RESOURCE AND PATIENT MANAGEMENT SYSTEM

IHS Dental Data System

(DDS/ADE)

User Manual

Version 6.0 Patch 39
October 2023

Office of Information Technology
Division of Information Technology

Table of Contents

Preface

This manual provides details concerning the contents and use of the IHS Dental Data System (DDS/ADE). Due to its nature, its primary audience will be Information System personnel and Site Managers responsible for utilizing the functions of this package in a clinic or dental office environment.

The HSA 42-2 and HSA-57 forms are rarely (if ever) used, but the information is included in this document, since it may be useful for historical guidance rather than current usage.

ADE v6.0 p39 contains changes to support the Social Security Number Fraud Prevention Act of 2017 and the Social Security Number Reduction Act.

1.0 Introduction

1.1 Overview of the DDS Package

The DDS software package of the RPMS has been designed to meet common data processing needs of facility-based dental program operations, as well as those of central management.

The DDS package can operate as an integrated module of the Patient Care Component (PCC) or as an independent package linked with the IHS Patient Registration System. The DDS captures the minimum data requirements for direct care and contract care programs and includes data extraction and transmission routines for central processing. Various additional data entry/edit and retrieval options are available which may be used and modified according to the needs of the local site.

1.2 Benefits of Using the PCC and DDS

There are important advantages in having the DDS as part of the PCC, as well as advantages in having the PCC operating in addition to the DDS package. The most obvious is that the PCC is designed to create an integrated, automated patient health record that can serve all health disciplines for various applications in care delivery, planning, management, and research.

If the DDS is operating as part of the PCC, the dental visit data entered into the DDS options automatically generates a patient encounter in the PCC. This is important for administrative reasons, but it also generates information in the Patient Health Summary of the PCC, which is of value to any type of care provider. Further development of the DDS package will occur under the auspices of the Dental Professional Services Group (PSG).

Dental users can also provide feedback, including functionality requests at the following location: https://www.ihs.gov/rpms/feedback/

2.0 Information for New Users

Before using the DDS package, the user should ensure that the administrative responsibilities for setting up the system have been addressed. These tasks are outlined below.

2.1 Site Manager

- Install the DDS package (see installation notes included with the distribution files).
- Set up user terminals and printers.
- Set up DDS users and add dental personnel and providers to the system. Be sure Social Security Numbers, Affiliation, and Provider Class are entered for all dental providers.
- Orient the dental supervisor and determine policies for operations.
- Assist with periodic data extraction and updating of controlled files as necessary. Provide technical assistance to users when needed.

2.2 Dental Supervisor

- Assist Site Manager with dental site preparations. Provide required data on personnel, providers, and key allocation.
- Determine where/who will enter dental visit data and orient personnel. (This may be designated key-entry personnel outside of dental).
- Add/edit data in controlled files and initiate periodic data extraction. Request changes/questions to Site Manager.
- Audit quality of dental data entered and seek or provide assistance to maintain smooth operations.

In addition to the DDS User Guide, the package also includes extensive automated help information, which users can access while they are signed-on to the computer. This information is contained in narrative text which has been created for most of the DDS menu options and data input prompts.

Online help information is available anytime you are unsure of how to respond to the computer by entering one or more question marks (**?**) and pressing the **Return** key. A question mark can also be used to view extensive information regarding any DDS menu option by invoking Help Frames stored in the computer. Many Help Frames contain Keywords [in brackets] that lead to related frames of information.

2.3 Some Basic Information for RPMS Users

There are common features and general rules (or conventions) for using RPMS applications, which users should learn quickly.

2.3.1 Responding to Computer Prompts

Users interact with RPMS computers by responding to specific requests for information called prompt lines. Common problems in responding are:

- New users do not understand what a prompt is asking them to do.
- Experienced users do not read prompts carefully before entering their responses.

All RPMS applications use similar conventions to accept input from the user. The databases (files) are set up to allow responses in two basic ways:

- To accept choices from only the existing entries in a file.
- Allow users to add new entries to the list of choices as they use the application.

The **Return** key must always be used to send responses to the computer. When a response cannot be matched by the computer with one or more acceptable choices, the **??** (unknown value) will be displayed by the system and the same prompt line will reappear. By entering **??** at any prompt a user can view the possible choices and how they can be entered.

2.3.2 Some Important Features on the Wyse Keyboard

There are several keys that serve important purposes in RPMS applications. Although the arrangement and labeling of keys on different types of computer keyboards vary, every keyboard can be used to execute virtually the same functions. The following information applies to the WYSE terminals (Table 2-1) used by the IHS.

Table 2-1: WYSE terminals keys used by the IHS

KEY	USE
SET UP	Sets up the Terminal and Function keys
LOCK	Caps Lock – Upper Case
Return	The Return or Enter Key
HOLD	Freezes the Screen
BACKSPACE	Backspace/Delete Key

Another important feature of WYSE terminals is the ability to program the **Function Keys (F6-20)** to execute frequently used commands. See the Site Manager for programming these keys.

2.3.3 Signing on to the System

To prevent unauthorized use of the computer system, each user is assigned codes allowing access. These codes are assigned by the local RPMS Site Manager.

Upon entering the system, the user is prompted for an **Access Code** and then a **Verify Code**. These codes are initially assigned by the Site Manager. Upon receiving their own codes, users should not write them down or share them with any other users. Entering these codes will identify the specific user to the computer, and the user's name will be associated with many of the functions performed through the computer (for example, sending messages, entering data, and registering a patient).

When users log on, they may see a message displaying the last time they were logged on. If a user suspects someone is using their codes, they should change them immediately. Users can change their own Verify Codes via the Automatic Menu option EDIT USER CHARACTERISTICS. They may also be required to change their Verify Code periodically. The Site Manager can change a user's Access Code.

Note: **ACCESS** and **VERIFY** can be entered on one line separated with a semicolon (**;**) to speed up the sign-on process.

