



RESOURCE AND PATIENT MANAGEMENT SYSTEM

Dental/EDR Interface

(BADE)

User Manual

Version 1.0
February 2010

Office of Information Technology (OIT)
Division of Information Resource Management
Albuquerque, New Mexico

Preface

The purpose of this manual is to provide user information about the Dental/EDR (Electronic Dental Record) Interface package and to assist the user in the use of this interface. The document contains information on the use of three menus:

- Upload Menu
- Dental Interface Management Menu
- HLO Management Menu

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

Table of Contents

1.0	Introduction.....	5
2.0	Orientation	6
2.1	System Overview.....	6
2.1.1	Initial Uploads.....	6
2.1.2	Ongoing Patient Data	7
2.1.3	Receiving Dental Data.....	7
2.2	Menu System.....	7
2.2.1	UPL – Upload Menu	8
2.2.2	MAN – Dental Interface Management Menu	9
2.3	HLO Menu	10
2.4	Conventions in the Software and Manual.....	10
2.4.1	The Enter Key	10
2.4.2	Double Slash (/).....	10
2.4.3	Screenshots	11
2.4.4	Online Help.....	11
2.4.5	Backspace and Arrow Keys.....	11
2.4.6	The Caret (^).....	11
2.4.7	The “Select Device” Prompt	12
3.0	Upload Menu	13
3.1	UAP – Load all Patients option.....	14
3.2	PUP – Pause Patient Load option	14
3.3	RUP – Restart Patient Upload option	15
3.4	UPV – Upload All Providers option	16
3.5	PPV – Pause Provider Upload option.....	16
3.6	RPV – Restart Provider Upload option	17
3.7	DSP – Display Progress option	17
3.8	ERR – List of Patients with Errors option.....	19
3.9	ERRP – List of Providers with Errors option	20
3.10	TCT – Pt Count for Throttle Action option	21
3.11	THR – Throttle Patient Upload option.....	21
3.12	Errors on Outbound Messages.....	22
4.0	Dental Interface Management Menu	26
4.1	A28 – Send a single A28 Message option.....	27
4.2	A31 – Send a single A31 Message option.....	27
4.3	MFN – Send an MFN Message option	27
4.4	CLN – Default Clinic for Interface option	28
4.5	DEFT – Default Time for Dental Visit option.....	29
4.6	USR Default User for Interface.....	30
5.0	HLO Management.....	32

6.0	Creating Dental Visits	33
6.1	Errors on Inbound Messages.....	34
6.2	Visit.....	38
6.3	V Provider.....	39
6.4	V POV.....	39
6.5	V Dental.....	40
6.6	Browse a Visit.....	40
7.0	Appendix A: RPMS Rules of Behavior	43
7.1	All RPMS Users	44
7.1.1	Access.....	44
7.1.2	Information Accessibility.....	45
7.1.3	Accountability	45
7.1.4	Confidentiality.....	45
7.1.5	Integrity.....	46
7.1.6	System Logon	46
7.1.7	Passwords.....	47
7.1.8	Backups.....	48
7.1.9	Reporting.....	48
7.1.10	Session Timeouts.....	48
7.1.11	Hardware	48
7.1.12	Awareness.....	49
7.1.13	Remote Access	49
7.2	RPMS Developers	50
7.3	Privileged Users.....	51
8.0	Contact Information	53

1.0 Introduction

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

During this same period, IHS and tribal dental programs have made use of the RPMS Dental Data System (DDS) as their primary system for maintaining a history of individual patient services; contributing dental data to the RPMS electronic clinical record; producing provider and department workload data; and contributing statistical data to the national data center located in Albuquerque, New Mexico. At many sites, data captured in the DDS has also been used in the RPMS Third Party Billing System.

With the replacement of the RPMS DDS with an Electronic Dental Record (EDR), RPMS applications are required to interact with the EDR to meet the needs of both the Dental Department and the local health program as a whole. The RPMS/HL7-Optimized (HLO) interface is a way to send patient information, Admission, Discharge, and Transfer (ADT) to the EDR, and is a way to receive dental procedures from the EDR and store them into the Patient Care Component (PCC) V Dental file.

When the EDR and the RPMS/EDR Interface are complete, the EDR is the primary data repository for dental data for sites that use the EDR. Information required by the RPMS PCC, the RPMS Scheduling Package, and the Electronic Health Record (EHR) is transferred from the EDR to the RPMS through the RPMS/EDR Interface.

It is the shared vision of IHS national representatives and the Division of Oral Health that the RPMS/EDR Interface described in this document will serve as a prototype to messaging framework for all HL7 message interfaces required by the IHS.

2.0 Orientation

2.1 System Overview

The Dental/EDR interface has many different functions which are described below.

2.1.1 Initial Uploads

The EDR system includes menu options to perform the initial upload of patient and provider information.

2.1.1.1 Patient Upload

The number of patients at a site can be quite large, so the initial patient upload is the most time consuming. Depending on computer capacity, expect the upload to progress at a rate of 5000 to 8000 patients per hour. Users can remain on the system during the upload, but the preference is to run the patient upload during off hours. Use the menus and options described in Section 2.2 to perform the following tasks:

- Start a TaskMan job to upload all living patients to the interface.
- Stop the TaskMan job if needed because of system slowness.
- Restart the TaskMan job when the system is ready to send more data.
- Set a timeframe (in seconds) that throttles the upload. The interface processes a certain number of patients, and then checks to determine if it should pause for the specified number of seconds before continuing.
- Set the number of patients to process before the interface pauses.
- Review the number of patients processed and the status of the upload.
- Determine which patients could not be uploaded.

2.1.1.2 Provider Upload

The number of dentists at any one site is usually not large, and this upload should take less time than ten minutes to complete. Only providers belonging to the PROVIDER CLASS of DENTIST (CODE 52) are sent through the interface. Providers also must have a National Provider Identification number (NPI) established before his/her data is sent through the interface.

Use the menus and options described in Section 2.2 to perform the following tasks:

- Start a TaskMan job to upload all dentists to the interface.
- Stop the TaskMan job if needed because of system slowness.
- Restart the TaskMan job when the system is ready to send more data.
- Review the number of dentists processed and the status of the upload.

2.1.2 Ongoing Patient Data

New patient data, patient updates, and new provider data are normally sent using triggers in protocols. When a new patient is registered or edited, a message is automatically sent. Likewise, editing a dentist's data causes an update message to be sent.

However, it is possible to manually send a message through the interface or to reprocess a message that has already been sent. Use the menus and options described in Section 2.2 to perform the following tasks:

- Resend a Patient Registration message (A28)
- Resend a Patient Update message (A31)
- Resend a Master File Update (MFN) message to update a provider
- Reprocess an inbound HL7 message

2.1.3 Receiving Dental Data

The EDR interface sends dental procedure and visit messages back to RPMS. When these messages are received, RPMS creates a visit (if needed), stores the visit provider (VPRV) and purpose of visit (VPOV), and creates an entry in the V DENTAL file for the visit procedure. These visits should be visible in all PCC applications and the EHR. The Dental Interface receives change and delete messages as well, and these changes are also reflected in PCC and RPMS.

The dental system uses a unique identifier that is stored in the External Key field of the V DENTAL file for lookups and editing.

2.2 Menu System

The main entry point into the Dental/EDR Interface module is the Dental Interface Management Option menu ([Figure 2-1](#)). This menu has two submenus, one for the initial patient upload and one for ongoing maintenance.

