RESOURCE AND PATIENT MANAGEMENT SYSTEM

# Patient Information Management System (PIMS)

## Sensitive Patient Tracking (BDG)

## User Manual

Version 5.3 Patch 1009
March 2009

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 Sensitive Patient Tracking module that is part of Patient Information and Management System (PIMS) package version 5.3. Included in this manual is the information providing instructional guidance to a broad range of users within IHS medical facilities in daily use of the Sensitive Patient Tracking Module of the PIMS software.

# Table of Contents

# 1.0 Introduction

The PIMS user manual is divided into three modules: ADT, Scheduling, and Sensitive Patient Tracking. Sensitive Patient Tracking and ADT share the BDG namespace. The PIMS Sensitive Patient Tracking user manual provides instructional guidance to a broad range of users within IHS medical facilities in daily use of the Sensitive Patient Tracking Module of the PIMS software.

Sensitive Patient Tracking contains the security options for assigning, displaying, and purging information related to sensitive patient records. Only holders of the DG SECURITY OFFICER key have access to this menu.

| | |
|---|---|
| **Note:** | MAS is an acronym for Medical Administration Service. This service, where it still exists, is now generally referred to as Health Administration Service. Several file names, option names, and reports in the PIMS software contain the initials MAS. These will be retained to avoid confusion and ensure continuity. |

As part of the effort to ensure patient privacy, additional security measures have been added to the patient access function. Any patient flagged as Sensitive will have access to his/her record tracked. In addition, warning messages will be displayed when staff (not holding special keys) accesses these records. If the person chooses to continue accessing the record, a bulletin is sent to a designated mail group.

The long warning message is removed when accessing inpatients since those records must be accessed many times a day. A site can also restrict staff members from accessing their own patient record.

The only menu associated with this module is the Security Officer Menu that must be placed on the proper person(s) main menu. This menu allows the designated security officer to flag records as sensitive, view who accessed the records, and purge entries in the log when appropriate.

All other staff will only see the effects of these measures if or when they access a sensitive record.

# 2.0 Display User Access to Patient Record (DUA)

This option permits holders of the DG Security Officer key to display a select user's access, or all users who accessed a particular patient record for a specified date range. You can then restrict the report to a specific user or list all users who accessed the record. If you choose to display the report to your computer screen, ListMan is used so you can scroll back and forth through the listing. Information provided on the report includes: report run date, patient name, social security number and date of birth, user(s) name, date record accessed, option used to access record, and whether or not the patient was an inpatient at the time the record was accessed.

1. To access the DUA options, type DUA at the "Select Sensitive Patient Tracking Option:" prompt.

```
                  ****************************************
                  *        INDIAN HEALTH SERVICE         *
                  *   SENSITIVE PATIENT TRACKING MODULE  *
                  *             VERSION 5.3              *
                  ****************************************

                              UNSPECIFIED HO


   DUA    Display User Access to Patient Record
   EPL    Enter/Edit Patient Security Level
   LSP    List Sensitive Patients
   PLOG   Purge Record of User Access from Security Log
   PPAT   Purge Non-sensitive Patients from Security Log
   USP    Update Security Parameters
   XSO    Sensitive Patient Tutorial

Select Sensitive Patient Tracking Option: DUA  Display User Access to Patient Record
```

Figure 2-1: Displaying user access (Step 1)

2. Type the patient's name at the "Select Patient Name:" prompt.

3. Type the start of the date range you want to be included at the "Beginning Date:" prompt.

4. Type the ending date of the date range you want to be included at the "Ending Date:" prompt.

```
     For holders of the DG SECURITY OFFICER key, use this option
     to display who accessed a particular patient record over
     a given date range.  You can view just one user's access or
     that of all users who accessed the record.

Select PATIENT NAME: PATIENT,ALLEN       M 12-14-1901 000141808    MH 2903

**** Date Range Selection ****

   Beginning DATE : T-365  (DEC 26, 2001)

   Ending    DATE : T  (DEC 26, 2002)
```

Figure 2-2: Displaying user access (Steps 2–4)

5. At the "Do you want to see when a select user accessed this record?" prompt:

   a. Type Y if you want to see if/when a specific user accessed the patient's file. Then type the user's name at the "Select New Person Name:" prompt. The

   b. Type N if you do not want to see if/when a specific user accessed the patient's file.