2.3.4 Exiting from Options and the DDS

There is more than one way to exit from RPMS applications. By entering only a **Return** at each prompt, the user will back out of the option being used and return to each preceding menu one layer at a time until the system prompts:

```
Do you really want to halt?: YES//
```

Figure 2-1: System Prompt

Press **Return** and the computer session will end. By entering **Halt** at any menu option, the user will immediately exit from the application and from the computer session. The user must then sign-on again to begin another session. The user is also permitted to use the **Continue** command instead of the **Halt** command when immediately returning to a particular menu option the next time the user signs onto the system.

2.3.5 Using the Menu System

The menu system is the way through which options are accessed. Menus are arranged in a hierarchical (or tree) structure. Starting at the top, the user can progress through levels to get to all desired options. When at the menu system, the following prompt (Figure 2-2) appears.

```
Select ... Option:
```

Figure 2-2: Menu System prompt

Respond to this prompt by naming an option available at this level. A group of options called the Automatic Menu are available at all times. This may include options particular to individual users. If more information is required to be able to respond to a **Select ... Option** prompt, entering question marks (**??**) will be of help.

2.3.6 Jumping to an Option

If users know the name or synonym of an option, they can go directly to it (or jump to it) by using the caret, **up-hat (^)** key. This means that they do not need to step through several levels of menus to get to an option.

In response to the **Select ... Option** prompt, enter **^OPTION NAME**, where **OPTION NAME** is the name or synonym of the option to which to jump. Enter only enough characters to uniquely identify the option. If what has been entered matches more than one option, the user is prompted for a choice. Occasionally a message about rebuilding menus appears. In such a case, a menu has been changed and the system must take a few moments to rebuild some internal structures. In such cases, the user may access the option through the menu tree. It is recommended that the user learn to use the Jump feature as soon as possible and to memorize the menu synonyms he frequently uses.

2.3.7 Using Question Marks in the Menu System

There are different sorts of help available by entering question marks (**??**) at a **Select ...Option** prompt.

- **?** – A single question mark lists all options that can be accessed from the current one.
- **??** – Two question marks list all options, showing their formal names.
- Also listed will be the automatic menu containing options that are always available to the user.
- **???** – Three question marks will show brief descriptions for each option on the menu.
- **????** – Four question marks show extended help for this menu.
- **?OPTION** – An option name preceded with a question mark (**?**) shows extended help for that option.

2.3.8 Using the Online Help Frame System

The DDS package makes extensive use of online help. When the user enters **???** and presses **Return** at any prompt to select a menu option, a brief description of each option appears. However, much more information, including instructions and examples, may also be available through the help processor if the words Extended Help Available appear after the Option Name described when using the **???**.

To get help for a given menu option enter a **?** followed immediately (no space) by the option synonym (the 2-4 letters in front of the option name). Help frames may also contain keywords that link to other Help Frames. Keywords in the Help Frame text will be highlighted on the video screen or enclosed in brackets.

2.3.9 Abbreviated Responses, Synonyms and Mnemonics

All RPMS applications allow abbreviated responses, synonyms, and mnemonics. This function permits users to enter only the first letter or series of letters for the response to be used. This saves time and helps control data entry errors. When a single letter response is sufficient to identify an item, the choice will be executed. When more than one possible answer exists based upon the response, the possible choices will be displayed (in groups of 5 items at a time) and the user will be prompted to select an item from those listed by entering its number. When entering a person's name, it is best to use enough letters of his name to prevent getting a long list of possible choices.

2.3.10 Understanding and Using Default Values

All RPMS applications provide default functions for responding to most prompts. A default value can be defined loosely as the most probable answer or the most recent answer to a prompt for input. Default values may be displayed automatically along with an input prompt (Figure 2-3) in the following format:

```
Input prompt: DEFAULT VALUE //
```

Figure 2-3: Input prompt

The double slash marks (//) always identify a default value. Pressing the **Return** key at a prompt with a default value will accept (use) that value as the input. If the default value is not desired, enter the correct input value and press **Return**. Not all prompts will have a default value displayed. However, the user may use the most recent value stored for a given prompt (data field) by pressing the **Space Bar** once, followed by a **Return**. This command works for menu options and other input prompts.

Note: Be careful, because indiscriminate use of this command can result in entering the wrong value into a database.

2.3.11 Identifying a Patient to the Computer

Patient names (and most other names) are stored in the RPMS Patient File in the form: **LASTNAME,FIRSTNAME MI**.

> **Note:** There is no space after the comma between the first and last name.

To identify a patient at any Select Patient: or Enter Patient's Name: prompt, enter either:

- The patient's Health Record Number (HRN), if known.
- Any portion of the patient's name, in the form shown above.

For example, entering the letters MIL will produce a list of all persons in the database whose last name begins with the letters MIL such as MILLER, MILTON, etc. The user then chooses from the names listed as choices.

Once a patient name is selected, the computer will list the patient's **name**, **date of birth**, and **HRN**. It will then prompt Figure 2-4):

```
OK?//
```

Figure 2-4: Patient Information OK prompt

At this moment, it is important to ensure these data match the person to be identified before accepting the name displayed.

2.3.12 Printers – Slaved Printers and Line Printers

RPMS users can direct outputs to a printer or any other local terminal by specifying:

- The device number
- The width of right margin for the report
- By queuing the report to print at a later time if necessary

There are two basic ways printers can be set up to function at RPMS sites:

- Connected to the main RPMS computer itself
- Connected to a video terminal

Printers connected to video terminals are called slave printers. Slave printers operate either through the PRINT SCREEN function of the terminal to which they are linked, or by entering **S** for slave at the Device: prompt.

- Slave printers are efficient for printing brief reports (for example, individual health summaries, or records) that are needed immediately.

Printers connected directly to the computer (line printers) can be accessed from any user terminal, unless restricted by the Site Manager. Such printers can produce outputs any time of day, even after the user has signed off, but slave printers usually cannot.

- Line printers are best for large jobs that can be queued to run overnight when fewer people are using the computer.