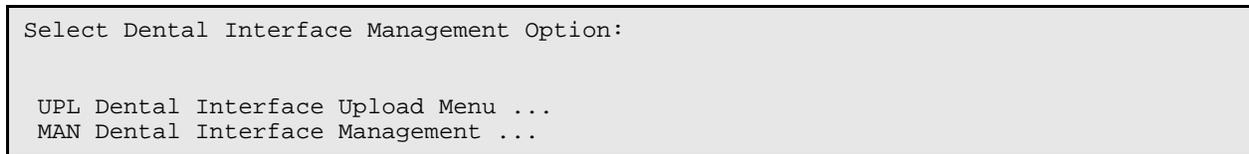


Figure 2-1: Main Dental Interface Management Option menu

2.2.1 UPL – Upload Menu

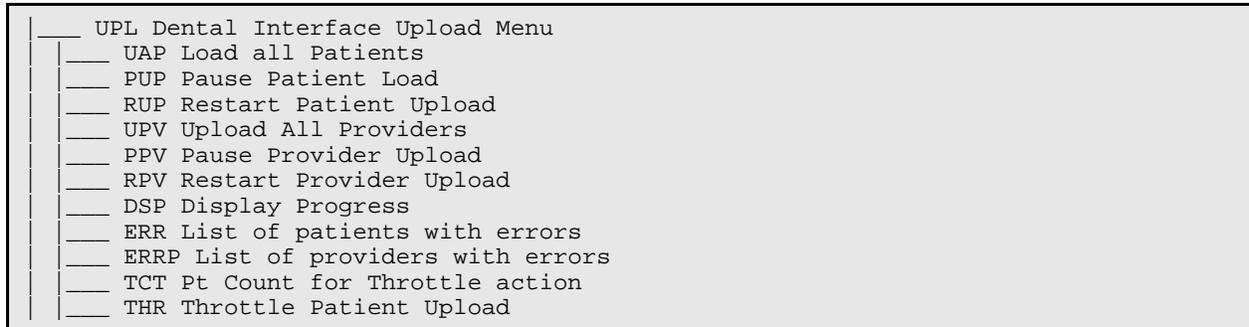


Figure 2-2: Dental Interface Upload Menu

The Dental Interface Upload Menu provides the following options for the initial patient upload:

- **UPL Load all Patients.** This option starts a TaskMan job and is unavailable after the upload is complete. It runs at a low priority on the RPMS server.
- **PUP Pause Patient Load.** This option pauses the patient upload job if necessary.
- **RUP Restart Patient Load.** This option restarts a paused patient upload job. It cannot be run if the job is already running and it is unavailable after the upload is complete.
- **UPV Upload All Providers.** This option starts a TaskMan job to load all dentists into the interface and is unavailable once the upload is completed.
- **PPV Pause Provider Upload.** This option pauses the provider upload job if necessary.
- **RPV Restart Provider Upload.** This option restarts a paused provider upload job. It cannot be run if the job is already running and it is unavailable once the upload is completed.
- **DSP Display Progress.** This option displays the status of the upload job.
- **ERR List of patients with errors.** The interface stores any patients that were not uploaded. This option allows the user to view them. Once corrected through the Patient Registration application, the trigger mechanism will reprocess the patient. The user can also manually reprocess the patient.

- **ERRP List of providers with errors.** The interface stores any providers that were not uploaded. This option allows the user to view them. Once corrected through the Provider Update menu the trigger mechanism will reprocess the provider. The user can also manually reprocess the provider.
- **TCT Pt Count for Throttle action.** If the system is running slow and messages waiting in the queue are backing up, the interface can stop the upload for a few seconds to let the HL7 messaging system 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.
- **THR Throttle Patient Upload.** This option allows the user to specify the number of seconds (up to 20) that the system should wait before continuing. The TCT above processes the number of patients as defined, then pauses for the number of seconds defined in the THR and then reprocesses the TCt value again.

2.2.2 MAN – Dental Interface Management Menu

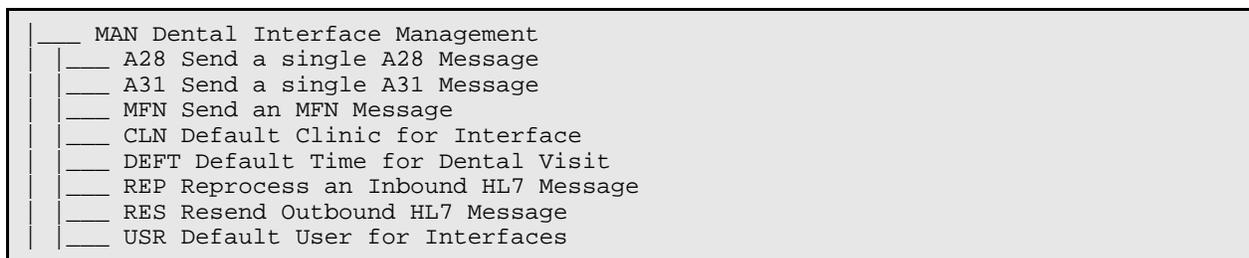


Figure 2-3: Dental Interface Management menu

The Dental Interface Management menu provides the following options for manually sending messages:

- **A28 Send a single A28 Message.** This option sends a Patient Registration message for any patient.
- **A31 Send a single A31 Message.** This option sends a Patient Update message for any patient.
- **MFN Send an MFN Message.** This option sends a Master File Update message to update a provider record. The user can select anyone in the new person file, but messages are only sent for dentists.
- **CLN Default Clinic for Interface.** This option allows the user to specify the default clinic assigned to visit records.
- **DEFT Default Time for Dental Visit.** This option allows the user to specify the default time assigned to visit records.
- **REP Reprocess an Inbound HL7 Message.** Not Used

- **RES Resend Outbound HL7 Message.** Not Used
- **USR 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 PCC Visit.

2.3 HLO Menu

The messages created in this interface can be sent to the interface using the HLO. The HLO menu options are located the HL7 Main Menu. Although the BADE application was written to use the HLO Menu, the transport process is controlled by the Ensemble Integration Engine (EIE). The user should monitor the message process using the EIE System Management Portal when possible. The user should refer to the EIE User Manual. The HLO menu options are included for documentation.

2.4 Conventions in the Software and Manual

The 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.

2.4.1 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.” (Most PC computer keyboards have an Enter key rather than a Return key.) Whenever the manual refers either <ENTER> or “the Enter key”, the user should press the Return or Enter key.

2.4.2 Double Slash (//)

Frequently, the software asks a question followed by a prompt and two slashes (//). The text displayed before the two slashes is the default response to the prompt. Pressing the Enter key selects the default response without retyping it. If the user does not want to use the default response (or if no default response is presented before double slashes), simply type a response and then press the Enter key. If a prompt has a default response that the user wants to be blank, either delete the default text or type@ at the prompt after the default response.

2.4.3 Screenshots

[Figure 2-4](#) shows an example of a screenshot or screen capture.

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

Figure 2-4: Example screenshot

Boldface type in a screenshot indicates text to be typed by the user. After every entry that is typed, 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.

2.4.4 Online Help

Online 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.

Some prompts display a list of available choices. If at any time the user is not sure 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.

2.4.5 Backspace and Arrow Keys

The Backspace key moves the cursor to the left, erasing characters as it moves. The Up and Down arrow keys moves the cursor up and down fields. The Left and Right arrow keys generally are not used. If the user is having problems with these keys, check with a site manager.

2.4.6 The Caret (^)

The caret (^ or Shift-6), 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.

Activate the 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.

2.4.7 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 a 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 the user to the last visited screen while the report is printing, rather than waiting for the report to finish printing before returning to the screen. This is helpful if the report takes a long time to run (search) or print. After typing **Q**, the system displays the “Queue to Print on Device” prompt. At this point, type the name of the printer on which the user wants to print the report.

3.0 Upload Menu

From the Dental Interface Main Menu, type **UPD** and press the Enter key to display the Dental Interface Upload Menu.

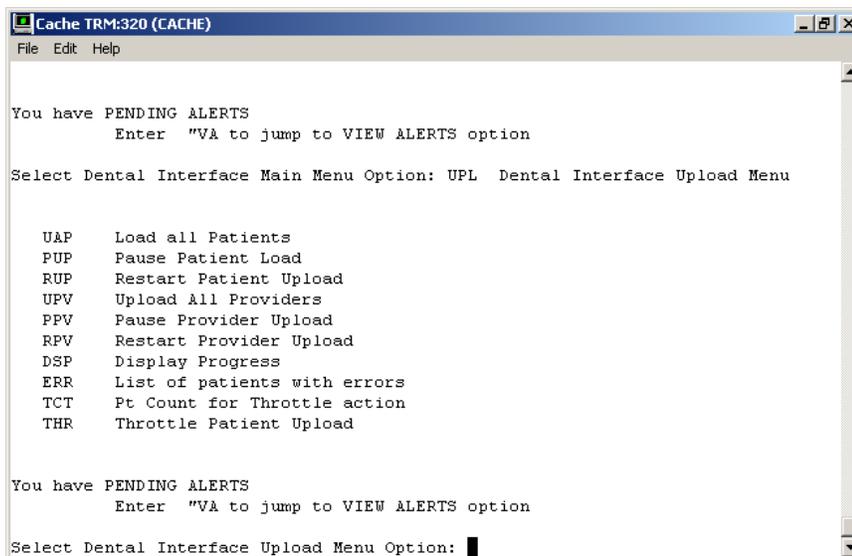
[Figure 3-1](#) shows the Dental Interface Main Menu and its submenus.

```
Select OPTION NAME: BADE EDR MAIN MENU  Dental Interface Main Menu

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

Figure 3-1: Dental Interface Main Menu

[Figure 3-2](#) shows the options on the Dental Interface Upload Menu. Each menu option is explained in the following sections.



