that need to be re-processed or you received another alert after reprocessing, contact IT support to assist.

```
Select Dental Interface Management <TEST ACCOUNT> Option: rep  Reprocess an Inbo
und HL7 Message
Select Message Number: Dental
     1   Dental 200000000001
     2   Dental 200000000002
     3   Dental 200000000003
     4   Dental 200000000004
     5   Dental 200000000005
Press <RETURN> to see more, '^' to exit this list, OR
CHOOSE 1-5: ^

Select Message Number: Dental 200000000001
         ...OK? Yes//   (Yes)

Message Reprocessed successfully
```

Figure 3-16: Reprocess an Inbound HL7 Message option

Figure 3-17 below shows an example of an RPMS alert received that includes the HL7 message number.

```
4.I  Msg: 200001371391 EDR ALERT:  Unable to create visit for message  DEMO
5.I  Msg: 200001371391 EDR ALERT:  Unable to create visit for message  DEMO
```

Figure 3-17: RPMS Alert

3.2.6 Resend an Outbound HL7 Message (RES)

In general, use the options shown in Sections 3.2.2–3.2.4 to reprocess outgoing HL7 messages (Send a Single A28, A31, or MFN message). Figure 3-18 shows an example of the resend option.

```
Select Dental Interface Management <TEST ACCOUNT> Option: res  Resend an Outboun
d HL7 Message
Select Message Number: ??

   Choose from:
   8993 200001365399
   8993 200001365400
```

Figure 3-18: Reprocess an Inbound HL7 Message option

A valid message number can also be found using the **HLO message search** option. Since we usually know the patient or provider name it is easier to use the **A28 (New Patient)**, **A31 (Update Patient)**, or **MFN (Provider/Dentist)** options instead of finding the entry using the Message number.

3.2.7 Default EDR Configuration Settings

The options in Figure 3-19 are used when setting up new EDR sites, or when changes are needed.

Clinic locations and their associated ASUFAC numbers should be set up on both RPMS and Dentrix. If the Dentrix application has a new clinic setup and being used to create dental visit data, but the clinic is not setup correctly, you will receive RPMS alerts stating, "There is no default clinic for this location", if the EDR clinic is not added using the **Set Default Clinic (CLN)** option, or "No location associated with ASUFAC". The two systems must be in sync, otherwise dental visit data will not be processed in RPMS.

```
CLN     Set Default Clinic
DTI     Set Default Time for Dental Visit
DUSR    Default User for Interface
DPR     Set Default Days for Message Purge Retention
```

Figure 3-19: EDR Configuration Settings

3.2.8 Set Default Clinic (CLN)

The **Set Default Clinic** option allows the user to specify the clinic locations that will be used when creating dental visits in RPMS. The clinics are created using the **Supervisor** menu—**Setup a Clinic** option in the Scheduling application. Only RPMS users with the Scheduling security keys for a supervisor can create new clinics.

The main facility and any divisions should already be set up in RPMS (including the Medical Center Division and Institution file) and have assigned ASUFAC location codes. One of the required fields in the Clinic setup (Division) is the Medical Center Division entry for that location (Figure 3-20).

```
Select MEDICAL CENTER DIVISION NAME: 2020 demo hospITAL       8993
ANOTHER ONE:
STANDARD CAPTIONED OUTPUT? Yes//   (Yes)
Include COMPUTED fields:  (N/Y/R/B): NO//  - No record number (IEN), no Computed
 Fields

NUM: 2                                  NAME: 2020 DEMO HOSPITAL
  FACILITY NUMBER: 8993
  INSTITUTION FILE POINTER: 2021 DEMO HOSPITAL (INST)
  PRINT WRISTBANDS: YES                 DEFAULT ROUTING SLIP PRINTER: PAMED1
  TRACK INCOMPLETE SUMMARIES?: NO
  DEFAULT PRIMARY PHYSICIAN: PRIMARY CARE PHYSICIAN
  ARE REPORTS REVIEWED?: NO
  DEFAULT REVIEWING PHYSICIAN: ATTENDING PHYSICIAN
```

Figure 3-20: Medical Center Division file entry using VA FileMan

The general rule is to create the clinic name starting with "EDR" to indicate it's not a standard clinic used for scheduling appointments (Figure 3-21). When setting up a new EDR clinic, the **Clinic Code** should be "Dental" for the main facility and all the divisions. The **Facility** field shown in Figure 3-21 is a pointer to the Institution file. The **Division** field entry points to the Medical Center Division file, in this example the entry is 2020 Demo Hospital.

```
                          SET UP A CLINIC                        Page 1 of 4

CLINIC NAME: EDRHS17                        ABBREVIATION: EDR
   DIVISION: 2020 DEMO HOSPITAL             FACILITY: 2021 DEMO HOSPITAL (

    MEETS AT THIS FACILITY?: YES
 NON-COUNT CLINIC? (Y OR N): NO
INCLUDE ON FILE ROOM LISTS?:
 PRINCIPAL CLINIC:
PHYSICAL LOCATION:                                  TELEPHONE:
      CLINIC CODE: DENTAL
 HOSPITAL SERVICE:

CLINIC OWNERS (responsible for setup)
```

Figure 3-21: Setup a Clinic (using the Scheduling Application)

Since dental visits are created using the incoming HL7 message transmitted from Dentrix and processed using the BADE routines, the **CREATE VISIT AT CHECK-IN** field for all EDR clinics should be set to **No**, in case the site accidently uses it for appointment check-in (Figure 3-22). All other required fields must be entered, even though they are not used by the application.

```
                          SET UP A CLINIC                        Page 4 of 4

 ASK FOR CHECK IN/OUT TIME:
 CREATE VISIT AT CHECK-IN?: NO
```

Figure 3-22: Setup a Clinic (Scheduling Application)

Add the newly created EDR clinic using the option. The main facility should be setup in 90–System and uses the assigned domain name and EDR clinic created (Figure 3-23).

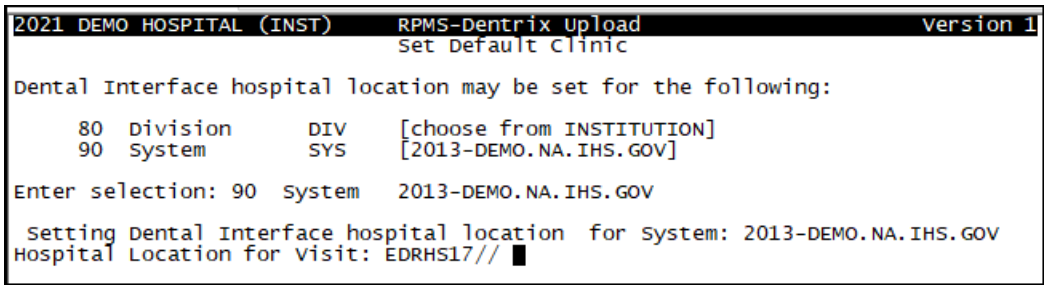


Figure 3-23: Set Default Clinic Option

All divisions using the EDR Interface are added under 80–Division. The institution entry above for the Division should match the EDR clinic(s) created in Scheduling for that division. The clinic entry (EDRHS17) is used for the Visit and added to the Hospital Location field and must have the correct Institution to ensure the ASUFAC values match.

3.2.9 Set Default Time for Dental Visit (DTI)

EDR visits have a default time of 11:38 a.m. Some sites like to use a different time stamp for dental visits and can use this parameter to edit the time stamp. This field is used when creating a dental encounter in the RPMS visit file since Dentrix transmits the encounter date and the date/time the message was transmitted to RPMS.

The default time should be formatted as *military time* with numbers only. *Do not include a colon in the default time value*. Figure 3-24 shows an example of this option. Figure 3-26 shows how the **Default Time** is applied in the visit.

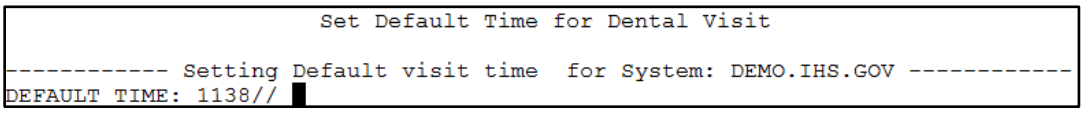


Figure 3-24: Set Default Time Option

3.2.10 Set Default User for Interface (DUSR)

There must be a User defined for each ASUFAC location. Figure 3-25 shows the **Default User** option. Most sites use Adam,Adam as the default user for the System and all their divisions. If an actual user is selected and stops working at the clinic the default user will need to be updated each time.

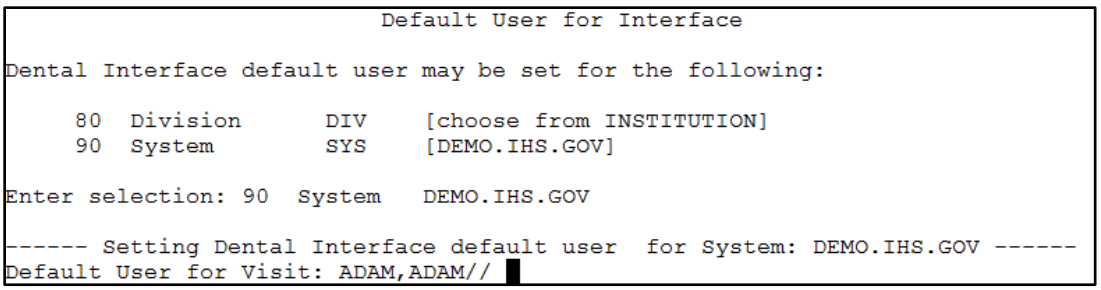


Figure 3-25: Set Default User for Interface Option

The **Default User for Interface** option allows you to specify a user for several fields in the visit file such as who created the visit and who last modified the visit.