3.0 Entering Dental Visit Data Into the DDS

There are four basic steps to entering dental visit data into the DDS package:

1. Select a patient name using their HRN as entered on the HSA 42-2 (pink slip) if used.
2. Enter the date of the visit as recorded on the HSA 42-2 (and approximate time if necessary).
3. Add/edit data on the **CURRENT VISIT ENTRIES TABLE** at the Select ADA Code (or Action) prompt:
    a. Visit Status Code
    b. Procedure Codes
    c. Quantity or Tooth Numbers, Operative Sites, and Surfaces
    d. Fees, if contract
    e. Brief notes, if desired
    f. Attending Dentist and Auxiliary Providers

3.1 Step Details

The following describes the details of each step:

- Begin each data entry session by entering a location (required). Thereafter, the user will be prompted to enter other core dental data beginning with a patient name and date of visit.
- Next, add or edit data at the ADA Code prompt by using the Responses (or Actions) allowed. These actions include adding the patient to RECALL or WAITING lists.
- Visits are not actually created (stored) in the DDS files or the PCC until the user presses Return at the ADA Code prompt. Users may easily edit the entries or erase the visit before it is actually created in the RPMS. However, once the visit exists in these files, users must edit or delete the visit in a different manner.
- After data entry for a visit is completed, users may add new visits, or enter Return at the prompt for a patient name to change the location, if necessary.

3.2 Dental Visit – Core Data Elements

The core data elements for dental visits are those specified by IHS to support centralized processing of clinical workload data as well as those to support patient and program evaluation. The core data inputs (Table 3-1) for entering direct and contract care dental visits are listed below in the sequence prompted by the computer.

Table 3-1: Core Data Inputs

Core Data Inputs	Description
FACILITY	Location of the dental visit
HYGIENIST/THERAPIST	The secondary provider
DENTIST	Reporting (or attending) dentist for the visit
PATIENT	Dental patient name or record number
DATE	Date of the visit
VISIT STATUS CODE	The dental visit status code
ADA CODE	Standard dental procedure codes
QUANTITY	The quantity of units for a procedure
OPERATIVE SITE	Dental operative site for a procedure
FEES	The fee charged for a dental procedure (contract only)

3.3 Identifying a Dental Patient Name

RPMS conventions have been established for entering patient names. It is recommended that the HRN be used routinely to identify patients for dental visit data entry (in lieu of entering a name) to prevent errors.

Patient names and HRNs are drawn from the database of the RPMS facility being used to report the dental visit data. Thus, patients who are registered at other facilities but not at the reporting facility will NOT be allowed unless their registration records have been merged with the local facility, including the RPMS facility where the data is being entered.

After an HRN is entered, the **name**, **HRN**, Social Security Number (**SSN)**, and **date of birth** will be displayed on the same line. If this is not the correct patient, enter **Return** at the prompt to select the Visit Date, then re-enter the correct patient name or ID number. The user may also edit the patient’s name by pressing **Return** at the Visit Status Code prompt, or start over by entering an Up Hat (^) and a **Return** at the ADA Code prompt.

A visit will not be created until a visit status code has been entered. If the user fails to correct a patient name before all data is entered and the visit files are updated, the user should delete that visit using the **VDEL** option. Although he can re-enter the correct name and data under the DDV or CDV entry options, he must delete the visit that was created under the wrong patient name.

3.3.1 The Reporting (Attending) Dentist

A Reporting Dentist for each dental visit is ALWAYS required. The Reporting Dentist is defined as the attending dentist for medico-legal purposes even though an auxiliary may actually provide certain expanded-duty services. Before data can be entered for a dentist, the provider must be added using the AVA Add/Edit Provider option by the Site Manager to include all required data for each dentist.

The Site Manager must handle the deactivation of provider names when they transfer to another facility or terminate their employment. It is essential that the Site Manager be advised when new dentists arrive or when incumbent dentists leave permanently.

It is recommended that mnemonics (initials) be used to enter a reporting dentist or auxiliary. The mnemonics (initials) must be added or edited using the RPMS AVA Add/Edit New Persons option or User Management, Edit an Existing User option (update the initials), prior to data entry. If mnemonics are not used to enter the reporting dentist, a surname can be entered. The name of the reporting dentist entered will be displayed on the CURRENT VISIT ENTRIES table.

At one-dentist clinics, the Dental Supervisor can set the Default Dentist to that dentist. Always check to ensure that correct dentist has been selected before entering the ADA procedure codes for the visit. If the dentist’s name displayed in the Current Visit Entries table is incorrect, enter **^D** at the Select ADA Code (or Action) prompt. The dentist’s name will reappear as a default value that the user can change.

After selecting a dentist, the system prompts the user to use this same dentist for subsequent visits during the current data entry session. If the response is **NO**, the dentist will only be changed for the current visit. If answering **YES**, the dentist selected will become the default dentist for the remainder of the data entry session or until there is a subsequent change in dentists.

3.4 Dental Hygienist/Therapists

The Dental Hygienist/Therapist is optional. All auxiliaries who will be named in this field must have Dental Hygienist/Auxiliary entered in the PROVIDER CLASS field of the RPMS New Person file by the local Site Manager prior to the entry of visit data. New auxiliaries are added or edited using the AVA ADD/EDIT Provider option or User Management, Edit an existing user to edit existing entries. Also, ensure their Affiliation is set to IHS for the Direct Dental Visit (DDV) option. For data entry purposes, the mnemonic (initial) established for each EF auxiliary and hygienist should be entered on the HSA 42-2 over the mnemonic for the reporting dentist. For example, FJ/WN in the signature space would mean FJ is the expanded-duty auxiliary and WN is the reporting dentist. The Hygienist/Therapist can be changed for the current visit for which the user is entering data by entering **^H** at the Select ADA Code Or Action: prompt.