6. Type a device name or press the Enter key to accept the default device at the "Device:" prompt.

```
Do you want to see when a select user accessed this record? No// [ENT]  (No)

DEVICE: HOME// [ENT]
```

Figure 2-3: Displaying user access (Steps 5-6)

7. The Access to Patient Record report will print (Figure 2-4). If you selected to display the report onscreen, use the options at the bottom of the screen to navigate through the report.

```
ACCESS TO PATIENT RECORD    Dec 26, 2002 13:57:45          Page:    1 of    1
Sensitive Patient Access for DEC 26,2001 to DEC 26,2002
Patient Name: PATIENT,ALLEN      #2903   Date of Birth : Dec 14, 1901

 USER                    DATE ACCESSED         OPTION/PROTOCOL USED  INPATIENT

 Adams, Adam A        DEC 03, 2002@10:01     Patient Inquiry         YES









          Enter ?? for more actions

Select Action:Quit//
```

Figure 2-4: Displaying user access (Step 7)

# 3.0 Enter/Edit Access Restrictions (EAR)

**ADDED WITH PIMS PATCH 1008**

Use this option to restrict access to specific patient records by specific users. You will be asked to select a user. Once the list template screen appears, it will display all patient restrictions for the user, if any. You may add new restricted records, lift restrictions already set, and resume restrictions that have been lifted.

The user will now see this message when trying to access that patient's record:

```
Select Patient: PATIENT,ONE              F 06-08-1990 XXX-XX-0645 THC 105242

        Sorry, you are restricted from accessing this patient's record.
           If you have questions, please contact your HIM department.
```

Figure 3-1: Displaying restricted patient message

**Note**: You may NOT select yourself for restriction.

1. To access the EAR option, type EAR at the "Select Sensitive Patient Tracking Options:" prompt.

```
                  ****************************************
                  *        INDIAN HEALTH SERVICE         *
                  *   SENSITIVE PATIENT TRACKING MODULE  *
                  *             VERSION 5.3              *
                  ****************************************

                                UNSPECIFIED HO


   DUA    Display User Access to Patient Record
   EAR    Enter/Edit Access Restrictions
   EPL    Enter/Edit Patient Security Level
   LSP    List Sensitive Patients
   PLOG   Purge Record of User Access from Security Log
   PPAT   Purge Non-sensitive Patients from Security Log
   USP    Update Security Parameters
   XSO    Sensitive Patient Tutorial

Select Sensitive Patient Tracking Option: EAR  Enter/Edit Access Restrictions

     Use this option to restrict a user from accessing specific
     patient records.  Restrictions can be lifted, either for a
     specific period of time or permanently.  This option is to
     to be used when a patient requests that particular staff or
     providers are not to view his/her record at all.


Select USER:
```

Figure 3-2: Sensitive Patient Tracking Module menu

2. At the Select User prompt, type in the user's name whose ability to access particular patient records you want to update.

```
User's Access Restrictions    Sep 20, 2007 11:05:24       Page:    1 of    1
User:       USER,TWO       BUSINESS OFFICE
            Last Signed on JUN 27, 2002@11:30:45
      Patient Name              Chart #   Restriction Status_______________
              NO RESTRICTED RECORDS FOUND




          Enter ?? for more actions
1  Add Restricted Record               3  Lift Restriction
2  View Restricted Record              4  Resume Restriction
Select Action: Quit//
```

Figure 3-3: Changing user restrictions

3. To add a new restricted patient record for this user, select Action #1

```
Select Action: Quit// 1   Add Restricted Record
Select RESTRICTED RECORD PATIENT NAME: Patient,One
```

Figure 3-4: Providing access to a patient

The patient will be automatically added to the list as shown below:

```
User's Access Restrictions    Sep 20, 2007 11:05:24       Page:    1 of    1
User:       USER,TWO       BUSINESS OFFICE
            Last Signed on JUN 27, 2002@11:30:45
      Patient Name              Chart #   Restriction Status_______________
  1   PATIENT,ONE               105177    RESTRICTED ACCESS




          Enter ?? for more actions
1  Add Restricted Record               3  Lift Restriction
2  View Restricted Record              4  Resume Restriction
Select Action: Quit//
```

Figure 3-5: Updating the patient list

4. To later remove this restriction, select action #3. Select the patient record from the list and enter the effective date when the user can access this patient again.

```
Select Action: Quit// 3   Lift Restriction
Select Restricted Record:  (1-3): 1
   DATE RESTRICTION LIFTED EFFECTIVE DATE:  TODAY
```