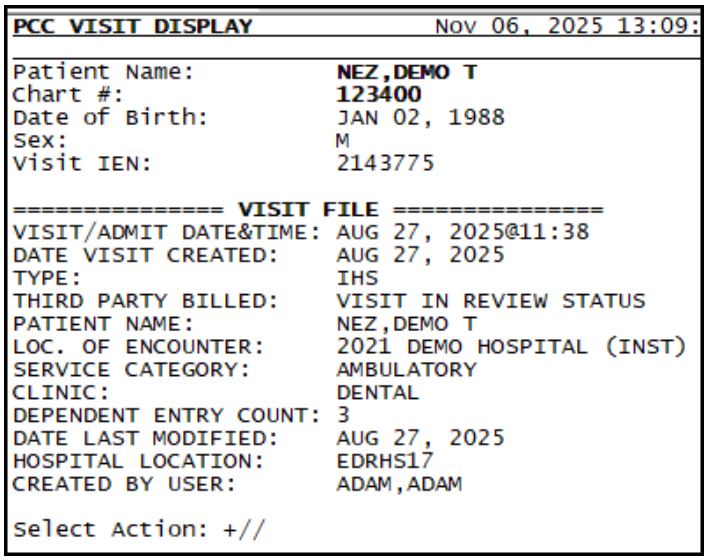


Figure 3-26: RPMS Visit showing the default user name

3.2.11 Set Default Days for Message Purge Retention (DPR)

This option sets the number of days to keep EDR HL7 messages from being purged by the nightly purge process. The default is 7 if no value is set. Recommendation is to retain messages for at least 60 days.

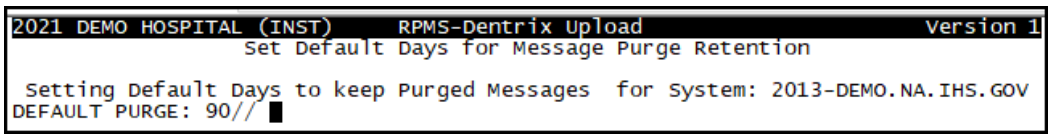


Figure 3-27: Set Default Days for Message Purge Retention Order

3.2.12 Dentist List Option (PRO)

This option displays a list of dental providers. The user can select all active dentists which would be uploaded (during the provider upload option) or all the dentists including inactive, terminated, or those with no NPI.

```
Select Dental Interface Management <TEST ACCOUNT> Option: pro  Dentist List

This option will display dentists in your RPMS system.
You may include dentists who are inactive, or only active dentists.


     Select one of the following:

          A         All
          O         Only Active

Do you want to display (A)ll dentists or (O)nly active dentists?: A//
```

Figure 3-28: Dentist List Option

3.2.13 Manual Purge EDR HL7 Messages (PUR)

This option purges all EDR HL7 messages by date range.

```
Select Dental Interface Management <TEST ACCOUNT> Option: pur  Manual Purge EDR
HL7 Messages

This option will purge all Dentrix messages which are older than a certain date.
For how many days would you like to keep messages:  (0-100): 90//
```

Figure 3-29: Manual Purge EDR HL7 Messages Options

3.2.14 EDR Dental Notes Menu (RPC)

This menu is used to manage dental notes and includes options to print, reprocess and purge saved dental note alerts. This is for sites that have the enhancement enabled to transmit completed clinical notes created in Dentrix (MDM-T04 HL7 messages).

```
  BYDT   Purge Dental Note Alerts based on Purge Date
  NOTE   Set Default TIU Parameter
  PALL   Purge ALL Note Alerts
  PRT    Print Failed Dental Notes
  REPR   Reprocess Dental Notes
```

Figure 3-30: EDR Dental Notes Options

3.2.14.1 Purge Dental Note Alerts based on Purge Date (BYDT)

This option is used to purge dental note alerts by purge date. Figure 3-31 shows that there are not any notes in the past 180 days that need to be purged, otherwise it would ask if you would like to purge those alerts.

```
Select EDR Dental Notes Menu <TEST ACCOUNT> Option: bydt  Purge Dental Note Aler
ts based on Purge Date
** There are no dental note alerts that need to be Purged **

Press enter to continue....:
```

Figure 3-31: Purge Dental Note Alerts based on Purge Date option

3.2.14.2 Set Default TIU Parameter (NOTE)

This option sets the default TITLE in the Parameter Definition file. This setting is for processing incoming Dental Notes created in Dentrix and must be set if the site has the enhancement enabled in Dentrix to transmit MDM-T04 HL7 messages to RPMS.

```
2021 DEMO HOSPITAL (INST)     RPMS-Dentrix Upload                    Version 1
                              Set Default TIU Parameter

------ Setting BADE EDR DENTAL TITLE  for System: 2013-DEMO.NA.IHS.GOV ------
BADE DENTAL TITLE: BADE EDR DEFAULT DENTAL NOTE//
```

Figure 3-32: Set Default TIU Parameter option

3.2.14.3 Purge ALL Note Alerts (PALL)

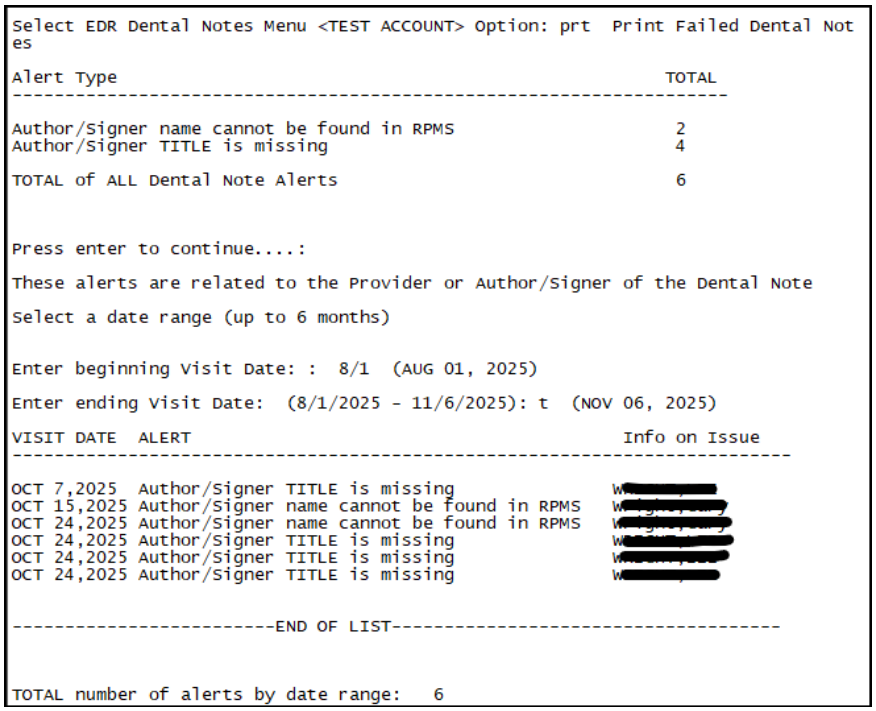
This option will remove all dental note alerts saved in ^XTMP("BADEMDM" temp global. The option will ask the user twice if you would like to purge all note alerts. If you purge all the saved dental note alerts you will not be able to reprocess them.

```
Select EDR Dental Notes Menu <TEST ACCOUNT> Option: pall  Purge ALL Note Alerts
This option deletes/purges ALL dental note alerts


Do you wish to continue (Y/N)?? N// YES

Are you sure.. this removes ALL Dental Note Alerts (Y/N)?? N// NO
Stopping the purge...
```

Figure 3-33: Purge ALL Note Alerts option

3.2.14.4 Print Failed Dental Notes (PRT)

This option will print failed dental notes by selected date range and print the visit date, alert type and total.



```
Select EDR Dental Notes Menu <TEST ACCOUNT> Option: prt  Print Failed Dental Not
es

Alert Type                                                          TOTAL
-------------------------------------------------------------------------

Author/Signer name cannot be found in RPMS                            2
Author/Signer TITLE is missing                                        4

TOTAL of ALL Dental Note Alerts                                       6


Press enter to continue....:

These alerts are related to the Provider or Author/Signer of the Dental Note

Select a date range (up to 6 months)


Enter beginning Visit Date: :  8/1  (AUG 01, 2025)

Enter ending Visit Date:  (8/1/2025 - 11/6/2025): t  (NOV 06, 2025)

VISIT DATE  ALERT                                          Info on Issue
-------------------------------------------------------------------------

OCT 7,2025  Author/Signer TITLE is missing                 W[redacted]
OCT 15,2025 Author/Signer name cannot be found in RPMS     W[redacted]
OCT 24,2025 Author/Signer name cannot be found in RPMS     W[redacted]
OCT 24,2025 Author/Signer TITLE is missing                 W[redacted]
OCT 24,2025 Author/Signer TITLE is missing                 W[redacted]
OCT 24,2025 Author/Signer TITLE is missing                 W[redacted]


-------------------------END OF LIST-----------------------------------


TOTAL number of alerts by date range:   6
```

Figure 3-34: Print Failed Dental Notes option

3.2.14.5 Reprocess Dental Notes (REPR)

This option will reprocess failed dental notes by type (Author/Signer or Provider) and date range selected. Some dental notes cannot be reprocessed and are noted. All issues will need to be corrected, then use the option as shown in Figure 3-38 and Figure 3-39.