After changing the Hygienist/Therapist, the system prompts the user to use this same Hygienist/Therapist for subsequent visits. If the response is **NO**, the Hygienist/Therapist will be changed for the current visit only. If answering **YES**, the Hygienist/Therapist entered will become the default for subsequent visit entries until it is changed again.

3.5 Location of a Dental Visit

The location of a dental visit is where the encounter actually took place, which is not necessarily the site from where the data are entered into the computer. The choices are drawn from the Dental Site Parameters file.

Enter the 6-digit area/su/facility code if desired, but mnemonics are recommended instead. The nn-nn-99 code (Undesignated Locations) may be used to enter data for private dentists working in their own offices.

Contact the area dental office if an undesignated location does not already exist for the service unit. Do not use the -98 code for dental laboratories because such reporting produces false dental visits in the RPMS patient records.

3.6 Date of a Dental Visit

The Select Date of Visit: prompt asks for the date on which the dental encounter actually took place. Visit dates will usually be taken from the HSA 42-2 or HSA 57. If the visit dates are missing or unreadable, the data entry form (pink slip) should be returned to the clinic or dentist involved for correction/clarification of the date(s).

The date may be entered in several forms that are shown below. Examples of valid date formats:

- JAN 22 l957
- 22 JAN 57
- 1/22/57
- 012257 – T (for TODAY)
- T+1 (for TOMORROW)
- T+2
- T+7
- T-1 (for YESTERDAY)
- T-3W (for 3 WEEKS AGO)

If the year is omitted, the computer uses the CURRENT YEAR. Pressing **?** at the Select Date of Visit: prompt produces a display of all the visit dates that have been entered for the selected patient. If needed, this is a crude way to check for previous visit dates during the current fiscal year before entering a Visit Status Code.

Create a new visit date to enter dental data or edit the data for an existing visit by selecting an existing date from the list. If a Visit Time is indicated on the HAS 42-2 next to the date, it must be entered with the date. For example, 10-1-2020@1030 would record a dental visit at 10:30 a.m.

Note: The time of a visit MUST be recorded if the patient was sent to the pharmacy for a dental prescription.

Multiple visits for the same date can be created by enclosing the date in double quotes (**" "**) for each subsequent visit for that date. Entering **Return** at the date prompt allows starting over with a patient name. The user may also start over by pressing **Return** at the Visit Status Code: prompt. Once a visit has been created in the DDS, the user must use the VDEL Delete Visit option to remove that visit date.

3.7 Current Visit Entries Table

The Current Visit Entries Table is displayed after the Visit Date has been entered. This table enables users to view and check all data entered for a dental visit to facilitate editing if necessary. It identifies the patient, facility, hygienist or therapist (if entered), reporting dentist, and date of the current visit for which ADA Codes will be entered. As ADA Codes are entered for the visit, they will be displayed on the table. The quantity of units and operative sites (if used) reported are displayed after each code.

3.8 Using the Dental Visit Status Codes

The Dental Visit Status Codes (**0000**, **0190**, **9986**, and **9987**) have been created by the IHS to count patients and visits in the central data processing system. If the site has been using the DDS since the beginning of the current fiscal year, the computer will automatically compute First Visit (**0000**) and Revisit (**0190**) codes. If not, always select a Visit Status Code for each visit immediately after the Visit Date has been selected. The Visit Status Code can be edited like other ADA Codes with certain exceptions. If the user deletes a Visit Status Code, one must be added back to the Current Visit Entries Table before the visit can be stored in the DDS files. Change a Visit Status Code by entering a new one and it automatically replaces the one listed on the Current Visit Entries Table. If the user enters the Missed Appointment (**9986**) or Cancelled Appointment Code (**9987**), no other ADA Codes can be added to the visit and any existing code entries will be cancelled.

3.9 Using the ADA Code Prompt

At the Select ADA Code or Action prompt, enter a procedure code, or invoke other actions (Table 3-2) to enter, edit or end data entry for the visit from the responses below:

Table 3-2: Procedure Code and Action

USER RESPONSE	ACTION EXECUTED
^ or ^Q Abort	Data entry without changing or adding anything. Use ^ or ^Q to start over.
4-digit ADA Code	To enter a dental procedure for the current visit. Only established codes in the ADA CODE FILE can be used in the DDS.
@ code	To delete a code from the visit, e.g., @2150.
^N	Enables user to enter a brief dental NOTE.
Re-enter a code	To edit the quantity, operative site, tooth surface or fee values.
^L	To change the LOCATION for the current visit.
^D	To change the DENTIST for current visit.
^H	To change HYGIENIST/THERAPIST for current visit.
^? or ??	To see Help frames (?) or use of ADA codes (??).
^C	To edit Total Charge on Contract Visits.
^P	To display primary tooth Opsites as Letter Codes.
^W	To add this patient to a treatment Waiting List (also see Patient Mgmt. options).
^R	To add this patient to a treatment Recall List (also see Patient Mgmt. options).
^V	To display the patient's dental record.
Return Only	To complete data entry for this visit. The system will prompt the user to file the data in the computer before proceeding to the next patient. Answer **Y** (Yes) for the visit data to be saved.

3.10 How to Get Information on ADA Codes

Most of the ADA Procedure Codes in the ADA Code file include narrative text to help users understand their proper use. To see this text, enter **??** twice and press **Return** at the Select ADA Code (or action): prompt. Then enter the ADA Code and press **Return** at the prompt given.

3.11 Using Dental Operative Sites

For certain types of ADA Codes that are not full-mouth procedures, users will be prompted to enter an Operative Site (tooth numbers, sextants, etc.). Anatomic names (or mnemonics) listed in the Dental Operative Site file are allowed. The sites contained in this file are considered exhaustive for reporting purposes; therefore, editing of this file should not be undertaken by a local RPMS site. A listing of entries in the operative site file can be obtained through the Dental Supervisor's Print/DisplayOptions of the DDS.