```
Cache TRM:320 (CACHE)
File Edit Help

You have PENDING ALERTS
  Enter  "VA to jump to VIEW ALERTS option

Select Dental Interface Main Menu Option: UPL  Dental Interface Upload Menu

UAP  Load all Patients
PUP  Pause Patient Load
RUP  Restart Patient Upload
UPV  Upload All Providers
PPV  Pause Provider Upload
RPV  Restart Provider Upload
DSP  Display Progress
ERR  List of patients with errors
TCT  Pt Count for Throttle action
THR  Throttle Patient Upload

You have PENDING ALERTS
  Enter  "VA to jump to VIEW ALERTS option

Select Dental Interface Upload Menu Option: █
```

Figure 3-2: Dental Interface Upload Menu

3.1 UAP – Load all Patients option

Use the UAP option to start the upload of 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; it is a tasked job that could take considerable time to run. 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. 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 load.

This option can be rerun only with assistance from the OIT Help Desk.

If this option is selected while the upload is running, a message indicating that the upload is already running is displayed. The upload will not run a second time.

While an upload job is running, the Restart Patient Upload option may not be used. Use the Pause Patient Load option to stop the load and then restart it later. The priority of this upload is set to 1 (the lowest priority). [Figure 3-3](#) shows what the user sees when selecting this option.

```
Select Dental Interface Upload Menu Option: UAP Load all Patients
Requested Start Time: NOW// (FEB 12, 2009@13:48:58)
Task number 21933
```

Figure 3-3: UAP Load all Patients option

3.2 PUP – Pause Patient Load option

Use the PUP option to cause the initial patient upload job to stop. Selecting this option sets a parameter that stops the upload. The program checks this parameter and stops processing if it is set to YES. [Figure 3-4](#) shows what this parameter looks like.

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.

To pause the patient upload process, type **YES** at the “Pause Dental Patient Load” prompt and press the Enter key.

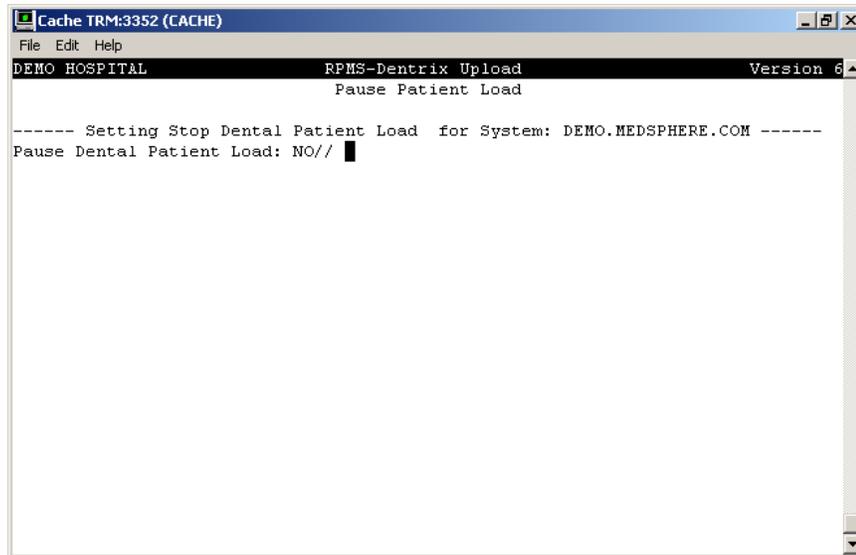


Figure 3-4: Pause Dental Patient Load prompt

3.3 RUP – Restart Patient Upload option

Use the RUP option to restart the patient upload. If the Pause Patient Load parameter is set to NO, a message indicating that the upload is already running is displayed (see [Figure 3-5](#)).

```
Select Dental Interface Upload Menu Option: RUP Restart Patient Upload
Process is already running
```

Figure 3-5: Unsuccessful Restart Patient Upload operation

If the upload has already been completed, this menu option is unavailable.

If the upload has been paused, the user is prompted to type a time to begin the restart. The task number is displayed after the start time is entered (see [Figure 3-6](#)).

```
Select Dental Interface Upload Menu Option: RUP Restart Patient Upload
Requested Start Time: NOW// (FEB 12, 2009@13:58:58)
Task number 21945
```

Figure 3-6: Successful Restart Patient Upload operation

3.4 UPV – Upload All Providers option

The provider upload is similar to the patient upload. This is a tasked job that runs through file 200 (the New Person file) and sends information on providers in the provider class of DENTIST. This option should be run to completion prior to doing the Patient Upload. If this option is selected while the upload is running, a message indicating that the upload is already running is displayed. The upload will not run a second time. This priority of this upload is 1 (the lowest priority). After the upload is complete, this menu option is unavailable. This upload takes only a few minutes to complete and can be run during normal operating hours.

This option can be rerun only with assistance from the OIT Help Desk.

A task number is displayed after the start time is entered (see [Figure 3-7](#)).

```
Select Dental Interface Upload Menu Option: UPV Upload All Providers
Requested Start Time: NOW// (FEB 12, 2009@14:28:26)
Task number 21937
```

Figure 3-7: Start Upload All Providers operation

3.5 PPV – Pause Provider Upload option

Use the PPV option to cause the initial provider upload to stop. Selecting this option sets a parameter that stops the upload. The program checks this parameter and stops processing if it is set to YES. [Figure 3-8](#) shows what this parameter looks like.

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.

To pause the provider upload process, type **YES** at the “Pause Provider Load” prompt and press the Enter key.

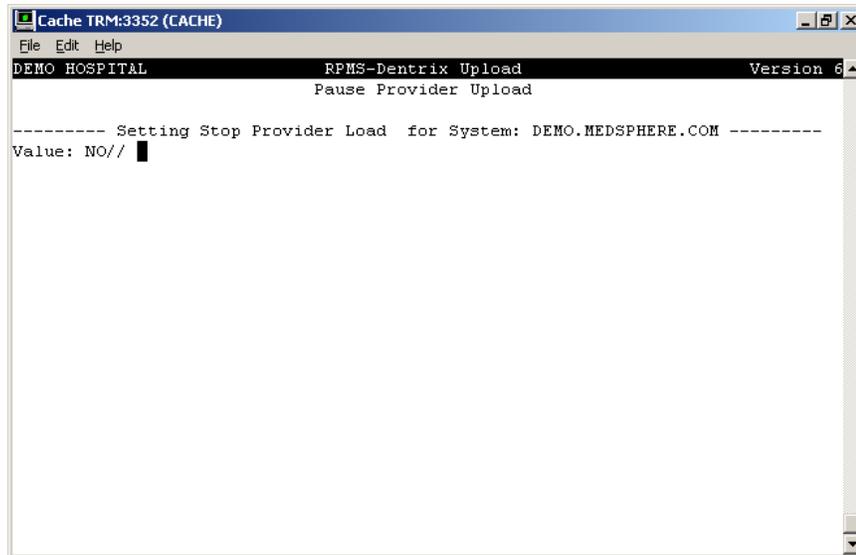


Figure 3-8: Pause Provider Upload screen

3.6 RPV – Restart Provider Upload option

Use the RPV option to restarts the provider upload. If the Pause Provider Load parameter is set to NO, a message indicating that the upload is already running is displayed (see [Figure 3-9](#)).

```
Select Dental Interface Upload Menu Option: RPV Restart Provider Upload
Process is already running
```

Figure 3-9: Unsuccessful Restart Provider Upload operation

If the upload has already completed, this menu option is unavailable.

If the upload has been paused, the user is prompted to type a time to begin the restart. The task number is displayed after the start time is entered (see [Figure 3-10](#)).