Use the print option before you try to reprocess the failed dental note(s). Use the **AVA Add/Edit New Persons** option (Figure 3-35) if the author/signer is missing in RPMS (Name cannot be found in RPMS). The name may be missing since Dentrix users can author a dental note in Dentrix but may not be setup in RPMS as a user. The name must match exactly what is listed in the print or reprocess option. Make sure to add the Title and Service/Section otherwise you can add it using the User Management/Edit an Existing User option (Figure 3-36). The user's electronic signature code fields need to be setup-the block printed name, title and code (Figure 3-37). See Section 5.0 for more information.

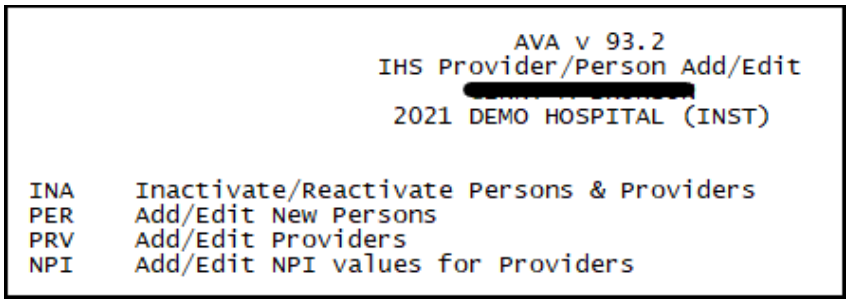


Figure 3-35: AVA Menu

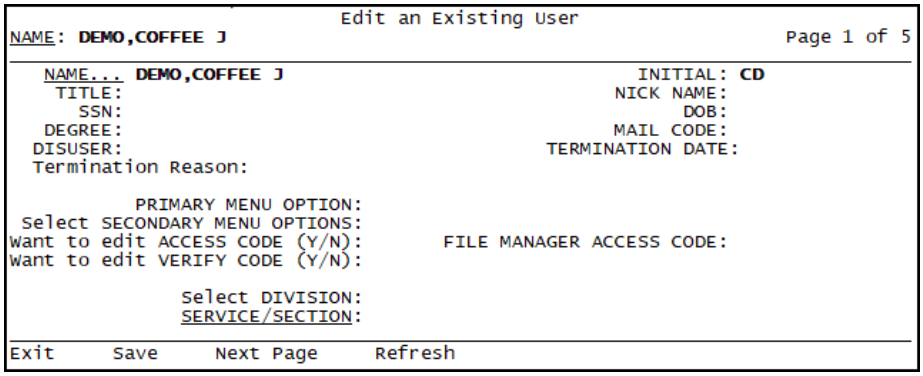


Figure 3-36: User Management-Edit an Existing User

Common alerts that need to be corrected:

- Author/signer name cannot be found in RPMS: Use the **AVA Add/Edit New Persons** option to add the user (see Figure 3-35).
- Author/signer TITLE is missing: Use the **User Management/Edit an Existing User** option (Figure 3-36) and add a title (starts with “Dent”).
- Author/signer TITLE is not a Dental Hygienist, Dental Assistant: Use the **User Management/Edit an Existing User** option (Figure 3-36) and add a valid title.
- Author/signer needs an Electronic Signature Code: Have the user login and using ^TBOX add their Signature Block Title, Printed Name and Code.

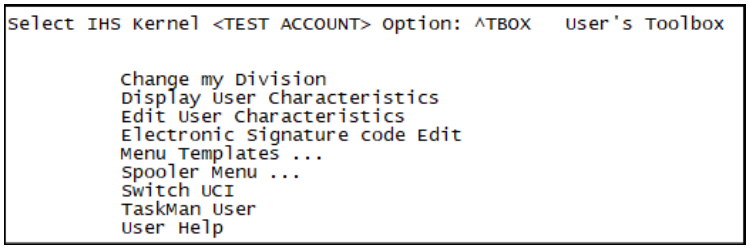
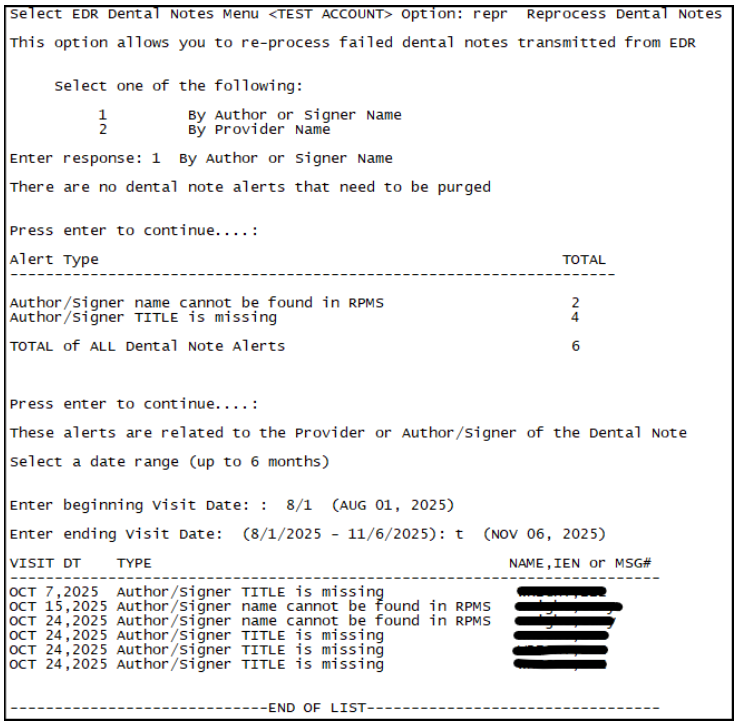


Figure 3-37: TBOX-User's Toolbox options/Electronic Signature code Edit option



```
Select EDR Dental Notes Menu <TEST ACCOUNT> Option: repr  Reprocess Dental Notes
This option allows you to re-process failed dental notes transmitted from EDR

     Select one of the following:

          1         By Author or Signer Name
          2         By Provider Name

Enter response: 1  By Author or Signer Name
There are no dental note alerts that need to be purged

Press enter to continue....:
Alert Type                                                          TOTAL
-------------------------------------------------------------------------

Author/Signer name cannot be found in RPMS                            2
Author/Signer TITLE is missing                                        4

TOTAL of ALL Dental Note Alerts                                       6


Press enter to continue....:
These alerts are related to the Provider or Author/Signer of the Dental Note
Select a date range (up to 6 months)

Enter beginning Visit Date: :  8/1  (AUG 01, 2025)
Enter ending Visit Date:  (8/1/2025 - 11/6/2025): t  (NOV 06, 2025)
VISIT DT    TYPE                                          NAME,IEN or MSG#
-------------------------------------------------------------------------
OCT 7,2025  Author/Signer TITLE is missing                [redacted]
OCT 15,2025 Author/Signer name cannot be found in RPMS    [redacted]
OCT 24,2025 Author/Signer name cannot be found in RPMS    [redacted]
OCT 24,2025 Author/Signer TITLE is missing                [redacted]
OCT 24,2025 Author/Signer TITLE is missing                [redacted]
OCT 24,2025 Author/Signer TITLE is missing                [redacted]


------------------------------END OF LIST---------------------------------
```

Figure 3-38: Reprocess Dental Notes option 1

```
Press enter to continue....:

Alerts that show the MSG# (Message number), CANNOT BE PROCESSED DUE TO:
No Provider (IEN) Number or Author/Signer name was transmitted
You can review the HLB entry or contact IHS IT Support for assistance

TOTAL number of alerts by date range that can be re-processed :   6

Correct any issues before re-processing or the note(s) will not process

Make sure the RPMS user:
(1) has a Title starting with Dent
(2) has Electronic signature fields: Code, Block Title & Printed Name
(3) is not Terminated or Inactivated

If you get another alert, use the Print (PRT) option

Are you ready to begin (Y/N)?? N// y  YES
Select a name from the list above (question marks "??" = name is NOT in RPMS)

Enter the name: DEMO,lee DEMO,LEE J       LW          DENTIST
Name found in RPMS:  DEMO,LEE J


Is this the correct name (Y/N)?? N// y  YES
This name will be used for the dental note reprocessing

Do you wish to continue(Y/N)?? N// y  YES
Re-process HLB MSG Number  200000001339
Re-process HLB MSG Number  200000001340

TOTAL Messages to be re-processed: 2
Make sure you correct all issues before you continue...


Do you wish to continue (Y/N)?? N// y  YES
BEGIN processing the dental notes selected...

The dental note is in the TIU Document (EHR) file
PATIENT HRN:        Visit Date
45                  JAN 08, 2026

Dental note has been re-processed, HLB Message #:  200000001339


The dental note is in the TIU Document (EHR) file
PATIENT HRN:        Visit Date
46                  JAN 08, 2026

Dental note has been re-processed, HLB Message #:  200000001340
```

Figure 3-39: Reprocess Dental Notes option 2

3.3 Dental Interface Utilities Menu (UTL)

Use the **UTIL** menu to perform the following actions shown in Figure 3-40.

```
Select Dental Interface Main Menu <TEST ACCOUNT> Option: util  Dental Interface
Utilities


   PAT    List of Patient Errors
   RES    Reset a HLO Message for EIE Transport
   PRO    List of providers with errors
   ASU    Display Dental Visit ASUFACs
   INB    Process a Single Inbound HLO Message
   TRC    Dental Interface Trace
```