Figure 3-6: Removing a restriction

This display now looks like Figure 3-7.

```
User's Access Restrictions    Sep 20, 2007 11:05:24       Page:    1 of    1
User:       USER,TWO       BUSINESS OFFICE
            Last Signed on JUN 27, 2002@11:30:45
      Patient Name              Chart #   Restriction Status_________________
  1   PATIENT,ONE               105177    ACCESS REINSTATED on SEP 20, 2007



          Enter ?? for more actions
1  Add Restricted Record               3  Lift Restriction
2  View Restricted Record              4  Resume Restriction
Select Action: Quit//
```

Figure 3-7: Updated patient list

5. If a lifted restriction must be reinstated, select Action #4 – Resume Restriction and enter the Date Restriction Resumes. The display will go back to showing Restriction Status as "ACCESS RESTRCITED" or "TEMPORARY ACCESS until <date>".

6. To view all actions taken on a patient record/user record pair, select Action #2 – View Restricted Record.

```
View Restriction Details      Sep 20, 2007 11:29:48       Page:    1 of    1
User:       USER,TWO       BUSINESS OFFICE
            Last Signed on SEP 20, 2007@11:26:12

Patient:    PATIENT,ONE  (ACCESS REINSTATED on SEP 20, 2007)

 First Restricted       Restriction Lifted   - Resumed            Added By__
 AUG 31, 2007@08:52:27                                           USER,HIM
                        SEP 07,2007                              USER,HIM
                                                SEP 08, 2007     USER,HIM
                        SEP 20, 2007                             USER,HIM




          Enter ?? for more actions

Select Action: Quit//
```

Figure 3-8: Displaying all actions on a patient record

# 4.0 Enter/Edit Patient Security Level (EPL)

This option allows holders of the DG Sensitivity key to assign .remove a security level to a patient. A patient can be either sensitive or non-sensitive. You will be prompted for a patient's name. Once selected, you enter the security level. When first adding a patient, the security level will be automatically set as sensitive. You can then later to remove the patient from the list by simply editing the security level to non-sensitive. The patient will stay in the security log but future access will no longer be tracked. Use of this option enters the patient into the DG Security Log file. Any access of a sensitive patient record is tracked in this file.

> **Note**: If the security level for a patient is changed from sensitive to non-sensitive, then a bulletin will be sent notifying the Station Security Officer of the change.

1. To access the EPL option, type EPL at the "Select Sensitive Patient Tracking Options:" prompt.

```
                  ****************************************
                  *        INDIAN HEALTH SERVICE         *
                  *   SENSITIVE PATIENT TRACKING MODULE  *
                  *             VERSION 5.3              *
                  ****************************************

                              UNSPECIFIED HO


   DUA    Display User Access to Patient Record
   EPL    Enter/Edit Patient Security Level
   LSP    List Sensitive Patients
   PLOG   Purge Record of User Access from Security Log
   PPAT   Purge Non-sensitive Patients from Security Log
   USP    Update Security Parameters
   XSO    Sensitive Patient Tutorial

Select Sensitive Patient Tracking Option: EPL  Enter/Edit Patient Security Level
```

Figure 4-1: Entering/Editing a patient security level (Step 1)

2. Type the patient's name at the "Select Patient Name:" prompt.
3. Type Y at the "OK?" prompt to continue with the selected patient.
4. Type 0 (Non-Sensitive) or 1 (Sensitive) at the "Security Level:" prompt to either edit or enter the desired security level.
5. Type the name of the remote source that assigned the patient's security level at the "Security Source:" prompt.

```
     For holders of the DG SENSITIVITY key, use this option to
     assign a security level to a patient. A patient can be
     either Sensitive (access tracked) or Non-Sensitive (access
     no longer tracked unless all patients tracked at facility).
     If the security level for a patient changes from sensitive
     to non-sensitive, a bulletin is sent to your site's mail
     group listed as "Sensitivity Removed Group" under the
     security parameters.


Select PATIENT NAME: PATIENT,ALLEN
COMANCHE,ALLEN STAFFORD               M 12-14-1901 000141808    MH 2903
         ...OK? Yes// [ENT]
SECURITY LEVEL: NON-SENSITIVE// ??
        This field contains a 1 if the patient record is presently listed as
        sensitive or a 0 if the patient's record is not currently sensitive.

     Choose from:
       0        NON-SENSITIVE
       1        SENSITIVE
SECURITY LEVEL: NON-SENSITIVE// 1  SENSITIVE
SECURITY SOURCE: Adams, Adam
```

Figure 4-2: Entering/Editing a patient security level (Steps 2–5)

# 5.0 List Sensitive Patients (LSP)

This option lists all patients (sensitive and non-sensitive) in the DG Security Log file. You will then able to edit a status or display who accessed a given patient's record. One of the actions you can take is to display who accessed a particular patient. That action uses the same report described in the DUA option.