```
Select Dental Interface Upload Menu Option: RPV Restart Provider UploadRequested
Start Time: NOW// (FEB 12, 2009@14:58:58)

Task number 21954
```

Figure 3-10: Successful Restart Provider Upload operation

3.7 DSP – Display Progress option

Use the DSP option to display the progress of the uploads. [Figure 3-11](#) shows an example of the progress information.

The following patient upload data is displayed:

- **Last Patient Processed.** This is displayed if the upload is still running. If the upload has been completed, it is blank.
- **Total Pts processed.** The number patients that have been uploaded.
- **Throttle seconds.** The number of seconds to hold when processing patients.
- **Throttle Pt. Ct.** The number of patients to be processed before holding for the number of seconds specified by “Throttle seconds.”
- **Currently stopped.** Displays YES if the patient upload process is currently paused; otherwise displays NO.
- **Task.** If the upload is still running, the task number is displayed. If the upload has been completed, the words “Upload complete” are displayed.

The following provider upload data is displayed:

- **Last Provider Processed.** This is displayed if the upload is still running. If the upload has been completed, it is blank.
- **Total Prov processed.** The number of entries in the New Person file that have been examined. This is *not* a count of the number of dentists uploaded.
- **Currently stopped.** Displays YES if the patient upload process is currently paused; otherwise displays NO.
- **Task.** If the upload is still running, the task number is displayed. If the upload has been completed, the words “Upload complete” are displayed.

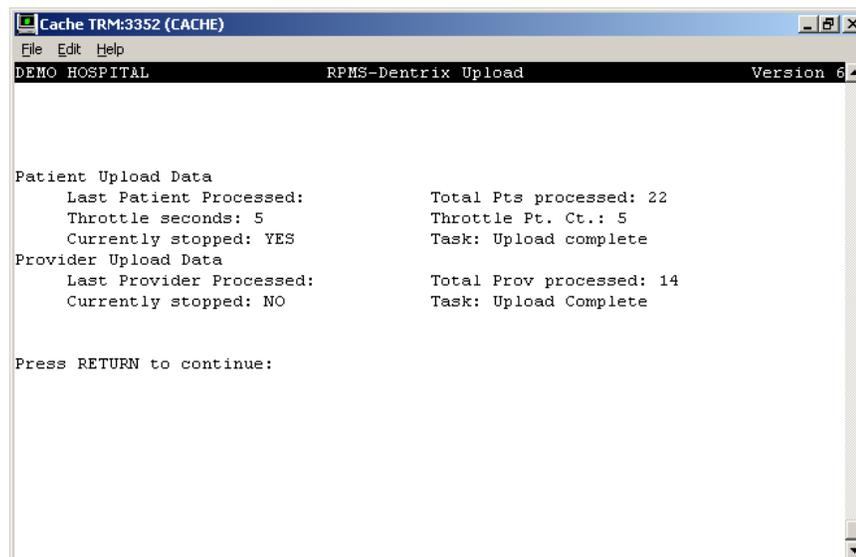


Figure 3-11: Displaying upload progress

3.8 ERR – List of Patients with Errors option

Because HL7 requires very little data to send a message, it is very rare that a patient entry cannot be processed. Only patient entries missing a name or health record number cannot be sent. However, other errors could occur. When errors occur, the program performs the following tasks:

- Sends an alert to people in the RPMS DENTAL mail group indicating that an error occurred and the message was not sent
- Stores the patient IEN (equivalent to the FileMan DFN variable) and a sequence number in the parameter information about patients who could not be processed (BADE EDR ERROR PTS)

To view the list of patients with errors, type ? at the “Select Display Sequence” prompt.

Figure 3-12 shows the ERR option listing two patients whose records were not transferred to the EDR. Determine the problem for each patient and revise the patient information in the Patient Registration System. Editing a patient record in this way automatically triggers a resend of the corrected record to the EDR.

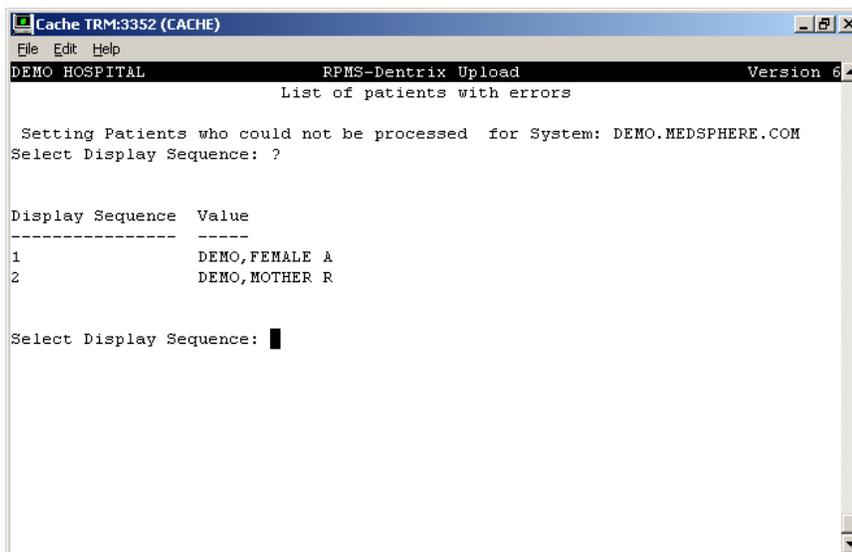


Figure 3-12: List of patients with errors screen

3.9 ERRP – List of Providers with Errors option

Because HL7 requires very little data to send a message, it is very rare that a provider entry cannot be processed. Only providers that are identified as dentists will be sent. However, the EDR requires a national identifier, and an error is generated if the dentist does not have one. Other errors could occur. When errors occur, the program performs the following tasks:

- Sends an alert to people in the RPMS DENTAL mail group indicating that an error occurred and the message was not sent
- Stores the patient DFN and a sequence number in the parameter information about patients who could not be processed (BADE EDR PROVIDER ERRORS)

To view the list of providers with errors, type ? at the “Select Display Sequence” prompt.

[Figure 3-13](#) shows the ERRP option listing one provider whose record was not transferred to the EDR. Determine the problem for each provider in the list and revise the provider information in the IHS Provider/Person Add/Edit package. Editing a provider record in this way automatically triggers a resend of the corrected record to the EDR.

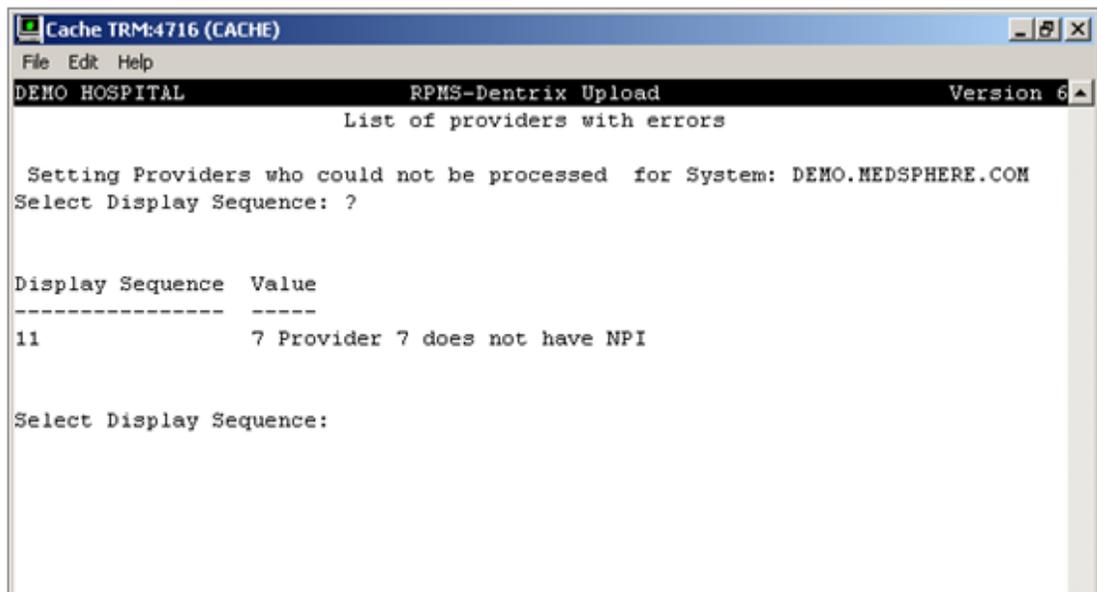


Figure 3-13: List of providers with errors screen

3.10 TCT – Pt Count for Throttle Action option

This parameter is used by the throttle mechanism for the upload process. If the interface is putting patients into the queue for message transmission faster than they can be transmitted, a site may choose to slow down the patient processing. There are two parameters involved in this throttling. This first parameter determines how many patients to process before checking to determine whether to shut down processing or hold for a set number of seconds.

This parameter is set to 10 by default. The maximum value is 1000.

[Figure 3-14](#) shows how to set this parameter by typing the number of patients to process.

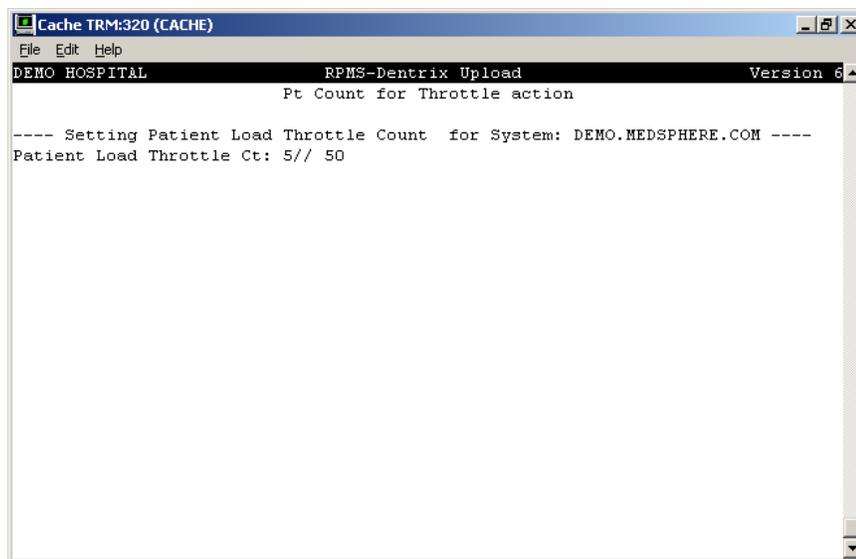


Figure 3-14: Pt Count for Throttle action screen

3.11 THR – Throttle Patient Upload option

The second parameter used by the throttle mechanism, Throttle Patient Upload (BADE EDR PT THROTTLE), is the number of seconds to wait before restarting the upload processing. The default value of this parameter is 0, and the maximum value is 20.

[Figure 3-15](#) shows how to set this parameter by typing the number of seconds to wait before restarting.

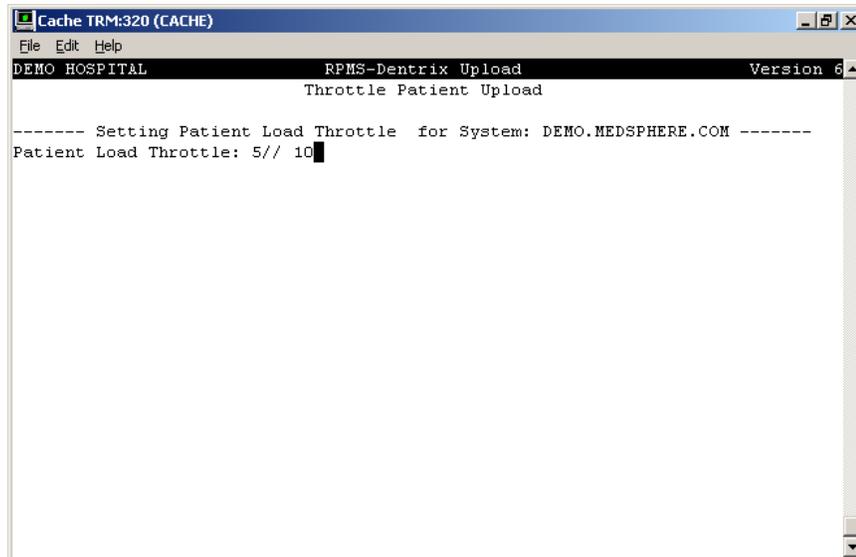


Figure 3-15: Throttle Patient Upload screen

3.12 Errors on Outbound Messages

Outbound messages that cannot send data to Dentrix send an alert to people 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.
```