Figure 3-40: Dental Interface Utilities Menu

3.3.1 List of Patient Errors (PAT)

Provides a list of patients with errors. In some cases, if there are a lot of errors, they are most likely caused by a patient push that was done before EDR was set up. For instance, the errors below indicate that the EDR setup was not complete. See the Installation manual for more information, for this error the HL configuration files may not be set up correctly.

```
2021 DEMO HOSPITAL (INST)     RPMS-Dentrix Upload                    Version 1
                              List of Patient Errors

 Setting Patients who could not be processed  for System: 2013-DEMO.NA.IHS.GOV
Select Display Sequence: ???


Display Sequence  Value
----------------  -----
0
2                 26628 Unable to send HL7 message. RECEIVING FACILITY STATION
3                 26628 Unable to send HL7 message. RECEIVING FACILITY STATION
4                 26629 Unable to send HL7 message. RECEIVING FACILITY STATION
5                 26629 Unable to send HL7 message. RECEIVING FACILITY STATION
6                 26630 Unable to send HL7 message. RECEIVING FACILITY STATION
7                 26630 Unable to send HL7 message. RECEIVING FACILITY STATION
8                 26631 Unable to send HL7 message. RECEIVING FACILITY STATION
9                 26631 Unable to send HL7 message. RECEIVING FACILITY STATION
```

Figure 3-41: List of Patient Errors option

3.3.2 Reset a HLO Message for EIE Transport (RES)

Resets an HL7 message to allow the processing of the message. This is used for testing purposes only and requires the user to know the internal entry number of the message. It is easier to use the **Management** menu options in Section 3.2.

```
Select Dental Interface Utilities <TEST ACCOUNT> Option: res  Reset a HLO Messag
e for EIE Transport
Reset a message in HLO for EIE transport

Are you sure you want to reset an HLO message? No// Y  (Yes)
Enter IEN to remove 16,17,20,21 DATA:
```

Figure 3-42: Reset a HLO Message

3.3.3 List of Providers with Errors (PRO)

Provides a list of IEN's and error text of providers for whom the upload message would not transmit. The most common issue is no NPI number. Add the NPI number using the AVA option (Figure 3-35).

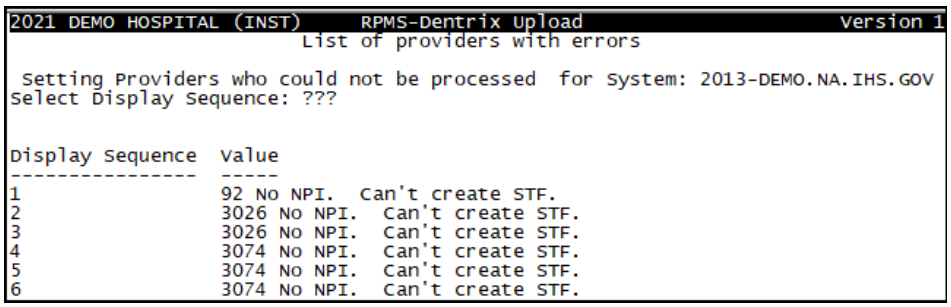


Figure 3-43: List of Providers with Errors option

3.3.4 Display Dental Visit ASUFAC's (ASU)

The option displays all the Dental ASUFAC location codes by date range.

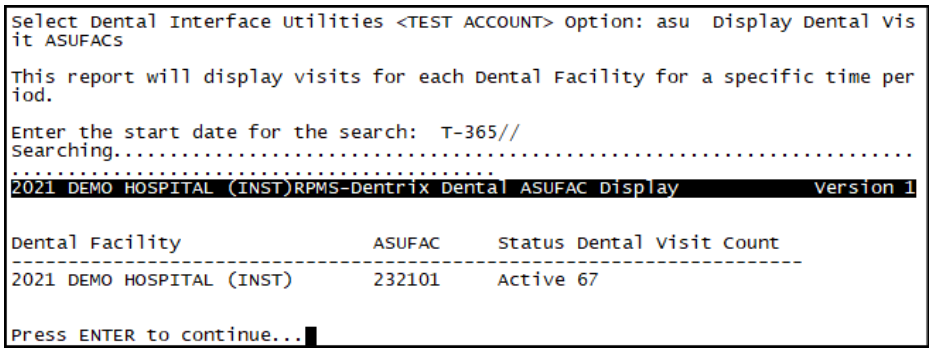


Figure 3-44: Display Dental Visit ASUFAC's

3.3.5 Process a Single Inbound HLO Message (INB)

Allows a user to process one HLO inbound message coming from Dentrix, such as a completed dental procedure. You must know the HLB message number (from the RPMS alert) to use this option.

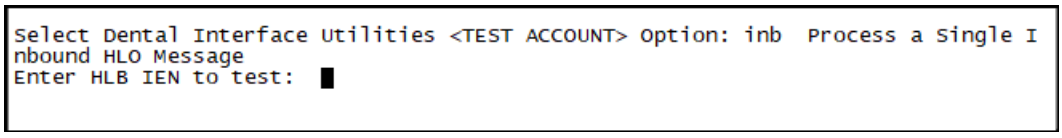


Figure 3-45: Process a Single Inbound HLO Message

3.3.6 Dental Interface Trace (TRC)

Run this option with caution; the trace can be set to "on" for a short period of time to debug the interface with Ensemble. If it runs for more than five minutes, it can slow down the system and could affect all running applications.

4.0 Receiving Dental Data

4.1 Dental Procedures

The EDR interface transmits dental procedures in the form of HL7 messages to RPMS. When these messages are received, RPMS creates a visit (if needed), stores the visit provider (V PROVIDER), purpose of visit (V POV), and creates an entry in the V DENTAL file for the visit. These visits should be visible in all PCC applications and the Electronic Health Record (EHR).

The EDR Interface also receives update and delete messages for dental procedures and are reflected in the PCC visit file in RPMS. See Section 4.3 for more information.

The EDR system uses a unique identifier that is stored in the External Key field of the V DENTAL file for lookups and uses the "AXK" cross reference.

4.2 Dental Notes

After the latest BADE patch is installed including BADE v1.0 p7 and a Dentrix technician enables the enhancement for the site, an MDM-T04 message (dental clinical note) will be created and transmitted to RPMS. Only finalized signed notes are transmitted. A visit will be created (if not already present), and the dental note is added to the V NOTE and the TIU Document file in RPMS for viewing in PCC and EHR. For more information see Section 5.0. For additional details on completing the setup, see the implementation guide for BADE v1.0 p7 located at https://www.ihs.gov/rpms/applications/clinical/ under the BADE application.

4.3 Dental Visits

Inbound DFT-P03 messages (dental procedures) transmitted from Dentrix allow the creation, update or deletion of dental data in the visit file. Every inbound message from Dentrix will contain patient, provider and dental information for a visit. If the dental note enhancement is enabled, MDM-T04 messages are also transmitted and can create a visit.

Dental visit data is received and stored into the RPMS visit file. Visits are created, ICD10 codes and providers are added, and the V DENTAL file is populated with the dental procedure. If the dental note enhancement is enabled (for MDM-T04 messages) the V NOTE file is also populated but only finalized/signed notes are transmitted, deletions and updates (addendums) are not transmitted.

Dental procedures, DFT-P03 HL7 messages are handled in the following manner:

1. The message arrives in RPMS, and an entry is created in ^HLB("QUEUE").

2. The Taskman task, BADE EDR TSK HLO IB FILER processes the message.
3. The Dentrix unique number is identified from the message in the FT1 segment.
4. The V DENTAL file is searched to determine if this is a new number.
5. The description field of the message is checked to determine whether it is "new," "update," or "delete."
6. If the key is new (not found in the V Dental file) and
    a. If the description is "new" (not an update or delete message)
        i. Create a new visit
        ii. Add a VPOV entry
        iii. Add a V PROVIDER entry
        iv. Add a new V DENTAL entry
    b. If the description is "update," it is an error (creates an alert) since the key was not found in RPMS to update the entry.
    c. If the description is "delete," it is an error (creates an alert) since the key was not found in RPMS to delete the entry.
7. If the key already exists:
    a. If the description is "new," it is an error (creates an alert) since it cannot be added twice.
    b. If the description is "update":
        i. If Dental field data was changed
            1. Delete the V DENTAL entry.
            2. Create a new one.
        ii. If the date of the visit changed:
            1. Delete the V DENTAL entry.
            2. Determine whether the visit should be deleted.
            3. Determine whether a new visit is needed.
            4. Make a new V DENTAL entry.
        iii. If the provider changed:
            1. Delete the old provider if this provider is not associated with other procedures on this visit.
            2. Add the new provider.
    c. If the description is "delete":

i. Remove the V DENTAL entry.

ii. Determine whether the visit should be deleted (no other entries in the visit).

4.3.1 RPMS Visit File

When a message is processed, the first dental procedure or note transmitted creates the visit. When another message is processed, it will add, update or delete the data if it's the same date of service.

Figure 4-1 displays a visit created by the EDR interface in the FileMan Visit file.

```
VISIT/ADMIT DATE&TIME: APR 01, 2025@11:38
  DATE VISIT CREATED: APR 01, 2025      TYPE: IHS
  THIRD PARTY BILLED: VISIT IN REVIEW STATUS
  PATIENT NAME: DEMO,ALEXANDERTHEGREATANDONE
  LOC. OF ENCOUNTER: 2021 DEMO HOSPITAL (INST)
  SERVICE CATEGORY: AMBULATORY          CLINIC: DENTAL
  DEPENDENT ENTRY COUNT: 6              DATE LAST MODIFIED: JUN 01, 2025
  HOSPITAL LOCATION: EDRHS17            CREATED BY USER: ADAM,ADAM
  OPTION USED TO CREATE: BADE EDR MAIN MENU
  USER LAST UPDATE: [redacted]
  OLD/UNUSED UNIQUE VISIT ID: 6064010002142878
  DATE/TIME LAST MODIFIED: JUN 12, 2025@07:54:19
  NDW UNIQUE VISIT ID (DBID): 999990002142878
  VISIT ID: 2DJC5-PAH
```

Figure 4-1: FileMan Output for a Dental Visit

The **Hospital Location** field uses the name of the clinic created in the **Set Default Clinic** option (Section 3.2.8), associated with the location. The **Created by User** field is populated by the entry added in the **Set Default User for Interface** option (Section 3.2.10) for that location.