The data items included in the report are user name, date/time accessed, menu option or protocol used and whether or not the patient was an inpatient at the time.

The sensitive patients are listed first, in alphabetical order, followed by any non-sensitive patients still in the file. One of the actions available from this list is Edit Security Level where you can change the security level of any patient on the listing. To add new patients, you must use the EPL option.

1. To access the LSP option, type LSP at the "Select Sensitive Patient Tracking Option:" prompt.

2. Press the Enter key at the "Press Enter to Continue:" prompt.

```
                  ****************************************
                  *        INDIAN HEALTH SERVICE         *
                  *   SENSITIVE PATIENT TRACKING MODULE  *
                  *             VERSION 5.3              *
                  ****************************************

                              UNSPECIFIED HO


   DUA    Display User Access to Patient Record
   EPL    Enter/Edit Patient Security Level
   LSP    List Sensitive Patients
   PLOG   Purge Record of User Access from Security Log
   PPAT   Purge Non-sensitive Patients from Security Log
   USP    Update Security Parameters
   XSO    Sensitive Patient Tutorial

Select Sensitive Patient Tracking Option: LSP  List Sensitive Patients


     Use this option to list all patients marked as sensitive
     in the DG SECURITY LOG file.  You can then change their
     security level or display who accessed each record.  You
     cannot add new patients to the list here. Instead use the
     Enter/Edit option.

Press ENTER to continue:  [ENT]
```

Figure 5-1: Listing sensitive patients (Steps 1–2)

3. All patients who are marked as sensitive will be displayed (Figure 5-2).

```
SENSITIVE FILE LISTING      Dec 26, 2002 14:02:21          Page:    1 of  1
          Patients stored in DG SECURITY LOG file as of Dec 26, 2002

     Patients               Date Last Updated     Assigned By
  1. PATIENT,BERNARD         Dec 04, 2002@14:03    WAP
  2. PATIENT,ALLEN           Dec 26, 2002@14:02    JT









          Enter ?? for more actions
1  Edit Security Level    2  Who Accessed Record    Q  Quit
Select Action: Next Screen//       .
```

Figure 5-2: Listing sensitive patients (Step 3)

## 5.1 Edit Security Level

This option allows you to edit the security level for a particular patient.

1. To edit a patient's security level, type 1 at the "Select Action:" prompt.

2. Type the number of the patient whose security level you want to change at the "Select Patient:" prompt.

3. The patient's current security level will be displayed, type 0 (Non-Sensitive) or 1 (Sensitive) at the "Security Level:" prompt to either edit or enter the desired security level. Press the Enter key to keep the current default level.

4. Type the name of the remote source that assigned the patient's security level at the "Security Source:" prompt. Press the Enter key to keep the current default source.

```
SENSITIVE FILE LISTING      Dec 26, 2002 14:02:21        Page:    1 of    1
          Patients stored in DG SECURITY LOG file as of Dec 26, 2002

     Patients               Date Last Updated     Assigned By
  1. PATIENT,BERNARD         Dec 04, 2002@14:03    WAP
  2. PATIENT,ALLEN           Dec 26, 2002@14:02    JT









          Enter ?? for more actions
1  Edit Security Level    2  Who Accessed Record    Q  Quit
Select Action: Next Screen// 1   Edit Security Level
Select Patient:  (1-2): 1
SECURITY LEVEL: SENSITIVE// [ENT]
SECURITY SOURCE: Adams, Adam// [ENT]
```

Figure 5-3: Editing security level

## 5.2 Who Accessed Record

This option allows you to display a list of people who have accessed a particular patient's record.