Users will not be prompted to enter operative sites for ADA Codes that involve the entire mouth (such as exams or prophylaxes). Only Opsites for deciduous teeth can be selected for the ADA Codes designated for primary teeth (**2110-2131**). Enter deciduous teeth as numbers (**4d through 20d**) or as letter codes (**A-T**) at the Opsite prompt. As many as 32 different operative sites can be entered for a procedure code in one visit by entering commas between each operative site mnemonic selected. For example, the following entry would store seven operative sites (Figure 3-1) for code 7110 (simple tooth extraction):

```
Select ADA CODE: 7110
Select OPSITE: 3,4,7,8,9,13,16
```

Figure 3-1: Operative Site storage example

The data would then appear in the Current Entries table. To delete or edit an operative site already entered, re-enter the **ADA Code** involved and the existing Opsite data for that code will be displayed as a default value at the Select OPSITE: prompt. Enter **@** and the **Opsite** to delete the Opsite. For example, type @3Enter + and the Opsite to insert a new Opsite (for example, +5).

3.12 Opsites for Deciduous Teeth

Only Opsites for deciduous teeth can be selected for ADA Codes designated for primary teeth (**2110-2131**). Enter deciduous teeth as numbers (**4d through 20d**) or as letter codes(**A-T**). The operative sites selected can be displayed in the Current Visit Entries Table either as tooth numbers or as tooth letters. Ordinarily the deciduous Opsites will be displayed as numbers until **^P** is entered at the prompt to Select ADA Code (or Action). Then, all primary tooth Opsites entered (either as numbers or letters) will be displayed on the table as letter codes.

3.13 Fees for a Contract Dental Service

Professional fees for dental services may be entered for each dental procedure code reported for a visit under the Contract Dental Visit Data Entry option. The Unit Fee for each code should be entered. Fees will normally be entered from the data listed on the HSA 57 Dental Contract Care Authorization (claim) form. If a contract care provider is paid on a fixed rate (not a fee-per-service rate), that provider may be regarded as a direct care provider for data reporting purposes (for example, contract dentists or hygienists who work part-time in a direct care facility).

Fees may be entered in whole dollars or dollars and cents. As each ADA Code and unit fee is entered, the total charge for the entire visit is automatically computed. The total charge for the visit may be edited if it is different from the sum of the fees entered. This is common when additional charges are assumed, discounts are given, or the payment for benefits is shared between the IHS and other agencies or insurance carriers. Enter **^C** to edit the total charge.

3.14 Using Brief Dental Notes

Brief Dental Notes can be created by entering **^N** at the Select ADA CODE or Action: prompt during visit data entry. For Dental Notes to be entered into the computer from the HSA 42-2 (the pink copy of Dental Progress Notes), dental personnel should ensure that the note is entered on the line immediately above the signature line of the HSA 42-2 in a consistent form that is legible and can be easily seen by the person who will enter the data into the DDS. Write the word **NOTE:** then enter the text on the same line. The following are examples of brief notes (Figure 3-2) that might be entered. Each note should not be more than one line (80 char) long.

```
NOTE: – PROLONGED HEMORRHAGE AFTER TOOTH EXTRACTION
NOTE: – SEVERE PERIODONTITIS AS COMPLICATION OF DIABETES
NOTE: – REFERRED FROM DENTAL DEPT. FOR HYPERTENSION EVAL.
NOTE: – SEVERE ANXIETY RX TO ROUTINE DENTAL TX.
NOTE: – ROUTINE DENTAL CARE COMPLETED: RTC IN ONE YEAR OF PRN.
NOTE: – PLACED ON DENTAL TX WAITING LIST FOR PARTIAL DENTURE.
NOTE: – REFFERED TO PRIVATE DENTIST FOR FURTHER WORK.
NOTE: – ROUTINE DENTAL CARE - PATIENT WARNED ABOUT BREAKING APPTS.
```

Figure 3-2: Brief Note examples

Brief notes that are frequently used can easily be programmed on a function key (**F6-F20**) of the Wyse Keyboard to simplify data entry.

3.15 Narrative Notes for a Dental Visit

The DDS contains two different options for entering a dental note in a patient's RPMS treatment record. Both types of notes, the unlimited length Narrative notes and the one-line Brief notes, appear when the patient's dental record is reviewed under the Patient Inquiry option (**^REVW**) of the DDS or in the PCC Health Summary. The narrative (word-processing) note may be entered for an existing visit from the **^NARR** suboption of the Dental Visit Data Entry menu, **^DVIS**.

3.16 Deleting Existing Dental Visits

Dental visits can be deleted by using the VDEL Delete Dental Visit suboption of the DVIS Dental Visit Data Entry menu. The VDEL option will delete an existing visit by date from the DDS Dental Service file and the PCC records as well. To delete a visit, enter the patient's ID or name in the accepted form. Ensure it is the same person for whom to delete a visit before proceeding to the Date of Visit: prompt. Select the date of the visit to delete. The data for that visit (ADA Codes, providers, etc.) is displayed and the user is prompted to confirm that the displayed visit is to be deleted. Type **YES** to the prompt to delete the visit.

4.0 Patient Management Options

4.1 Patient Management Menu

The dental treatment Waiting List (WAIT) and Recall List (CALL) menu options will take time for users to learn well. However, they enable users to set and change priorities, vary time intervals for Recall, and maintain patients on more than one type of followup list over time.

This data is also displayed when a patient's dental record is reviewed (REVW). The Recall List menu options are exactly the same, and function in exactly the same manner as the Waiting List menu options. Any type of Waiting or Recall list can be created, but providers will be reminded, and prompted to take action after patients have remained on these lists for a specified period of time. Followup actions can be taken in various ways on individual patients and groups of patients. Use the Help Frames provided with each menu option before they are used routinely.

New options in v6.0 allow users to generate patient mailing labels in a standard format from search templates that have been created from ANY patient file. The template must be created before using this option by using the SEARCH feature of FileMan or the options included in the Dental Wait or Recall list options. All patient names stored in the template will be printed in alphabetic order using the mailing address data from the Patient Registration file. Keep in mind that search templates must be updated periodically as new names are added to Dental Followup lists or other lists of patients. To use this option, users must specify the exact template name. Type **?** and press **Return** at the Select Template: prompt to see a list of existing templates.