All Outbound messages contain a MSH and EVT (Event) segment. If HLO is able to 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.
```

All Outbound messages contain a MSH and EVT (Event) segment. If HLO is able to 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.

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.

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.

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.

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 is corrupt for this DFN and needs to be manually fixed by a programmer. The error is unrelated to the EDR application.

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

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 using Fileman.

Medicare segment could not be created.

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 using Fileman.

Insurance segment could not be created.

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 or using Fileman.

Railroad insurance could not be created.

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 using Fileman.

ZPM2 segment could not be created.

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.

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.

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-P03 for this provider will not be created. Use the Provider Update menu and add the provider's NPI to correct this problem.

Unable to create the MFI segment.

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.

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 PROVIDER UPDATE menu.

Unable to build PRA segment.

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 PROVIDER UPDATE menu.

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

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 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.

4.0 Dental Interface Management Menu

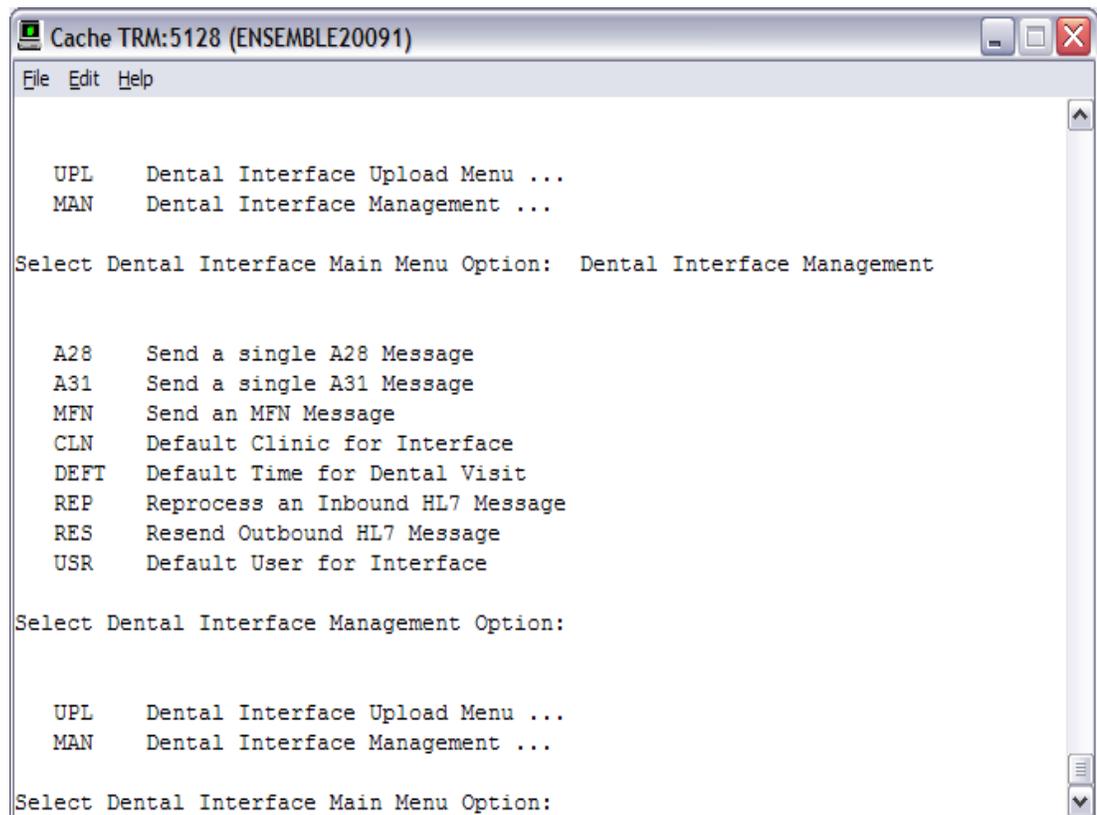
When in the Dental Interface Main Menu, type **MAN** and press the Enter key to display the Dental Interface Management menu. [Figure 4-1](#) shows the main menu and its submenus.

```
Select OPTION NAME: BADE EDR MAIN MENU  Dental Interface Main Menu

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

Figure 4-1: Dental Interface Main Menu

[Figure 4-2](#) shows the options on the Dental Interface Management menu. Each menu option is explained in the following sections.



```
Cache TRM:5128 (ENSEMBLE20091)
File Edit Help

UPL  Dental Interface Upload Menu ...
MAN  Dental Interface Management ...

Select Dental Interface Main Menu Option:  Dental Interface Management

A28  Send a single A28 Message
A31  Send a single A31 Message
MFN  Send an MFN Message
CLN  Default Clinic for Interface
DEFT Default Time for Dental Visit
REP  Reprocess an Inbound HL7 Message
RES  Resend Outbound HL7 Message
USR  Default User for Interface

Select Dental Interface Management Option:

UPL  Dental Interface Upload Menu ...
MAN  Dental Interface Management ...

Select Dental Interface Main Menu Option:
```

Figure 4-2: Dental Interface Management menu

4.1 A28 – Send a single A28 Message option

Use this option to resend one A28 (Patient Registration) message. Use a normal FileMan patient lookup to select any patient in the Patient File. The system should display an acknowledgment that the message was sent. [Figure 4-3](#) shows what the user would see when sending a single message.

```
Select Dental Interface Management Option: A28 Send a single A28 Message
Select Patient: DEMO,MOTHER
Message was sent
```