1. To view a list of who accessed a particular patient's record, type 2 at the "Select Action:" prompt.
2. Type the number of the patient whose security access record you want displayed at the "Select Patient:" prompt.
3. Type the start of the date range you want to be included at the "Beginning Date:" prompt.
4. Type the ending date of the date range you want to be included at the "Ending Date:" prompt.
5. At the "Do you want to see when a select user accessed this record?" prompt:
   a. Type Y if you want to see if/when a specific user accessed the patient's file. Then type the user's name at the "Select New Person Name:" prompt.
   b. Type N if you do not want to see if/when a specific user accessed the patient's file.
6. Type a device name or press the Enter key to accept the default device at the "Device:" prompt.

```
SENSITIVE FILE LISTING        Dec 27, 2002 11:53:44        Page:    1 of    1
          Patients stored in DG SECURITY LOG file as of Dec 27, 2002

     Patients               Date Last Updated     Assigned By
  1. PATIENT,BERNARD         Dec 27, 2002@11:53    JT
  2. PATIENT,ALLEN           Dec 27, 2002@11:43    JT









          Enter ?? for more actions
1  Edit Security Level    2  Who Accessed Record    Q  Quit
Select Action: Next Screen// 2   Who Accessed Record
Select Patient:  (1-2): 1

**** Date Range Selection ****

   Beginning DATE : T-365  (DEC 27, 2001)

   Ending    DATE : T  (DEC 27, 2002)


Do you want to see when a select user accessed this record? No//   (No)


DEVICE: HOME// [RET]
```

Figure 5-4: Listing who accessed a record (Steps 1–6)

7. The Access to Patient Record screen will be displayed (Figure 5-5). Use the options at the bottom of the screen to navigate through the report.

```
ACCESS TO PATIENT RECORD      Dec 27, 2002 11:54:18       Page:    1 of    2
Sensitive Patient Access for DEC 27,2001 to DEC 27,2002
Patient Name: ABEITA,BERNARD            #7250   Date of Birth : Oct 27, 1978

 USER                    DATE ACCESSED          OPTION/PROTOCOL USED  INPATIENT

 BEATTY,P                DEC 04, 2002@10:53     EDIT a patient's fil    YES
 PIMS,USER               DEC 04, 2002@14:33     Admission Forms         NO
 PIMS,USER               DEC 04, 2002@14:27     Incomplete Charts Ed    NO
 PIMS,USER               DEC 04, 2002@14:24     Incomplete Charts Ed    NO
 PIMS,USER               DEC 04, 2002@14:23     Inpatient Chart Codi    NO
 PIMS,USER               DEC 04, 2002@14:19     Provider Change         NO
 PIMS,USER               DEC 04, 2002@12:27:10  Extended Inpatient I    NO
 PIMS,USER               DEC 04, 2002@12:27     Extended Bed Control    NO
 PIMS,USER               DEC 04, 2002@12:25     Discharge a Patient     YES
 PATIENT,DEMO            DEC 03, 2002@16:03     Incomplete Charts Ed    YES
 PATIENT,DEMO            DEC 03, 2002@12:39     Patient Inquiry         YES
 PATIENT,DEMO            DEC 03, 2002@11:29     Patient Inquiry         YES
 PATIENT,DEMO            DEC 03, 2002@11:27     Patient Inquiry         YES
 USER,GUY                DEC 03, 2002@10:35:10  Patient Inquiry         YES
+         Enter ?? for more actions

Select Action:Next Screen//
```

Figure 5-5: Listing who accessed a record (Step 7)

# 6.0 Purge Record of User Access from Security Log (PLOG)

This option permits holders of the DG Security Officer key to purge the access log for a select patient, or all patients during a specified date range. However, any access made to a sensitive patient record must be kept in the log at least 30 days. The number of days to keep access can be between 30 and 365 and is specified in the MAS Parameters file, Days to Maintain Sensitivity field. The user may choose to print the names of the users that are purged or run the option as a background job. If the names are printed, a message will be displayed when the purge is completed which includes the total number of records deleted. Only holders of security key DG Security Officer may access this option.