4.2 How to Use Waiting List Options

The Dental Waiting List option enables users to place registered patients in a DDS file when they need and request further dental treatment, but an appointment cannot be scheduled.

Create various types of Waiting Lists as desired by using the EFOL option in the Dental Supervisors DEO menu. The patient’s mailing address can be edited, their priority for treatment set, the date added to the list, and the time interval for taking further followup action. Patients can be added to more than one list, and they can be removed, or their priority (action interval) changed when necessary. The provider who requests that the patient be added to the list must also be entered. The Waiting List Reports can be used to sort patients by date and type of treatment to schedule patients for appointments when needed. These patient lists can be searched to create groups of patients who can then be deleted, sent letters, or other actions can be taken as desired.

4.2.1 Setting Up Recall and Waiting Lists

Each category type of Recall or Waiting List (Table 4-1) must be set up using the EFOL menu option in the Dental Supervisor's Data Entry menu before patients can be added to the list. When creating a new followup type, the system will prompt for several pieces of information:

Table 4-1: Recall or Waiting List categories

Category	Description
TYPE	Enter the type of the list to create (either Waiting or Recall).
ACTION	This is the time interval (in days) with which the Action took place.
INTERVAL	Date will be computed. The Action Date is the date by which some sort of action should be taken for patients on the list. There are two action intervals, one for routine priority patients, and one for high or urgent priority patients. This interval determines the Recall date. The DDS will send a reminder mail (bulletin) to the dentist who placed the patient on the list when the action interval date is exceeded. The dentist can then schedule an appointment, remove the patient from the list, or charge the priority.
TEXT	This word processing field contains the text of letters to be sent to patients placed on this type of followup. The DDS comes pre-packaged with several generic followup types. Use the pre-packaged letters as a model when treating the dentist's own followup types. Before using the pre-packaged letters, the user should edit them to customize them to the particular facility.

4.2.2 Option: PFOL – Print Patient Followup Summary

This option prints a summary of the followup activity (Waiting or Recall) for an individual patient. The summary includes:

- Failed Dental Appointments: – Dates
- Active Dental Followup: – Lists that the patient is presently on.
- Actions Taken: – Types and dates of followup activity.
- Previous Followup: – Inactive followup activity including dates when patient was added and removed from lists.

The Followup Summary is also automatically included in the options for reviewing a patient's dental record (REVW and LAST), as well as in the Dental Health Summary component of the PCC (if it is running at the site).

4.2.3 Option: WADD – Add Patient to Waiting or Recall List

The options to add patients to Waiting and Recall lists work in the same manner. In addition to the options WADD and RCAD in the Patient Management (PM) Menu, the user may also add patients to the followup lists during Direct Dental Visit (DDV) data entry by using the **^W** or **^R** command (for Wait or Recall) at the prompt to Select ADA Code (or Action).

Using either method to add a patient to a Waiting or Recall list, the user is first prompted for a Followup List Type.

1. Enter a "?" to view a list of available types. New types can be added by the Dental Supervisor. After selecting a patient name, the user will be prompted for the following:
    - The patient's current mailing address that is in the Registration system. If the mailing address is left blank, the user will be unable to add the patient to the list.
    - The phone number (this may be left blank).
2. Select a priority category for the patient. The priority will determine the Action Interval as defined in the Followup List Type. Priority codes are:
    - U – Urgent
    - R – Routine
    - H – High
3. Enter the date added to this list (not always the day entered in computer).
4. Enter a recall date or accept the date displayed by the computer based upon the patient's priority and date added.
5. Finally, select the provider who requested this patient to be added.

4.2.4 Option: Delete Individual from Waiting or Recall List

Select this option to remove an individual from a followup list. The user will first be prompted for the Waiting List Type, and then for the name of the patient. Once the patient is removed from the list, the patient's Followup Record will automatically be updated to show that the patient was previously on the list and the date removed.

Groups of patients can be deleted from lists using the RCGR or WGRP options. When a patient’s dental record is reviewed using the REVW or LAST option, the previous followup history is displayed along with active followup information and other data.

4.2.5 Option: Print Letter for Individual Patient

Select this option to print a letter to an individual patient. The type of letter printed will be defined by the Dental Supervisor for that Followup List Type. The supervisor may modify the letter as necessary. If a patient is on more than one followup list, the system prompts to choose which type of letter should be printed.

4.2.6 Option: Print Waiting or Recall Lists Sorted By Date Added

This option prints all patients on the followup lists sorted by the date they were added. The report can be limited to only one List Type by specifying the appropriate range at the Start with Type: FIRST// prompt.

For example, to print only the ENDODONTIC list (Figure 4-1), start with EN and go to EO since the word ENDODONTIC collates alphabetically after EN and before EO, as shown below:

```
START WITH TYPE: FIRST// EN <Return>
GO TO TYPE: LAST// EO <Return>
```

Figure 4-1: Print Only ENDODONTIC List

To obtain a printout of ALL lists, accept the default FIRST. That is, press the **Return** key at the Start with Type: FIRST// prompt.

4.2.7 Print Waiting or Recall Lists Sorted by Action Date

This option prints patients on the followup lists sorted by their Action Date. The report can be restricted to a range of List Types (see Help Frame on printing followup lists sorted by date added). Additionally, the report can be restricted to patients whose Action Dates fall within a given range. For example, to print a report showing all patients on all Followup Lists whose action intervals have already elapsed (Figure 4-2), respond to the prompts like this:

```
START WITH TYPE: FIRST// <Return> (This selects All Types)
START WITH ACTION DATE: FIRST// 1-1-84 (Arbitrarily early date)
GO TO ACTION DATE: LAST// T (For Today)
```

Figure 4-2: Followup Lists whose action intervals have already elapsed

Note: The Action Interval is defined by the Dental Supervisor when he sets up the ListType. The Action Date is the date the patient was added to the list plus the ActionInterval. It is automatically calculated when the patient is added to the list.