4.3.2 V Provider File

The provider attached to the procedure is stored as the primary provider. An update message could change the provider, in which case the program would add the new provider and delete the old one (if the old provider is not associated with any other procedures on that visit). Figure 4-2 shows the FileMan output from the V Provider file for a dental visit.

```
PROVIDER: [redacted]
  PATIENT NAME: DEMO,ALEXANDERTHEGREATANDONE
  VISIT: APR 01, 2025@11:38              PRIMARY/SECONDARY: PRIMARY
  DATE/TIME ENTERED: APR 01, 2025@10:23:01
  ENTERED BY: ADAM,ADAM
  DATE/TIME LAST MODIFIED: APR 01, 2025@10:23:01
  LAST MODIFIED BY: ADAM,ADAM
```

Figure 4-2: FileMan Output for the V Provider entry

4.3.3 V POV File

The purpose of visit (POV) for all dental visits was v72.2 prior to the implementation of ICD10. After BADE v1.0 p5 was released, up to 4 POV's may be attached to a single dental procedure (DFT-P03 message) and added to the visit.

Figure 4-3 shows the output of a V POV entry for a dental visit. The example shows a "K02.52" ICD10 code. The external key field will match up with a dental procedure and POV entry.

A "ZZZ.999" code is added to the visit if the incoming ICD10 code from Dentrix is v72.2 (it's missing and sending a default of v72.2) and since it's an old ICD9 code it's replaced with "ZZZ.999". Sites should consider mapping their dental codes to ICD10 codes in Dentrix to prevent the uncoded diagnosis (ZZZ.999) in the RPMS visit file.

```
POV: K02.52
  PATIENT NAME: DEMO,ALEXANDERTHEGREATANDONE
  VISIT: APR 01, 2025@11:38
  PROVIDER NARRATIVE: DENTAL/ORAL HEALTH VISIT
  PRIMARY SNOMED: 63161005                EXTERNAL KEY: 1004534
  DATE/TIME ENTERED: APR 01, 2025@10:23:01
  ENTERED BY: ADAM,ADAM
  DATE/TIME LAST MODIFIED: APR 01, 2025@10:23:01
  LAST MODIFIED BY: ADAM,ADAM
```

Figure 4-3: FileMan Output for the V POV entry

4.3.4 V Note File

The V Note file stores the dental note information for the visit, see Figure 4-4.

```
DOCUMENT TITLE: BADE EDR DEFAULT DENTAL NOTE
  PATIENT: DEMO,ADULT B                  VISIT: AUG 23, 2025@11:38
  EVENT DATE&TIME: OCT 23, 2025@16:10:23
  AUTHOR: DEMO,SAM                       DATE/TIME ENTERED: OCT 23, 2025@15:12:01
  ENTERED BY: ADAM,ADAM
  DATE/TIME LAST MODIFIED: OCT 23, 2025@15:12:01
  LAST MODIFIED BY: ADAM,ADAM
```

Figure 4-4: FileMan output for a V Note entry

The TIU Document file stores the actual text data, see Figure 4-5.

```
DOCUMENT TYPE: BADE EDR DEFAULT DENTAL NOTE
  PATIENT: DEMO,ADULT B                  VISIT: AUG 23, 2025@11:38
  PARENT DOCUMENT TYPE: PROGRESS NOTES   STATUS: COMPLETED
  EPISODE BEGIN DATE/TIME: AUG 23, 2025@11:38
  VISIT TYPE: A                          ENTRY DATE/TIME: OCT 23, 2025@16:10:23
  AUTHOR/DICTATOR: DEMO,SAM              EXPECTED SIGNER: DEMO,SAM
  HOSPITAL LOCATION: EDRHS17             VISIT LOCATION: EDRHS17
  REFERENCE DATE: OCT 23, 2025@16:10:23
  CAPTURE METHOD: upload                 SERVICE: BUSINESS OFFICE
  SIGNATURE DATE/TIME: OCT 23, 2025@16:11:02
  SIGNED BY: DEMO,SAM                    SIGNATURE BLOCK NAME: S[redacted]
  VISIT ID: 2DKPM-PAH
 REPORT TEXT:
------------------------------------------------------------------------------
Test 1 Author: s[redacted]n signer: s[redacted]----- Signed on Thursday, October
23, 2025 at 4:11:00 PM ----- ----- Provider: SMOR[redacted] --
Clinic: EDRDEHR -----
```

Figure 4-5: FileMan output for a TIU Document entry

The TIU Document file entry allows the dental note to be viewed in EHR, see Figure 4-6. Select the **Notes** tab in EHR to view the entire note.

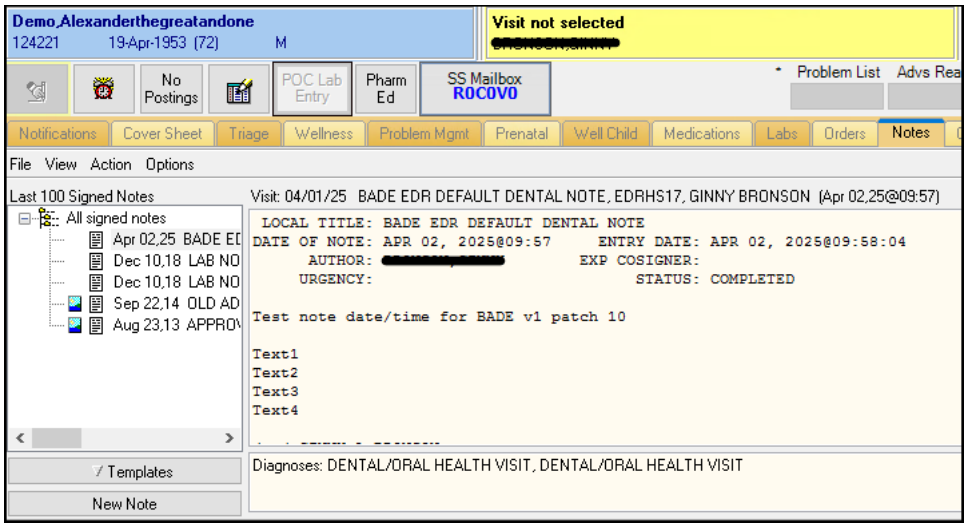


Figure 4-6: EHR output for a Dental Note

4.3.5 V Dental File

The V Dental file stores the dental procedure information. The following fields are populated:

- Dental Service Code (pointer to the ADA Code file)
- Patient Name (pointer to the Patient file)
- Visit (pointer to the Visit file)

- Number of Units (always set to 1)
- Operative Site (pointer to the Dental Operative Site file)
- Tooth Surface (free text)
- Fee (if transmitted from Dentrix)
- Event Date and Time (visit date and time)
- Ordering Provider (provider of the visit, pointer to New Person file)
- Clinic–DENTAL (pointer to Clinic Stop for dental)
- Encounter Provider (same as ordering provider, pointer to New Person file)
- External Key (A Unique ID which must be included in the message. This is the transaction ID in Dentrix and is used for lookup in the V Dental "AXK" cross-reference.

The FileMan output of a V Dental entry in RPMS is shown in Figure 4-7 below.

```
SERVICE CODE: 2140
  PATIENT NAME: DEMO,ALEXANDERTHEGREATANDONE
  VISIT: APR 01, 2025@11:38              NO. OF UNITS: 1
  OPERATIVE SITE: PERMANENT SECOND MOLAR,MAX LEFT
  TOOTH SURFACE: M                       FEE: 10
  EVENT DATE&TIME: APR 01, 2025@11:38    ORDERING PROVIDER: [redacted]
  CLINIC: DENTAL                         ENCOUNTER PROVIDER: [redacted]
  EXTERNAL KEY: 1004534                  DATE/TIME ENTERED: APR 01, 2025@10:23:01
  ENTERED BY: ADAM,ADAM
  DATE/TIME LAST MODIFIED: APR 01, 2025@10:23:01
  LAST MODIFIED BY: ADAM,ADAM
```

Figure 4-7: VA FileMan output for the V DENTAL entry

4.4 Browse a Visit

The user can view and process these dental visits the same as any other RPMS visit. Figure 4-8 shows a dental visit viewed through Display Data for a Specific Patient Visit option in RPMS PCC.

```
PCC VISIT DISPLAY                Nov 07, 2025 10:35:50

Patient Name:              DEMO,ALEXANDERTHEGRE
Chart #:                   124221
Date of Birth:             APR 19, 1953
Sex:                       M
Visit IEN:                 2142878

=============== VISIT FILE ===============
VISIT/ADMIT DATE&TIME:  APR 01, 2025@11:38
DATE VISIT CREATED:     APR 01, 2025
TYPE:                   IHS
THIRD PARTY BILLED:     VISIT IN REVIEW STATUS
PATIENT NAME:           DEMO,ALEXANDERTHEGREATANDONE
LOC. OF ENCOUNTER:      2021 DEMO HOSPITAL (INST)
SERVICE CATEGORY:       AMBULATORY
CLINIC:                 DENTAL
DEPENDENT ENTRY COUNT:  6
DATE LAST MODIFIED:     JUN 01, 2025
HOSPITAL LOCATION:      EDRHS17
CREATED BY USER:        ADAM,ADAM
```

Figure 4-8: Dental Visit in PCC

The user can view the visit in EHR, see Figure 4-9 below.