1. To purge the record of user access from the security log, type PLOG at the "Select Sensitive Patient Tracking Options:" prompt.

```
                  ****************************************
                  *         INDIAN HEALTH SERVICE        *
                  *   SENSITIVE PATIENT TRACKING MODULE  *
                  *              VERSION 5.3             *
                  ****************************************

                              UNSPECIFIED HO



   DUA    Display User Access to Patient Record
   EPL    Enter/Edit Patient Security Level
   LSP    List Sensitive Patients
   PLOG   Purge Record of User Access from Security Log
   PPAT   Purge Non-sensitive Patients from Security Log
   USP    Update Security Parameters
   XSO    Sensitive Patient Tutorial

Select Sensitive Patient Tracking Option: PLOG  Purge Record of User Access from
Security Log
```

Figure 6-1: Purging the record (Step 1)

2. Type the name of the single patient whose file you want to purge or type All to purge all records at the "Select Patient:" prompt.

3. Type the start of the date range you want to be included at the "Beginning Date:" prompt.

> **Note**: You cannot purge files that are 30 or fewer days old. Select dates that are more than 30 days in the past.

4. Type the ending date of the date range you want to be included at the "Ending Date:" prompt.

5. Type Y to print a paper copy of the access log before purging or N to not print a paper copy at the “Do you want to print users as they are purged?” If you type Y, you will then be prompted to select a print device.

6. Type the time and date for which you would like to begin the purge or press the Enter key to accept the default time of now at the “Requested Start Time:” prompt.

7. The message Request Queued! will be displayed.

8. Press the Enter key at the “Press Enter to continue:” prompt.

```
     Use this option to purge the access log for a select
     patient or for all patients within a date range.  Any
     access made to a sensitive record must be kept at least
     30 days.



   Enter 'ALL' or a select patient to purge user access from security log.

Select PATIENT: PATIENT,ALLEN               M 12-14-1901 000141808 MH 2903

Record of user access can not be purged prior to 30 day(s), please select a day on
or before NOV 25, 2002.

**** Date Range Selection ****

   Beginning DATE : T-365  (DEC 26, 2001)

   Ending    DATE : T-35  (NOV 21, 2002)

Do you want to print users as they are purged? No (No)

Requested Start Time: NOW// [ENT] (DEC 27, 2002@12:36:24)

Request Queued!
Press ENTER to continue: [ENT]
```

Figure 6-2: Purging the record (Steps 2–8)

# 7.0 Purge Non-sensitive Patients from Security Log (PPAT)

This option is used to purge patients with a non-sensitive security level from the security log. You choose to print the names of the patients that are purged or run the option as a background job. If the names are printed, a message will be displayed when the purge is completed which includes the total number of records deleted. Only holders of security key DG SECURITY OFFICER may access this option.

> **Warning**: Be very careful, as this will delete all record of users accessing this patient, even while the patient was designated as sensitive. You are not given the choice to just remove specific patients.

1. To purge non-sensitive patients from the security log, type PPAT at the "Select Sensitive Patient Tracking Option:" prompt.

2. Type Y to continue or N to go back at the "Are You Sure You Want to Purge All Non-Sensitive Patients?" prompt. If you typed N, press the Enter key at the "Press Enter to Continue:" prompt.

3. Type Yes or No at the "Do You Want to Print Patients as they are purged?" prompt. If you type yes, you will be prompted to type the name of a print device.

```
                                UNSPECIFIED HO

   DUA    Display User Access to Patient Record
   EPL    Enter/Edit Patient Security Level
   LSP    List Sensitive Patients
   PLOG   Purge Record of User Access from Security Log
   PPAT   Purge Non-sensitive Patients from Security Log
   USP    Update Security Parameters
   XSO    Sensitive Patient Tutorial

Select Sensitive Patient Tracking Option: PPAT  Purge Non-sensitive Patients from
Security Log


     Use this option to purge patients from the DG SECURITY LOG
     file if the patient's security level is non-sensitive.

Are you sure you want to purge all non-sensitive patients? No// Y
 (Enter 'YES' to purge non-sensitive patients, or 'NO' to exit this process.)

Do you want to print patients as they are purged? No// Y  (Yes)

DEVICE: HOME//
```

Figure 7-1: Purging non-sensitive patients

# 8.0 Update Security Parameters (USP)

Use this option to updated the security parameters for your facility.