Figure 4-3: Send a single A28 Message option

4.2 A31 – Send a single A31 Message option

Use this option to resend one A31 (Patient Update) message. Use a normal FileMan patient lookup to select any patient in the Patient File. The system should display an acknowledgment that the message was sent. [Figure 4-4](#) shows what the user would see when sending a single message.

```
Select Dental Interface Management Option: A31 Send a single A31 Message
Select Patient: TEST
1 TEST, JOHN      M 10-01-1960 XXX-XX-2929 SOUC 23929
2 TEST,INPATIENT M   M 07-22-1945 XXX-XX-5465 SOUC 23434
3 TEST,JOHN      M 10-03-1949 XXX-XX-2312 SOUC 32102
4 TEST,PATIENT A   M 10-12-1948 XXX-XX-4321 SOUC 36445
5 TEST,PATIENT B   F 06-03-1951 XXX-XX-2323 SOUC 44323
ENTER '^' TO STOP, OR CHOOSE 1-5: 4
TEST,PATIENT A   M 10-12-1948 XXX-XX-4321 SOUC 36445
Message was sent
```

Figure 4-4: Send a single A31 Message option

4.3 MFN – Send an MFN Message option

Use this option to resend one MFN (Master File Update) message. Use a normal FileMan lookup to select any provider in the New Person file. The system should display an acknowledgment that the message was sent or that the provider was not a dentist. [Figure 4-](#) shows what the user would see when sending a single message.

```
Select PROVIDER: USER
  1 USER,DEMO  DU
  2 USER,NURSE  UN
CHOOSE 1-2: 1 USER,DEMO

Not a dentist

Select Dental Interface Management Option: MFN Send an MFN Message
Select PROVIDER: HAGER,MARY G HAGER,MARY G  MGH  CLINICAL COORDINATOR

Message was sent
```

Figure 4-: Send an MFN Message option

4.4 CLN – Default Clinic for Interface option

The Dental/EDR Interface stores visits into PCC files, especially the visit and V DENTAL files. These visits can be seen in the EHR. In the Dental DFT-P03 message coming from the EDR Dental package, only the ASUFAC is sent. There must be an assigned Clinic and assigned User defined for each ASUFAC. The example below shows how to assign the values. If a facility only supports one ASUFAC then the System interface should be populated with the Institution default dental clinic as defined in the HOSPITAL LOCATION (44) file. The Entry in the HOSPITAL LOCATION file must have the proper Institution defined to assure that the ASUFAC values match. Additionally, a user needs to be associated with this clinic to allow the filer creating the PCC Visit and Dental Procedures to have a user to identify who added the PCC entry or updated the PCC entry. If a site has multiple supported Divisions, then the additional Divisions should be added. Note that there must be one Dental Clinic complete with the Dental Clinic Stop Code and the Dental Treating Specialty assigned in RPMS. Each Clinic should indicate the proper ASUFAC and should be named to reflect the site. Use the Default Clinic for Interface screen ([Figure 4-5](#)) to set this parameter.

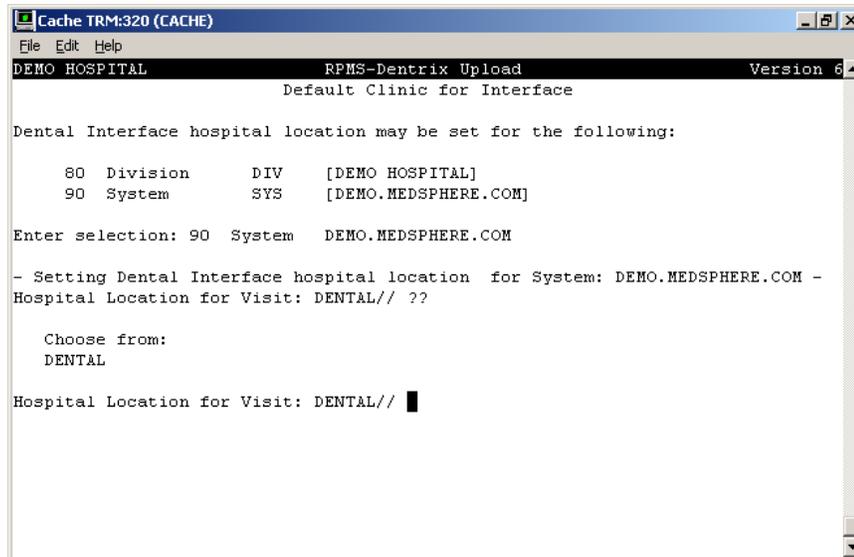


Figure 4-5: Default Clinic for Interface screen

4.5 DEFT – Default Time for Dental Visit option

Visits in PCC need both a date and time, but the EDR only requires a date. Visits missing a time are given a default time of 12:00 p.m. (noon) by RPMS. However, noon is also used for many ancillary visits. Sites wanting to use a unique time for dental visits can use this parameter to set up a time to be used if no time is sent in the message. The default time should be formatted as *military time* with numbers only. *Do not include a colon in the default time value.*

[Figure 4-6](#) shows an example of default time.

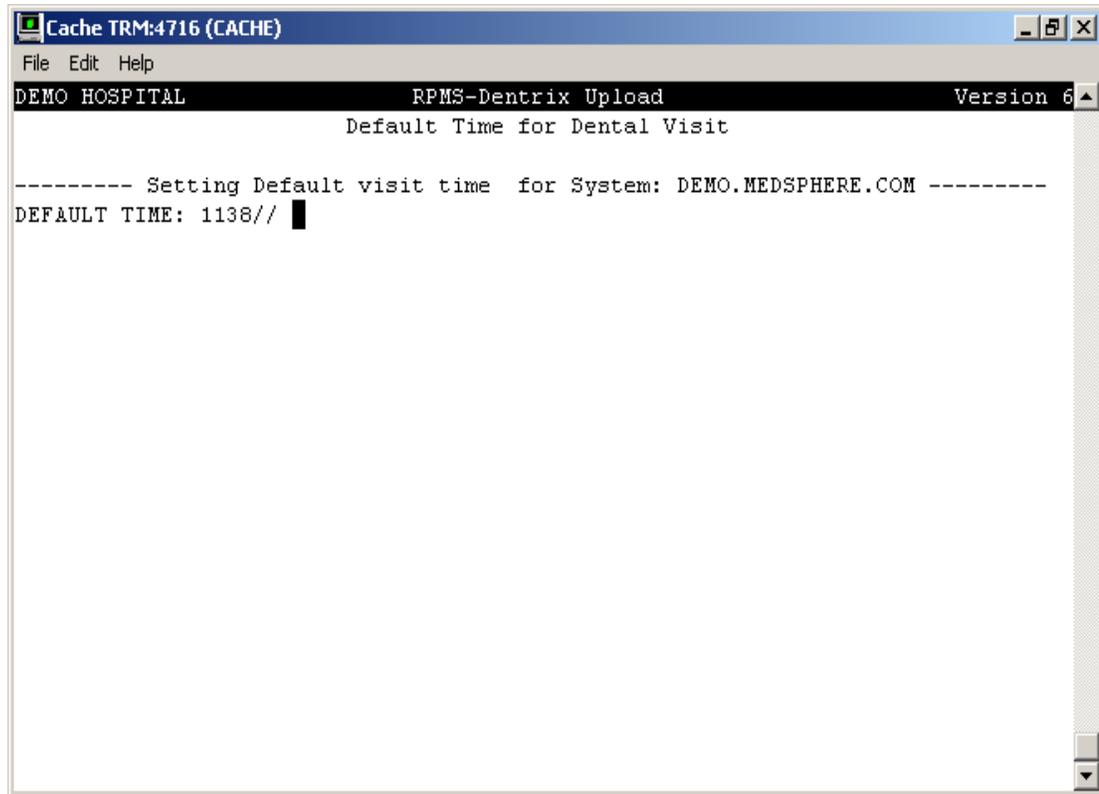


Figure 4-6: Default Time for Dental Visit screen

4.6 USR Default User for Interface

The Dental/EDR Interface stores visits into PCC files. These visits can be seen in the EHR. In the Dental DFT-P03 message coming from the EDR Dental package, only the ASUFAC is sent. There must be an assigned User defined for each ASUFAC. The example below shows how to assign the values. If a facility only supports one ASUFAC then the System interface should be populated with the Institution default dental clinic as defined in the HOSPITAL LOCATION (44) file. The Entry in the HOSPITAL LOCATION file must have the proper Institution defined to assure that the ASUFAC values match. Additionally, a user needs to be associated with this clinic to allow the filer creating the PCC Visit and Dental Procedures to have a user to identify who added the PCC entry or updated the PCC entry. If a site has multiple supported Divisions, then the additional Divisions should be added. Note that there must be one Dental Clinic complete with the Dental Clinic Stop Code and the Dental Treating Specialty assigned in RPMS. Each Clinic should indicate the proper ASUFAC and should be named to reflect the site. Use the Default User for Interface screen ([Figure 4-6](#)) to set this parameter.