4.2.8 Option: Followup File Search

The Search option for the Waiting List and Recall files allows searching the followup file based on criteria of the choice. Store the names of patients found in the search in a template, then print out lists or letters to the patients stored in that template using the WPRT and RPRT options. It is permitted to also delete entire groups from the Waiting and Recall lists based on templates created with the Search option. The Search option is very flexible so that it may be used in a variety of clinical settings. The price of that flexibility is that the Search option requires some study and forethought. Since the Search option uses FileMan's search utility, general details of interacting with the search prompts can be found in the *FileMan User's Guide.*

4.2.9 Option: Deleting Groups from Followup Using Search Templates

To use this option, first create a Search Template using the Search Followup Files option.

Note: Be very careful using this option. It can remove large numbers of patients from the followup file. Before deleting groups, it is best to print out a list and verify that the group should be deleted.

To delete a group, specify the template name in which the entries are stored. Ensure this is the correct template. Each patient whose entry is stored in the template will be removed from active followup. An entry will automatically be made in that patient's dental file showing what date it was removed.

4.2.10 Option: Printing Search Results

To use this option, the user must first have created a Search Template using the Search Followup File option. Once created, this option allows printing out each entry in the template in one of three formats. Print letters, a standard list, or a list that the user designs personally.

The dental supervisor may edit and customize the format of the letters using an option available in the Supervisor's Data Entry menu.

The Standard list is a pre-formatted printout that gives most of the information in the followup file.

The Customized list allows the use of FileMan formatting specifications to create the user's own list. If the output format is a list, the system will prompt for an ACTION TO BE TAKEN. Enter the action for which the list is planned. For example, if the user plans to use the list to telephone patients, enter PATIENT CALLED. This action will be printed out whenever the patient's followup summary is displayed. To skip this prompt, press **Return** without entering anything.

4.2.11 Option: Patients Removed from Followup Lists

This report works the same way for Waiting Lists and Recall Lists. It provides a list of patient names that have been removed from the various followup lists during the past calendar year (365 days).

The report displays the data for all types of followup lists that have been created by the local dental program. Thus, the user is not prompted to select from a range of followup list types. Only the output device to send the report to is prompted.

4.3 Deferred Services Register

This module of the DDS package enables a local program to maintain a Deferred Services Register based upon the guidelines established by the Contract Health Services (CHS) Branch of the IHS. Any registered patient can be entered into the registry, even if the patient has not had a dental visit at this clinic. Fifteen types of needs can be entered along with the number of units for each need.

The total cost estimate for each patient and for all types of patients is automatically computed based upon the CHS fee values edited by the Dental Supervisor. These fees represent an estimate of the cost to contract the needed care to private dentists.

Deferred needs and their estimated costs are also organized into the basic categories designated by the CHS Branch as:

- Preventive/Primary Care
- Secondary Care (Acute& Chronic)
- Tertiary Care (Acute and Chronic)

Note: Generally speaking, the options of this module are largely self-explanatory and can be easily used. Needs data for each patient can be entered from an HSA 42-1 or HSA 42-2 (put it on back) or any other form a local program wants to devise.

5.0 Patient Record Inquiry Options

This option may be one of the most frequently used in the DDS package. It contains suboptions to allow users to inquire into the patient records in the Registration database, the dental files, and the Patient Care Component (PCC) records.

Names can be scanned to determine if they are registered at the local site, or to obtain HRNs prior to dental appointments. A patient's dental record can also be listed (including narrative notes, if entered). Data from the registration file can be reviewed, but entries cannot be made in these records by dental personnel.

If PCC is operating locally, health summaries can be generated for individuals or groups. This is useful when health records are pulled prior to dental appointments or when a printed treatment summary is needed to accompany a patient who is referred to another facility for consultation or treatment. The content of Health Summaries can be tailored (built) to suit the needs of dental care providers.

5.1 Viewing a Summary of the Last Dental Visit

This option enables the receptionist or dentist to obtain a brief summary from a patient's dental record. The summary is useful when making appointments or prior to scheduled visits because it provides access to key data without having to pull the patient's chart from medical records. This summary currently includes:

- Failed dental appointment history.
- Active followup actions if the patient is listed on any Recall or Treatment Waiting lists.
- Previous followup activity if patient was previously on Recall or Waiting lists.
- List of dental services provided during the patient's most recent visit. This includes any narrative notes.

5.2 Reviewing a Patient's Dental Record

This option enables the DDS user to print out the details of a patient's dental record for each visit to the dental clinic. It begins with a summary of failed/broken appointments, the patient's followup status on Recall or Waiting lists, and the list of dental services (ADA Codes) reported for the patient at each dental visit, starting with the most recent visit. All brief or narrative dental notes are included.

The report automatically displays all dental visits over the past three years, up to 10 encounters. However, the period of time (in years) and the maximum number of visits this report displays can be changed by the Dental Supervisor if desired. The Edit Dental Site Parameters option can be used for this purpose. Like all other reports, the REVW output can be displayed on the video screen or directed to a printer.

Note: If the PCC Health Summary System is available, the data included in this REVW option will also be included in all Dental Health Summaries generated.

Appendix A Rules of Behavior

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

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

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

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

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

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

A.1 All RPMS Users

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

A.1.1 Access

RPMS users shall:

- Only use data for which you have been granted authorization.
- Only give information to personnel who have access authority and have a need to know.
- Always verify a caller’s identification and job purpose with your supervisor or the entity provided as employer before providing any type of information system access, sensitive information, or nonpublic agency information.

- Be aware that personal use of information resources is authorized on a limited basis within the provisions *Indian Health Manual* Part 8, "Information Resources Management," Chapter 6, "Limited Personal Use of Information Technology Resources."