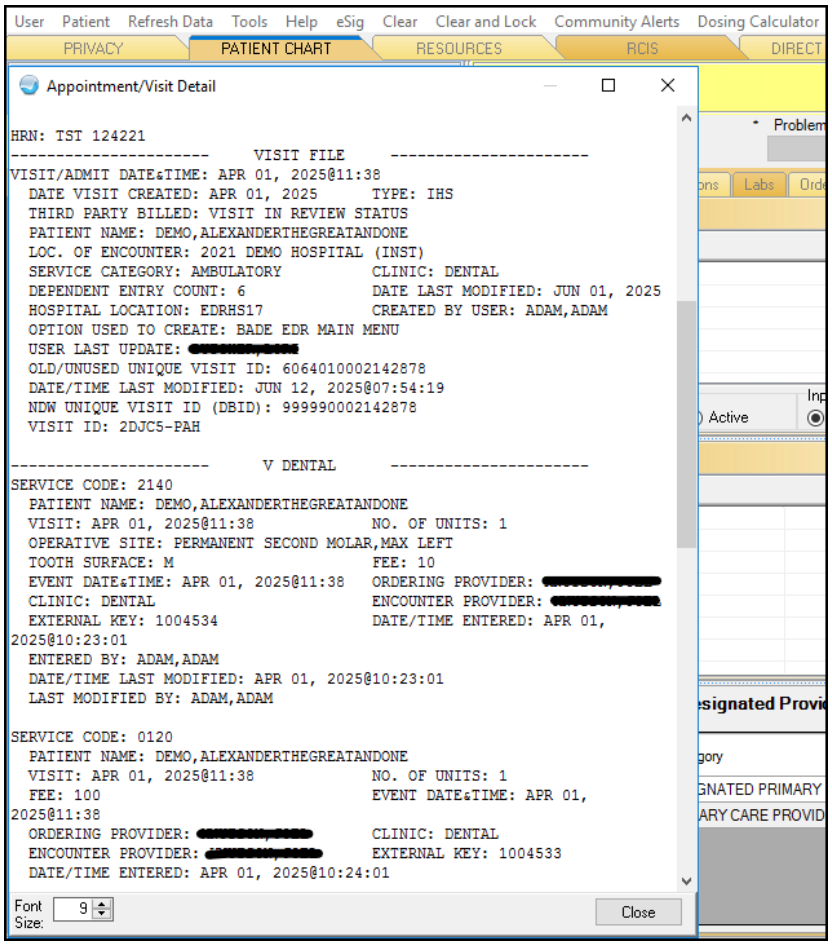


Figure 4-9: Dental Visit in EHR

5.0 Dental Note Enhancement

The enhancement was added to the EDR interface to process incoming dental notes created in Dentrix. This enhancement is available in Dentrix v 8.0.96.553 or later and requires BADE v1.0 p7 to process the dental note in RPMS. The following was included in BADE p7 for the dental note:

- Added an MDM-T04 message type to the BADE Production (BADE.EDR.HL7) to accept and process the new message type.
- Added routines to process the incoming MDM-T04 messages (BADEHL5, BADEHL6, BADEHL7, and BADEHL8).
- Added a menu option to set up the new Note Title called “BADE EDR DEFAULT DENTAL NOTE”.
- Added an entry to the TIU Document Definition file called BADE EDR DEFAULT DENTAL NOTE to be used for dental notes.
- Updated the HLO Application Registry file adding the MDM-T04 entry to process the new message type.

Before Dentrix enables the dental note enhancement, do the following in RPMS:

1. Add the default parameter in the **EDR Dental Notes Menu**, **Set TIU Default Parameter** option (Section 3.2.14.2) using “BADE EDR DEFAULT DENTAL NOTE” for the entry. This is used as the note title for all dental notes incoming from Dentrix.

2. All authors and signers of the dental note in Dentrix must be set up in RPMS with an active user account. See below for instructions on setting up these users.

    a. **For Providers**: Current providers being utilized in Dentrix should already be set up in RPMS but are also required to have an electronic signature code, Block Title, Block Printed Name, and Title = ”Dentist” or the note will not be created, and an alert will be sent.

    b. **For Dental Hygienist/Assistants**: All others who originate or sign the dental note in Dentrix must have an active user account set up in RPMS that includes required fields identified below or the note will not be created, and an alert will be sent.

Use the **AVA Add/Edit New Person** option in RPMS to create a new user for the authors and signers of the note, making sure you do not create duplicates.

All required fields must be entered as well as fields needed for logging in, these include **Title**, **Primary Menu Option**, **Access/Verify codes**, **File Manager Access Codes, Division**, and **Service/Section**. After adding the new user with the **AVA** option, use the **User Management** menu, **Editing an existing user** option to add these fields (Figure 5-1). Once this is completed, have the user login to RPMS and use ^TBOX to add their electronic signature information as explained in #5 below.

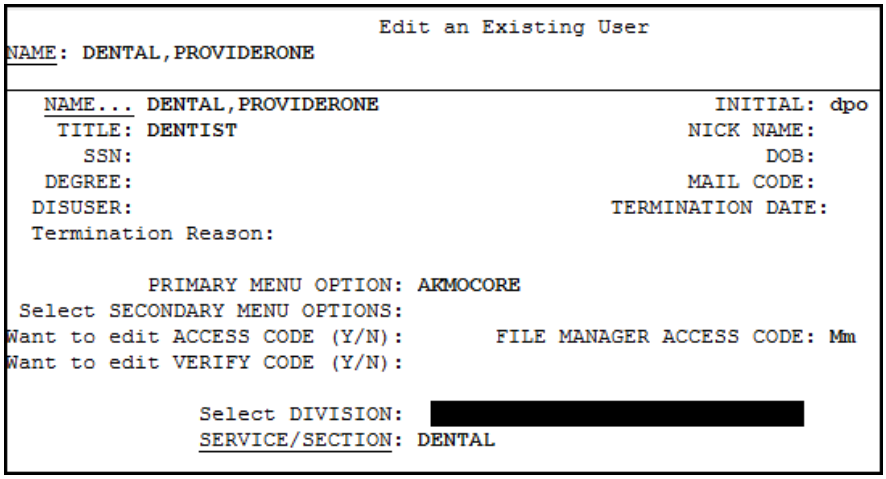


Figure 5-1: Adding a New User

The **Signature Block Printed Name**, **Signature Block Title,** and an **Electronic Signature Code** must be present in RPMS to process dental notes for Providers (Dentists), Dental Hygienists, and Dental Assistants who author or sign notes in Dentrix. The user must sign in and use ^TBOX to add this information.
See Figure 5-2.

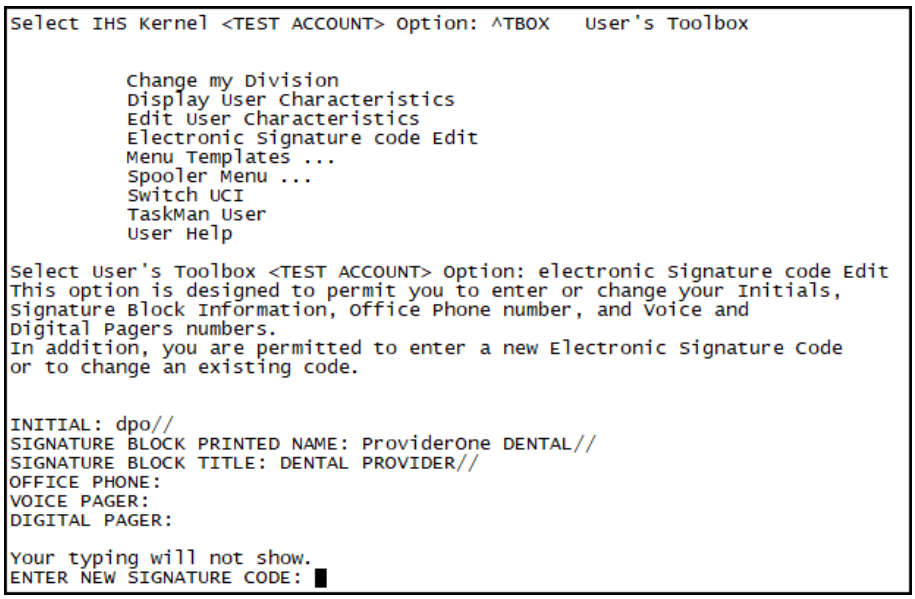


Figure 5-2: User's Toolbox–Adding Electronic Signature Information

3. All RPMS users who will be reviewing the dental note alerts must be added to the RPMS Dental Mailman group. Use Manage Mailman/Group Distribution Management/ Mail Group Edit to add users to this group. An example is shown in Section 6.1. It's important to review these alerts so that EDR issues can be identified including problems with the dental notes. Section 3.2.14 shows the options available to re-process failed dental notes. You must have BADE v1.0 p10 installed.

4. Only completed and signed notes are transmitted from Dentrix to RPMS. Once the enhancement is activated in Dentrix, addendums will not be created or transmitted to RPMS.

5. Viewing the Dental Note: the dental note can be viewed in EHR under the notes tab. In PCC, use "Display Data for a Specific Patient Visit" and you will see an entry that points to the V NOTE file (see Section 4.3.4).

6.0 EDR Alerts

Since the majority of issues related to the EDR Interface create RPMS alerts, Site managers and IT staff supporting the interface should be able to view the alerts (Section 6.2 and 6.3) to resolve issues or correctly identify problems that can be resolved by IT Support staff or the programmer.