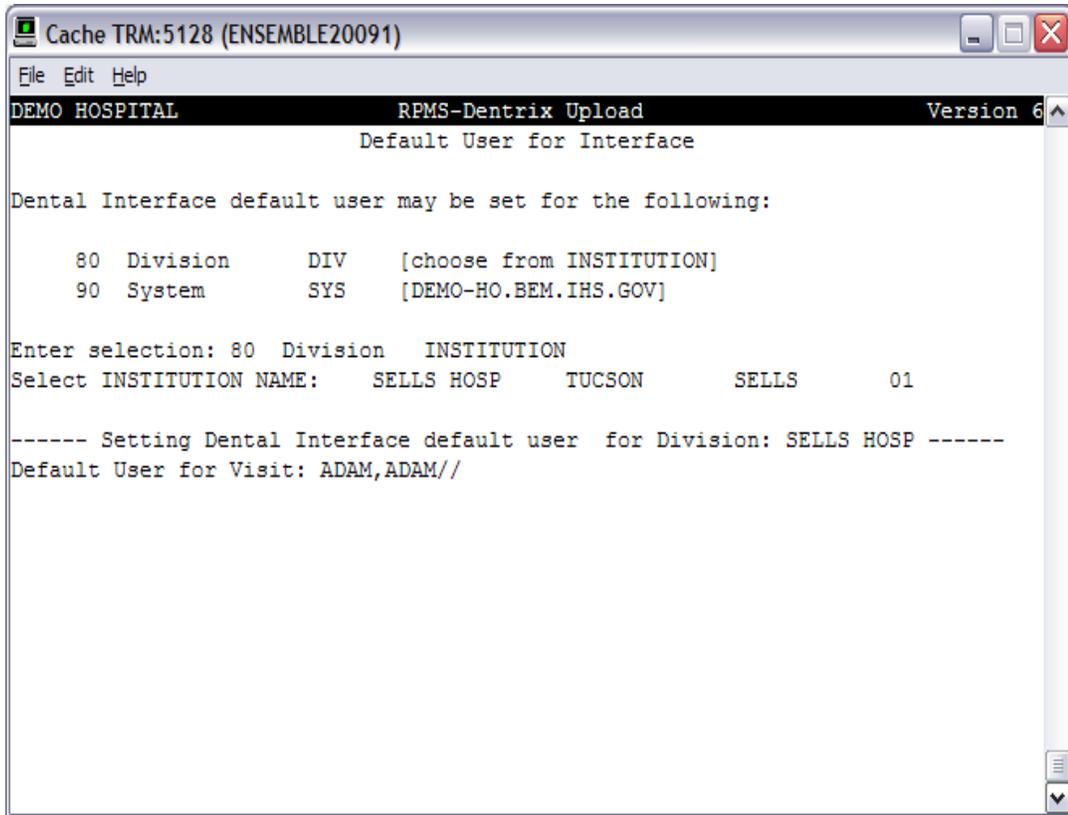


Figure 7: Example of setting Default User for Interface (USR)

5.0 HLO Management

Use the HLO Menu to enter the system parameters which allow messages to be created using the HLO application. Refer to the installation guide to set these parameters. After initial setup, the user should have no reason to use the HLO Management system to monitor the message system. All of the monitoring is preformed in the Ensemble System Management Portal using the Integration Engine. The HLO links associated with the EDR system should not be turned on. See the following manuals for questions about HLO:

- VistA HL7 – Optimized (HLO) Installation manual /Release notes (hl_1_6_126_ig.pdf)
- VistA HL7 – Optimized (HLO) Technical Manual (hl_1_6_126_tm.pdf)

HLO is accessed from the HL7 Main Menu (Figure 5-1). At the “Select HL7 Main Menu Option” prompt, type **HLO** and press the Enter key.

```

Cache TRM:3352 (CACHE)
File Edit Help
<NOLINE>
EHRD>D ^XUP

Setting up programmer environment
This is a TEST account.

Terminal Type set to: C-VT100

Select OPTION NAME: HL7 MAIN MENU  HL MAIN MENU    HL7 Main Menu

      Event monitoring menu ...
      Systems Link Monitor
      Filer and Link Management Options ...
      Message Management Options ...
      Interface Developer Options ...
      Site Parameter Edit
HLO   HL7 (Optimized) MAIN MENU ...

You have PENDING ALERTS
      Enter "VA to jump to VIEW ALERTS option

Select HL7 Main Menu Option: █

```

Figure 5-1: HL7 Main Menu

[Figure 5-2](#) shows the HLO Main Menu options. The SM HLO SYSTEM MONITOR and the MV HLO MESSAGE VIEWER options are frequently the most used.

```

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

```

Figure 5-2: HLO Main Menu

6.0 Creating Dental Visits

Inbound HL7 messages from the EDR create, update, and/or delete PCC data. Each inbound message contains patient data and data for a dental visit.

Dental visit data is received and stored into PCC. Visits are created, POVs and providers assigned, and the V DENTAL file populated. New messages are handled in the following manner:

1. The message arrives.
2. The Dentrax unique number is found. This number is stored in the EXTERNAL KEY field of the V DENTAL file.
3. The V DENTAL file is searched to determine if this is a new number.
4. The description field of the message is checked to determine whether it is “new,” “update,” or “delete.”
5. If the key is new:
 - a. If the description is “new”:
 - i. Find or create a new visit
 - ii. Add a VPOV if it’s a new visit
 - iii. Add the provider if it’s a new visit
 - iv. Add a new V DENTAL entry
 - b. If the description is “change,” it is an error since the key was not found in RPMS.
 - c. If the description is “delete,” it is an error since the key was not found in RPMS.
6. If the key already exists:
 - a. If the description is “new,” it is an error since it cannot be added twice.
 - b. If the description is “change”:
 - 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.

6.1 Errors on Inbound Messages

Errors can be generated for a variety of reasons. Inbound messages that cannot be filed in PCC from Dentrrix send an alert to people in the mail group RPMS DENTAL. RPMS Inbound DFT-P03 message errors and descriptions:

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

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 Ensemble EIE 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.
```

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.
```

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.
```

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.

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.

Patient merge DFN identifier cannot be found in RPMS.

The patient merge indicator was set, but there is no merged DFN in RPMS. If this alert is created, a developer of the EDR RPMS system will need to determine cause and correction.

Last names for _DFN_ do not match in message.

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.

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.

FTI segment not found in message.

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.

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.

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 VDental file to update or delete. If there is no corresponding EXTERNAL KEY then this alert will be generated. The most common cause is that the original procedure was not properly filed and also 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.

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 VDental 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.

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.

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.

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.

Unable to find code _ADA CODE_ in message.

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. If this alert is created, a developer of the EDR system will need to determine cause and correction.

No location found in the message.

Every message coming from Dentrix must have an associated ASUFAC. The ASUFAC was not in FT1 16.1 or was non numeric. 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.

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.

Clinic does not exist in RPMS in the message.

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.

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 HOSPIAL 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.

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.

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.

Multiple visits exist and cannot match.

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.
```

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 Dentrrix matches to the VDent 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 got to Dentrrix with the name change. If this alert is created, a developer of the EDR RPMS system will need to determine cause and correction.

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

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 VDent file entry and the Visit entry associated with the VDent 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.
```

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 VDent file entry and the Visit entry associated with the VDent 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.
```

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.

```
EDR message (message number) did not receive a correct commit acknowledgement.
```

Then a message is processed in RPMS, an acknowledgement message is generated to notify Dentrrix that some action has occurred on the message. Dentrrix does not process acknowledgements. This message alert occurs frequently and can be ignored.

6.2 Visit

When a message is processed, a call is made to find or create a new visit. Since there can be more than one procedure on a visit, it is not always necessary to make a new visit.