1. To update security parameters, type USP at the "Select Sensitive Patient Tracking Option:" prompt.

```
                 ****************************************
                  *        INDIAN HEALTH SERVICE         *
                  *   SENSITIVE PATIENT TRACKING MODULE  *
                  *            VERSION 5.3               *
                  ****************************************

                              UNSPECIFIED HO



   DUA    Display User Access to Patient Record
   EPL    Enter/Edit Patient Security Level
   LSP    List Sensitive Patients
   PLOG   Purge Record of User Access from Security Log
   PPAT   Purge Non-sensitive Patients from Security Log
   USP    Update Security Parameters
   XSO    Sensitive Patient Tutorial

Select Sensitive Patient Tracking Option: usp  Update Security Parameters
```

Figure 8-1: Updating security parameters (Step 1)

2. Three options will be displayed (Figure 8-2). Sections 8.1 through 8.3 will explain how to use each option.

```
     Use this option to update such parameters as "Days to
     Maintain Sensitivity" and "Restrict Patient Record
     Access".  You can assign mail groups to bulletins and
     add members to the mail groups.  A listing of all users
     with access to this menu and sensitive records is available.


          1. Edit Security Parameters
          2. Edit Mail Group Members
          3. List Security Key Holders

  Select Action:  (1-3):
```

Figure 8-2: Updating security parameters (Step 2)

## 8.1 Edit Security Parameters

Use this option to edit the existing security parameters for your facility.

1. To edit security parameters, type 1 at the "Select Action:" prompt.

2. The Update Security Parameters screen will be displayed (Figure 8-3). This screen uses ScreenMan.

3. Type YES to track access to all patients all the time at the "Track all Patient Access?:" prompt.

| | |
|---|---|
| **Warning:** | This can put quite a load on your system and storage capabilities. It will automatically add patients as non-sensitive to the DG Security Log file the first time their record is accessed. |

4. Type a number between 30 and 365 days at the "Days to Maintain Sensitivity Log:" prompt. This parameter determines the number of days in the past you want to keep information on who accessed patient information. The parameter is used by the Purge Record of User Access from Security Log option.

5. Type YES or NO at the "Restrict Access to User's Own Record:" prompt. Do you want to restrict users from accessing their own records? If you answer YES, only users holding the DG Record Access key can access their own patient record. If turned on, this parameter requires that all users accessing patient records have their correct social security number (SSN) defined in the New Person file. The SSN is used to find that user's patient record in file 2.

6. Type the mail group to be notified when sensitive records are accessed by users not holding the DG Sensitivity key "Sensitive Record Accessed Group:" prompt. This must be a mail group already defined. You can add new mail groups under Action 2 – Edit Mail Group Members detailed below.

7. Type the mail group to be notified when a patient's security level is changed from sensitive to non-sensitive "Sensitivity Removed Group:" prompt. This must be already defined in the Mail Group file.

```
UPDATE SECURITY PARAMETERS
 -------------------------
   TRACK ALL PATIENT ACCESS?: YES
     (Track user access to ALL patients all the time?)

   DAYS TO MAINTAIN SENSITIVITY LOG: 30
    (Choose between 30 and 365 days)

   RESTRICT ACCESS TO USER'S OWN RECORD: YES
    (Allow users to access their own records?)

   SENSITIVE RECORD ACCESSED GROUP: DG SECURITY
    (Mail group to notify when sensitive record accessed)

   SENSITIVITY REMOVED GROUP:
    (Mail group to notify when patient removed from sensitive list)

_____________________________________________________________________________




COMMAND:                                    Press <PF1>H for help    Insert
```

Figure 8-3: Editing security parameters

## 8.2 Edit Mail Group Members

Use this option to either add or edit Mail Groups. The add function automatically sets the mail group type to public, self-enrollment to No and restrictions to Unrestricted. If you want these changed, you must access the Mail Group Edit on the site manager menu.

You will also need to add members to the DG Missing New Person SSN mail group. This mail group receives bulletins when users don't have their SSN defined in the New Person file. The bulletin is only sent if the Restrict Access to User's Own Record parameter is turned on, the user does not hold the DG Record Access key, and there is no SSN in file 200 for that user. These users cannot access any patient record because the software cannot determine if the user is accessing his/her record. Until at least one member is added to this mail group, you will be reminded to add members when you select this action.