See the BADE Technical Manual for EDR Interface transmission issues in the BADE Production.

6.1 RPMS Mailman

To receive RPMS alerts related to the EDR Interface–either incoming messages (from Dentrix) or outgoing (Patient/Provider additions and updates), you need to be a member of the RPMS Dental Mailman group. Select **Manage Mailman**, **Group/Distribution Management**, **Mail Group Edit**, then enter **RPMS Dental**. Figure 6-1 shows how to add a name to the mailman group to receive RPMS alerts related to the EDR Interface.

```
Select Group/Distribution Management <TEST ACCOUNT> Option: mail group
    1    Mail Group Coordinator's Edit
    2    Mail Group Coordinator's Edit W/Remotes
    3    Mail Group Edit
CHOOSE 1-3: 3  Mail Group Edit

Select MAIL GROUP NAME:    RPMS DENTAL
MAIL GROUP NAME: RPMS DENTAL//
Select MEMBER: DEMO,DOCTOR//
  MEMBER: DEMO,DOCTOR//
  TYPE: INFO//
Select MEMBER: DEMO,PROVIDER MN       MAN
  Are you adding 'DEMO,PROVIDER MN' as a new MEMBER (the 6TH for this MAIL GROUP
)? No// y  (Yes)
  TYPE: I  INFO
Select MEMBER: ^

Do you wish to forward past mail group messages
to the user(s) you just added to the mail group(s)? No// n  NO

Select MAIL GROUP NAME:
```

Figure 6-1: RPMS Dental Mailman Group

6.2 Errors on Outbound Messages

Outbound messages that cannot send data to Dentrix send an alert to users in the mail group RPMS DENTAL. Along with the messages, patient information is stored in the parameters. Below are RPMS Outbound ADT-A28, ADT-A31, MFN-M02 message errors and descriptions:

```
Unable to build HL7 message. HLO message could not be created.
```

Figure 6-2: Example HLO message error

All Outbound messages contain an MSH and EVT (Event) segment. If HLO can open and build the MSH segment for a message but cannot create the EVT segment, this error alert is generated. This is a fatal error and indicates a problem associated with the HLO HL7 application and not the EDR application. Most likely cause is an error in installing a new HL7 patch.

```
EVT segment could not be created.
```

Figure 6-3: Example EVT segment creation error

All Outbound messages contain an MSH and EVT (Event) segment. If HLO can open and build the MSH segment for a message but cannot create the EVT segment, this error alert is generated. This is a fatal error and indicates a problem associated with the HLO HL7 application and not the EDR application. Most likely cause is an error in installing a new HL7 patch.

```
No health record number for _DFN_. Patient did not have a health record
number.
```

Figure 6-4: Example no health record number error

DFN is the Internal Entry Number of the patient data location in the ^DPT and ^AUPNPAT globals. Every ACTIVE patient must have a Health Record Chart Number (HRCN) associated with each Location/Institution where the patient is registered. Both the location (ASUFAC) and HRCN are required to create an ADT-A28 or ADT-A31 message. Patient Registration allows the user to enter this data. The error is unrelated to the EDR application.

```
No ASUFAC record number for – DFN . An ASUFAC record could not be created
for the patient.
```

Figure 6-5: Example no ASUFAC record number error

DFN is the Internal Entry Number of the patient data location in the ^DPT and ^AUPNPAT globals. Every ACTIVE patient must have a Health Record Chart Number (HRCN) associated with each Location/Institution where the patient is registered. Both the location (ASUFAC) and HRCN are required to create an ADT-A28 or ADT-A31 message. Patient Registration allows the user to enter this data. The error is unrelated to the EDR application.

```
No name for _DFN_. Patient has no name.
```

Figure 6-6: Example No name for DFN error

DFN is the Internal Entry Number of the patient data located in the ^DPT and ^AUPNPAT globals. There is a ^DPT(DFN,0) node where the .01 (first piece) of the node does not have the patient name data. The error indicates that the data is corrupt for this DFN and needs to be manually fixed by a programmer. The error is unrelated to the EDR application.

```
No DOB for _DFN_. Patient has no date of birth.
```

Figure 6-7: Example no DOB for DFN error

DOB is Date of Birth. DFN is the Internal Entry Number of the patient data location in the ^DPT and ^AUPNPAT globals. There is a ^DPT(DFN,0) node where the .03 (third piece) of the node does not have the patient DOB data. The error indicates that the data could be corrupt for this DFN. Check the DOB entry to ensure it's been entered and try resending again using **Patient Registration** or use the **EDR Management menu/A28** or **A31** option to send a single A28 or A31.

```
Medicaid segment could not be created. Insurance segment could not be made.
```

Figure 6-8: Example Medicaid/Insurance segment could not be created/made error

The Patient Registration application or corrupt data shows that this patient has a Medicaid Insurance entry that is incomplete or missing. This can usually be deleted/fixed through the Registration application or if necessary, using FileMan.

```
Medicare segment could not be created.
```

Figure 6-9: Example Medicare segment could not be created error

The Patient Registration application or corrupt data shows that this patient has a Medicare Insurance entry that is incomplete or missing. This can usually be deleted/fixed through the Registration application or if necessary, using FileMan.

```
Insurance segment could not be created.
```

Figure 6-10: Example Insurance segment could not be created error

The Patient Registration application or corrupt data shows that this patient has a Third Party Insurance entry that is incomplete or missing. This can usually be deleted/fixed through the Registration application.

```
Railroad insurance could not be created.
```

Figure 6-11: Example Railroad insurance could not be created error

The Patient Registration application or corrupt data shows that this patient has a Railroad Insurance entry that is incomplete or missing. This can usually be deleted/fixed through the Registration application or if necessary, using FileMan.

```
ZPM2 segment could not be created.
```

Figure 6-12: Example ZPM2 segment could not be created error

The ZP2 segment contains locally defined data not specifically defined by the HL7 standard. Data associated with this segment is missing or corrupt. A programmer will need to correct this error.

```
Unable to build MFE segment.
```

Figure 6-13: Example unable to build MFE segment error

The MFE (Master File Entry) Segment is part of the MFN-M02 Provider Update message. MFE identifies the type of update for the provider entry. If this segment is corrupt, the HLO message creation software is corrupt. A developer will need to fix this problem.

```
Provider _IEN_ does not have NPI. Dentists need an NPI.
```

Figure 6-14: Example Provider IEN does not have NPI error

IEN is Internal Entry Number and identifies where the provider data is stored in the ^VA(200 global. NPI is National Provider Identifier. If a Provider does not have a NPI then the MFN-M02 message for this provider will not be created. Use the **AVA** option and add the provider's NPI to correct this problem, then use **AVA Add/Edit Providers** option (re-enter the TITLE) to trigger another MFN message. The **Management** menu also has an option to send a single MFN message.

```
Unable to create the MFI segment.
```

Figure 6-15: Example unable to create the MFI segment error

The MFI (Master File Identification) Segment is part of the MFN-M02 Provider Update message. MFI contains the identifier that defines the person being entered is a provider or staff. If this segment is corrupt, the HLO message creation software is corrupt. A developer will need to fix this problem.

```
Unable to build STF segment.
```

Figure 6-16: Example unable to build STF segment error

The STF (Staff Identification) Segment is part of the MFN-M02 Provider Update message. STF contains the Provider demographic data. Some of the data for this provider is missing or corrupt. This can usually be corrected by using the **AVA Add/Edit Providers** option.

```
Unable to build PRA segment.
```

Figure 6-17: Example unable to build PRA segment error

The PRA (Practitioner Detail) Segment is part of the MFN-M02 Provider Update message. PRA contains the Provider class information. The specialty for this provider is missing or corrupt. This can usually be corrected by using the **AVA Add/Edit Providers** option.

```
Provider _IEN_ does not have a name. Provider must have a name.
```

Figure 6-18: Example provider IEN does not have a name error

IEN is the Internal Entry Number of the provider data located in the ^VA(200 global. There is a ^VA(200,IEN,0) node where the .01 (first piece) of the node does not have the provider name. The error indicates that the data is corrupt for this DFN and needs to be manually fixed by a programmer. The error is unrelated to the EDR application.

6.3 Errors on Inbound Messages

Errors can be generated for a variety of reasons. Inbound messages that cannot be filed in PCC from Dentrix send an alert to users in the RPMS DENTAL mailman group. The following are Inbound DFT-P03 message errors and descriptions.

```
PID segment not found in message.
```

Figure 6-19: Example PID segment not found in message error

This means the message coming over did not have any data to identify the patient because the PID segment is missing. This error should be trapped in the IRIS Production (BADE) and never generate an alert. If this alert is created, a developer of the EDR system will need to determine cause and correction.

```
Patient DFN identifier missing in message.
```

Figure 6-20: Example DFN identifier missing in message error

There was no Medical Record number in the message. If this alert is created, a developer of the EDR system will need to determine cause and correction.

```
Patient DFN cannot be found in RPMS.
```

Figure 6-21: Example patient DFN cannot be found in RPMS error

The DFN in the message does not exist in RPMS. If this alert is created, a developer of the EDR system will need to determine cause and correction.

```
Patient ASUFAC identifier missing in message.
```

Figure 6-22: Example Patient ASUFAC identifier missing in message error

The ASUFAC number is required and is missing or corrupt. If this alert is created, a developer of the EDR system will need to determine cause and correction.

```
Patient HRCN not found for DFN.
```

Figure 6-23: Example patient HRCN not found for DFN error

A HRCN for the DFN was sent, but the health record number sent does not have a corresponding HRCN for this patient in RPMS. If this alert is created, a developer of the EDR system will need to determine cause and correction.

```
Last names for _DFN_ do not match in message.
```