RPMS users shall not:

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

A.1.2 Information Accessibility

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

RPMS users shall:

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

A.1.3 Accountability

RPMS users shall:

- Behave in an ethical, technically proficient, informed, and trustworthy manner.
- Log out of the system whenever they leave the vicinity of their personal computers (PCs).
- Be alert to threats and vulnerabilities in the security of the system.
- Report all security incidents to their local Information System Security Officer (ISSO).

- Differentiate tasks and functions to ensure that no one person has sole access to or control over important resources.
- Protect all sensitive data entrusted to them as part of their government employment.
- Abide by all Department and Agency policies and procedures and guidelines related to ethics, conduct, behavior, and information technology (IT) information processes.

A.1.4 Confidentiality

RPMS users shall:

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

RPMS users shall not:

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

A.1.5 Integrity

RPMS users shall:

- Protect their systems against viruses and similar malicious programs.
- Observe all software license agreements.
- Follow industry standard procedures for maintaining and managing RPMS hardware, operating system software, application software, and/or database software and database tables.
- Comply with all copyright regulations and license agreements associated with RPMS software.

RPMS users shall not:

- Violate federal copyright laws.
- Install or use unauthorized software within the system libraries or folders.

- Use freeware, shareware, or public domain software on/with the system without their manager's written permission and without scanning it for viruses first.

A.1.6 System Logon

RPMS users shall:

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

A.1.7 Passwords

RPMS users shall:

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

RPMS users shall not:

- Use common words found in any dictionary as a password.
- Use obvious readable passwords or passwords that incorporate personal data elements (e.g., user's name, date of birth, address, telephone number, or social security number; names of children or spouses; favorite band, sports team, or automobile; or other personal attributes).
- Share passwords/IDs with anyone or accept the use of another's password/ID, even if offered.
- Reuse passwords. A new password must contain no more than five characters per eight characters from the previous password.
- Post passwords.

- Keep a password list in an obvious place, such as under keyboards, in desk drawers, or in any other location where it might be disclosed.
- Give a password out over the phone.

A.1.8 Backups

RPMS users shall:

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

A.1.9 Reporting

RPMS users shall”

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

RPMS users shall not:

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

A.1.10 Session Timeouts

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

RPMS users shall:

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

A.1.11 Hardware

RPMS users shall:

- Avoid placing system equipment near obvious environmental hazards (e.g., water pipes).

- Keep an inventory of all system equipment.
- Keep records of maintenance/repairs performed on system equipment.

RPMS users shall not:

- Eat or drink near system equipment.

A.1.12 Awareness

RPMS users shall:

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

A.1.13 Remote Access

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

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

Remote RPMS users shall:

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

Remote RPMS users shall not:

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

A.2 RPMS Developers

RPMS developers shall:

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

RPMS developers shall not:

- Write any code that adversely impacts RPMS, such as backdoor access, Easter eggs, time bombs, or any other malicious code or make inappropriate comments within the code, manuals, or help frames.
- Grant any user or system administrator access to RPMS unless proper documentation is provided.
- Release any sensitive agency or patient information.

A.3 Privileged Users

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

Privileged RPMS users shall:

- Verify that any user requesting access to any RPMS system has completed the appropriate access request forms.
- Ensure that government personnel and contractor personnel understand and comply with license requirements. End users, supervisors, and functional managers are ultimately responsible for this compliance.
- Advise the system owner on matters concerning information technology security.
- Assist the system owner in developing security plans, risk assessments, and supporting documentation for the certification and accreditation process.
- Ensure that any changes to RPMS that affect contingency and disaster recovery plans are conveyed to the person responsible for maintaining continuity of operations plans.
- Ensure that adequate physical and administrative safeguards are operational within their areas of responsibility and that access to information and data is restricted to authorized personnel on a need-to-know basis.
- Verify that users have received appropriate security training before allowing access to RPMS.
- Implement applicable security access procedures and mechanisms, incorporate appropriate levels of system auditing, and review audit logs.
- Document and investigate known or suspected security incidents or violations and report them to the ISSO, Chief Information Security Officer (CISO), and systems owner.
- Protect the supervisor, superuser, or system administrator passwords.
- Avoid instances where the same individual has responsibility for several functions (i.e., transaction entry and transaction approval).
- Watch for unscheduled, unusual, and unauthorized programs.
- Help train system users on the appropriate use and security of the system.
- Establish protective controls to ensure the accountability, integrity, confidentiality, and availability of the system.
- Replace passwords when a compromise is suspected. Delete user accounts as quickly as possible from the time that the user is no longer authorized system. Passwords forgotten by their owner should be replaced, not reissued.
- Terminate user accounts when a user transfers or has been terminated. If the user has authority to grant authorizations to others, review these other authorizations. Retrieve any devices used to gain access to the system or equipment. Cancel logon IDs and passwords and delete or reassign related active and backup files.

- Use a suspend program to prevent an unauthorized user from logging on with the current user's ID if the system is left on and unattended.
- Verify the identity of the user when resetting passwords. This can be done either in person or having the user answer a question that can be compared to one in the administrator's database.
- Shall follow industry best standards for systems they are assigned to and abide by all Department and Agency policies and procedures.

Privileged RPMS users shall not:

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

Glossary

Archiving

The storage of historical or little-used data off-line.

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).

Queuing

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

Up-Hat (^)

A circumflex, also known as a hat or carat, is used as a delimiter in a global. The Up-Hat is denoted as ^ and is typed by pressing Shift+6 on the keyboard.

Acronym List

Acronym	Term Meaning
ADA	American Dental Association
ADE	RPMS Namespace for the DDS application
DDS	Dental Data System (namespace=”ADE”)
HRN	Health Record Number (of the patient)
IHS	Indian Health Service
OPSITE	Operative Site Location (tooth number, sextant, etc) from the Dental Operative Site file
PCC	Patient Care Component (RPMS application)
PM	Patient Management
PSG	Professional Services Group
SSN	Social Security Number
ROB	Rules of Behavior
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