[Figure 6-1](#) shows what a visit created by the dental interface looks like in FileMan output.

```
VISIT/ADMIT DATE&TIME: FEB 09, 2009@11:33
DATE VISIT CREATED: FEB 10, 2009 TYPE: IHS
PATIENT NAME: TEST,PATIENT A LOC. OF ENCOUNTER: DEMO HOSPITAL
SERVICE CATEGORY: AMBULATORY CLINIC: DENTAL
DEPENDENT ENTRY COUNT: 3 DATE LAST MODIFIED: FEB 10, 2009
MFI STATUS: ADD HOSPITAL LOCATION: DENTAL
CREATED BY USER: HAGER,MARY G USER LAST UPDATE: HAGER,MARY G
COMPUTER GENERATED: DEMO HOSPITAL
OLD/UNUSED UNIQUE VISIT ID: 3531730000000161
DATE/TIME LAST MODIFIED: FEB 10, 2009@18:15:42
NDW UNIQUE VISIT ID (DBID): 137520000000161
VISIT ID: 10HX-DEM
```

Figure 6-1: Visit details

If the CLN option (Default Clinic for Interface) was used to set a default clinic, the clinic name appears in the CLINIC field.

6.3 V Provider

The provider attached to the procedure is stored as the visit provider. A change 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 6-2](#) shows the FileMan output from the V PROVIDER file for a dental visit.

```
PROVIDER: HAGER,MARY G PATIENT NAME: DEMO,BOY
VISIT: FEB 09, 2009@11:33 PRIMARY/SECONDARY: PRIMARY
```

Figure 6-2: Visit provider details

6.4 V POV

The purpose of visit for dental visits is always V72.2. [Figure 6-3](#) shows the output of a VPOV for a dental visit.

```
POV: V72.2 PATIENT NAME: DEMO,FATHER
VISIT: FEB 09, 2009@11:33
PROVIDER NARRATIVE: DENTAL/ORAL HEALTH VISIT
```

Figure 6-3: V POV details

6.5 V Dental

The V Dental file holds the dental data. This is *not* stored in the dental package files, only in the PCC V DENTAL. The following fields are populated:

- Dental Service Code (the ADA code)
- Patient Name (pointer to the patient file)
- Visit (pointer to the visit file)
- Number of Units (always set to 1)
- Operative Site
- Tooth Surface
- Fee
- Event Date and Time (same as visit date and time)
- Ordering Provider (provider of the visit and sent in the message)
- Clinic – DENTAL (pointer to clinic stop for dental)
- Encounter Provider (same as ordering provider)

[Figure 6-4](#) shows the FileMan output of a V DENTAL entry performed through the interface.

```
SERVICE CODE: 2721      PATIENT NAME: DEMO,MOTHER R
VISIT: FEB 05, 2009@11:33  NO. OF UNITS: 1
OPERATIVE SITE: PERMANENT CENTRAL INCISOR,MAND LEFT
TOOTH SURFACE: MOODL      FEE: 300
EVENT DATE&TIME: FEB 05, 2009@11:33 ORDERING PROVIDER: HAGER,MARY G
CLINIC: DENTAL          ENCOUNTER PROVIDER: HAGER,MARY G
EXTERNAL KEY: 1000012
```

Figure 6-4: V DENTAL details

6.6 Browse a Visit

The user can see and process these dental visits the same as any other PCC visit. [Figure 6-5](#) shows a dental visit viewed through Display Data for a Specific Patient Visit in PCC.

```
Patient Name: DEMO,FATHER
Chart #: 5465
Date of Birth: MAR 05, 1955
Sex: M
Visit IEN: 165

===== VISIT FILE =====
VISIT/ADMIT DATE&TIME: FEB 09, 2009@11:33
DATE VISIT CREATED: FEB 10, 2009
TYPE: IHS
PATIENT NAME: DEMO,FATHER
LOC. OF ENCOUNTER: DEMO HOSPITAL
SERVICE CATEGORY: AMBULATORY
CLINIC: DENTAL
DEPENDENT ENTRY COUNT: 4
DATE LAST MODIFIED: FEB 10, 2009
MFI STATUS: ADD
HOSPITAL LOCATION: DENTAL
CREATED BY USER: HAGER,MARY G
USER LAST UPDATE: HAGER,MARY G
COMPUTER GENERATED: DEMO HOSPITAL
OLD/UNUSED UNIQUE VIS: 3531730000000165
DATE/TIME LAST MODIFI: FEB 10, 2009@18:57:34
NDW UNIQUE VISIT ID (: 137520000000165
VISIT ID: 10J3-DEM

===== DENTALS =====
SERVICE CODE: 2330
NO. OF UNITS: 1
OPERATIVE SITE: PERMANENT FIRST BICUSPID,MAND RIGHT
FEE: 55
EVENT DATE&TIME: FEB 09, 2009@11:33
ORDERING PROVIDER: HAGER,MARY G
CLINIC: DENTAL
ENCOUNTER PROVIDER: HAGER,MARY G
EXTERNAL KEY: 1000018
V FILE IEN: 17

===== PROVIDERS =====
PROVIDER: HAGER,MARY G
AFF.DISC.CODE: 152MGH
PRIMARY/SECONDARY: PRIMARY
V FILE IEN: 174

PROVIDER: HAGER,MARY G
AFF.DISC.CODE: 152MGH
PRIMARY/SECONDARY: PRIMARY
V FILE IEN: 175

===== POVs =====
POV: V72.2
ICD NARRATIVE: DENTAL EXAMINATION
PROVIDER NARRATIVE: DENTAL/ORAL HEALTH VISIT
V FILE IEN: 120
```

Figure 6-5: View PCC Dental Visit

Figure 6-6 shows a dental visit viewed through the EHR.

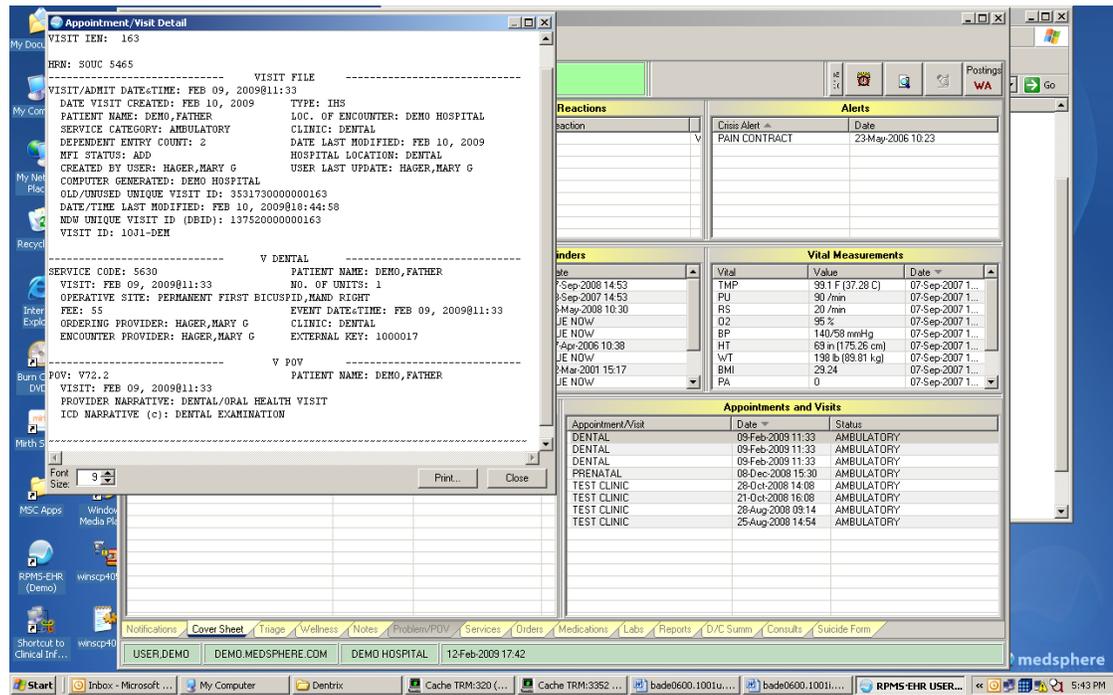


Figure 6-6: EHR View Dental Visit

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

Both documents are available at this IHS web site,

<http://security.ihs.gov/>

The Rules of Behavior listed in the following sections are specific to RPMS.

7.1 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).

7.1.1 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.

7.1.2 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.

7.1.3 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.

7.1.4 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.

7.1.5 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.

7.1.6 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).

7.1.7 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.

7.1.8 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.

7.1.9 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

7.1.10 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.

7.1.11 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

7.1.12 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.

7.1.13 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) when ever 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.

7.2 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.

7.3 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.
- Not release any sensitive agency or patient information.

8.0 Contact Information

If you have any questions or comments regarding this distribution, please contact the OIT Help Desk (IHS).

Phone: (505) 248-4371 or (888) 830-7280 (toll free)

Fax: (505) 248-4363

Web: <http://www.ihs.gov/GeneralWeb/HelpCenter/Helpdesk/index.cfm>

Email: support@ihs.gov