Figure 6-24: Example last names for DFN do not match in message error

The last name of the patient in RPMS with the DFN in the message does not match the last name of the patient in the message. This alert would occur if RPMS merged a patient with a patient that does not have the same last name. If this alert is created, a developer of the EDR system will need to determine cause and correction.

```
Birth dates for _DFN_ do not match in message.
```

Figure 6-25: Example birth dates for DFN do not match in message error

The birthdates of the DFN in RPMS and the patient in the message do not match. This alert would occur if RPMS merged a patient with a patient that does not have the same DOB. If this alert is created, a developer of the EDR system will need to determine cause and correction.

```
FT1 segment not found in message.
```

Figure 6-26: Example FT1 segment not found in message error

The message coming over from Dentrix did not contain any dental procedure data. If this alert is created, a developer of the EDR system will need to determine cause and correction.

```
No date of visit in the message.
```

Figure 6-27: Example no date of visit in the message error

All visits must have a date. The message visit information coming from Dentrix could not be converted to a proper internal date format required by RPMS. If this alert is created, a developer of the EDR system will need to determine cause and correction.

```
No unique ID found in message.
```

Figure 6-28: Example no unique ID found in message error

The unique ID from the EDR is for lookup and must be in the message to identify the procedure. It is the transaction ID in Dentrix. If the message type coming from Dentrix is an update or delete message, there must be a corresponding message EXTERNAL KEY in the V Dental file to update or delete. If there is no corresponding EXTERNEL KEY then this alert will be generated. The most common cause is that the original procedure was not properly filed and created an alert. If this alert is created, a developer of the EDR system will need to determine cause and correction.

```
Unique id _APCDTEXK_ already exists as No add in message.
```

Figure 6-29: Example unique id APCDTEXK already exists as No add in message error

The message type was “add,” but the unique identifier (EXTERNAL KEY) is already there. Only a message type of update or delete can process an existing V Dental entry. This frequently occurs when support resends a block of messages from Dentrix. If this alert is created, a developer of the EDR system will need to determine cause and correction.

```
Dentrix procedure not in the file, so cannot be updated.
```

Figure 6-30: Example Dentrix procedure not in the file, so cannot be updated error

The unique ID sent over in an update message and does not exist in the V DENTAL file. This usually occurs when a block of messages are resent from Dentrix. If this alert is created, a developer of the EDR system will need to determine cause and correction.

```
Dentrix procedure not in the file, so cannot be deleted.
```

Figure 6-31: Example Dentrix procedure not in the file, so cannot be deleted error

The unique ID sent over in an update message and does not exist in the V DENTAL file. This usually occurs when a block of messages are resent from Dentrix. If this alert is created, a developer of the EDR system will need to determine cause and correction.

```
No dental code in message.
```

Figure 6-32: Example no dental code in message error

The message did not send an ADA code. If this alert is created, a developer of the EDR system will need to determine cause and correction, most likely an error in the Dentrix transmission.

```
Unable to find code _ADA CODE_ in message.
```

Figure 6-33: Example Unable to find code ADA Code in message error

The ADA code sent in the message does not exist in RPMS. The ADA Code file in RPMS does not match the ADA Code file in Dentrix. This usually occurs after an ADA update has been added in Dentrix without installing the ADA RPMS Patch. Another cause is if someone in RPMS has modified the ADA entry or modified the code file in Dentrix. If this alert is created, a developer of the EDR system will need to determine cause and correction.

```
No location found in the message.
```

Figure 6-34: Example no location found in the message error

Every message coming from Dentrix must have an associated ASUFAC. The ASUFAC was not in FT1 16.1 or was nonnumeric. If this alert is created, a developer of the EDR system will need to determine cause and correction.

```
Location does not belong to the ASUFAC number.
```

Figure 6-35: Example location does not belong to the ASUFAC number error

The location (ASUFAC) in the message does not have a corresponding location entry in RPMS. The ASUFAC defined in Dentrix is incorrect. If this alert is created, a developer of the EDR system will need to determine cause and correction. Most likely occurred because a clinic was added in Dentrix and a corresponding clinic was not added to the Default Clinic setup.

```
Clinic does not exist in RPMS in the message.
```

Figure 6-36: Example clinic does not exist in RPMS in the message error

If a default clinic has not been defined in the BADE system parameters or the clinic entered is not in the RPMS HOSPITAL LOCATION file, this alert will be generated. If this alert is created, a developer of the EDR RPMS system will need to determine cause and correction.

```
Clinic _HOSLOC_ is not define for ASUFAC location.
```

Figure 6-37: Example Clinic HOSLOC is not define for ASUFAC location error

If a clinic was sent with the location, the clinic has not been associated with the proper ASUFAC in the HOSPITAL LOCATON file. The ASUFAC and Clinic name in Dentrix must match the Clinic name and associated ASUFAC in the RPMS HOSPITAL LOCATION file. There must also be a default clinic and ASUFAC defined in the BADE system parameters. If this alert is created, a developer of the EDR system will need to determine cause and correction.

```
No provider for procedure in the message.
```

Figure 6-38: Example no provider for procedure in the message error

There was no provider for the procedure in the message. If this alert is created, a developer of the EDR system will need to determine cause and correction.

```
Unable to create visit for message.
```

Figure 6-39: Example unable to create visit for message error

The call to create a visit failed for some unknown reason. If this alert is created, a developer of the EDR RPMS system will need to determine cause and correction. In some cases, the patient cannot be found in RPMS.

```
Multiple visits exist and cannot match.
```

Figure 6-40: Example multiple visits exist and cannot match error

The call for visit creation found multiple visits and does not know which visit to add the procedure to. This is a very rare message type. If this alert is created, a developer of the EDR RPMS system will need to determine cause and correction.

```
Pt in message does not match pt.
```

Figure 6-41: Example PT in message does not match pt error

Patient name in the message does not match the patient name associated with the Unique EDR ID in the V dental file. An update or delete message type coming from Dentrix matches the V Dental file entry using the EXTERNAL KEY. If the patient names do not match an alert is filed. Most likely, the name has been changed in RPMS and the ADT-A31 update from Patient Registration never transmitted to Dentrix with the name change. If this alert is created, a developer of the EDR RPMS system will need to determine cause and correction and an ADT message will need to be triggered.

```
Visit to update in message _HLMSGIEN_ does not exist in visit file.
```

Figure 6-42: Example visit to update in message HLMSGIEN does not exist in visit file error

HLMSGIEN is the IEN of the message in the ^HLB global. The visit found in the update message does not exist in RPMS. The message is trying to update data in a V Dental file entry, and the Visit entry associated with the procedure is missing. If this alert is created, a developer of the EDR RPMS system will need to determine cause and correction.

```
Visit to delete in message _HLMSGIEN_ does not exist in visit file.
```

Figure 6-43: Example visit to delete in message HLMSGIEN does not exist in visit file error

HLMSGIEN is the IEN of the message in the ^HLB global. The visit found in the delete message does not exist in RPMS. The message is trying to delete data in a V Dental file entry, and the Visit entry associated with the V Dental procedure is missing. If this alert is created, a developer of the EDR RPMS system will need to determine cause and correction.

```
Unable to delete V file entry.
```

Figure 6-44: Example unable to delete V file entry error

Program was unsuccessful in deleting a V file entry. If this alert is created, a developer of the EDR RPMS system will need to determine cause and correction.

Appendix A RPMS Rules of Behavior

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

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

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

Both documents are available at this IHS Web site:
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., PCC, Dental, and 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 non-public 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 your 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 job 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 function 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.
- Logout of the system whenever they leave the vicinity of their PC.
- 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.
- Shall abide by all Department and Agency policies and procedures and guidelines related to ethics, conduct, behavior, and IT information processes.

A.1.4 Confidentiality

RPMS users shall

- Be aware of the sensitivity of electronic and hardcopy information, and protect it accordingly.
- Store hardcopy 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 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 your system 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 your 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 5 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 password immediately if password has been seen, guessed, or otherwise compromised; and report the compromise or suspected compromise to your ISSO.
- Keep user identifications (ID) 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 8 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 your ISSO that you have identified an IT security incident and you will 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 your 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 non-recovery of temporary files created in processing sensitive data, virus protection, intrusion detection, and provides 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.
- Shall not access live production systems without obtaining appropriate written access, shall only retain that access for the shortest period possible to accomplish the task that requires the access.
- Shall observe separation of duties policies and procedures to the fullest extent possible.
- Shall 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.
- Shall use checksums or other integrity mechanism when releasing their certified applications to assure the integrity of the routines within their RPMS applications.
- Shall follow industry best standards for systems they are assigned to develop or maintain; abide by all Department and Agency policies and procedures.
- Shall 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.
- Not 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, 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 back up 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; 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

File

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

FileMan

The database management system for RPMS.

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).

Health Level Seven (HL7)

HL7 specifies a number of flexible standards, guidelines, and methodologies by which various healthcare systems can communicate with each other. Such guidelines or data standards are a set of rules that allow information to be shared and processed in a uniform and consistent manner. These data standards are meant to allow healthcare organizations to easily share clinical information.

Kernel

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

Menu

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

Namespace

A unique set of two to four alpha characters that are assigned by the database administrator to an RPMS 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.

Acronym List

Acronym	Term Meaning
EDR	Electronic Dental Record
HL7	Health Level Seven
IHS	Indian Health Service
IRIS	InterSystems IRIS Database Management System
IT	Information Technology
OIT	Office of Information Technology
PII	Personally Identifiable Information
QA	Quality Assurance
RPMS	Resource and Patient Management System

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