1. To edit mail group members, type 2 at the "Select Action:" prompt.

2. Type the name of an existing mail group or type the name of a new mail group at the "Select Mail Group Name:" prompt. If you choose to add a new group, you will be prompted to confirm that you are adding a new group by typing Y at the "Are you adding 'X' as a new MAIL GROUP?" prompt.

```
     Use this option to update such parameters as "Days to
     Maintain Sensitivity" and "Restrict Patient Record
     Access".  You can assign mail groups to bulletins and
     add members to the mail groups.  A listing of all users
     with access to this menu and sensitive records is available.


          1. Edit Security Parameters
          2. Edit Mail Group Members
          3. List Security Key Holders

  Select Action:  (1-3): 2

Don't forget to add members to DG MISSING NEW PERSON SSN mail group


Select MAIL GROUP NAME: New Group
Are you adding 'NEW Group' as a new MAIL GROUP? Y (Yes)
```

Figure 8-4: Editing mail groups (Steps 1–2)

3. The Edit Security Mail Groups screen will be displayed (Figure 8-5). This screen uses ScreenMan.

4. Fill in or edit the prompts on your screen to edit or add the selected Mail Group.

```
EDIT SECURITY MAIL GROUPS
-------------------------

       NAME: New Group
COORDINATOR:
DESCRIPTION:

MAIL GROUP MEMBERS
----------------------------------









_______________________________________________________________________________



COMMAND:                                    Press <PF1>H for help    Insert
```

Figure 8-5: Editing mail groups (Steps 3–4)

## 8.3 List Security Key Holders

This option lists everyone who holds security keys used by this module. This option is provided to help you keep track of who has which level of access.

1. To list security key holders, type 3 at the “Select Action:” prompt.

```
     Use this option to update such parameters as "Days to
     Maintain Sensitivity" and "Restrict Patient Record
     Access".  You can assign mail groups to bulletins and
     add members to the mail groups.  A listing of all users
     with access to this menu and sensitive records is available.


          1. Edit Security Parameters
          2. Edit Mail Group Members
          3. List Security Key Holders

  Select Action:  (1-3): 3
```

Figure 8-6: Listing security key holders (Step 1)

2. The Sensitive Patient Keys screen will be displayed (Figure 8-7). Use the options at the bottom of the screen to navigate through the report.

```
Sensitive Patient Keys        Dec 27, 2002 13:21:47        Page:    1 of    5
          Listing of Users with keys important to this module

     User Name                      Service/Section
DG SECURITY OFFICER      (Full access to this module)
     USER,CHARLES                  BUSINESS OFFICE
     USER,MD                         ADMINISTRATION
     USER,WALTER A                   ADMINISTRATION
     USER,P                          CLINIC
     USER,DEMO                       ADMINISTRATION
     USER,USER                       ADMINISTRATION
     USER, DEMO                      BUSINESS OFFICE
     USER, DEMO                      BUSINESS OFFICE
     USER, DEMO                      CLINIC
     USER, DEMO                      ADMINISTRATION
     USER, DEMO                      ADMINISTRATION
     USER, DEMO A                    ADMINISTRATION
     USER, DEMO                      ADMINISTRATION
     USER, DEMO                      ADMINISTRATION
     USER,ANGELA                     ADMINISTRATION
+         Enter ?? for more actions

Select Action:Next Screen//
```

Figure 8-7: Listing security key holders (Step 2)

# 9.0 Sensitive Patient Tutorial (XSO)

This option provides you with a detailed help menu for options in the Sensitive Patient Tracking module. You will be given the option to either display the help onscreen or print the information to paper.

1. To use the sensitive patient tutorial, type XSO at the "Select Sensitive Patient Tracking Option:" prompt.

```
                  ****************************************
                  *         INDIAN HEALTH SERVICE        *
                  *    SENSITIVE PATIENT TRACKING MODULE  *
                  *              VERSION 5.3               *
                  ****************************************

                              UNSPECIFIED HO



   DUA    Display User Access to Patient Record
   EPL    Enter/Edit Patient Security Level
   LSP    List Sensitive Patients
   PLOG   Purge Record of User Access from Security Log
   PPAT   Purge Non-sensitive Patients from Security Log
   USP    Update Security Parameters
   XSO    Sensitive Patient Tutorial

Select Sensitive Patient Tracking Option: XSO  Sensitive Patient Tutorial
```

Figure 9-1: Using sensitive patient tutorial (Step 1)

2. Type either 1 (Display help on your screen) or 2 (Print help to your printer) at the "Choose One:" prompt. If you typed 2, you will be prompted to type a print device. If you typed 1, continue with Steps 3 through 5.

```
                    PIMS ON-LINE HELP UTILITY


   How do you want me to present this help?

     1.  DISPLAY help to your screen
     2.  PRINT help to your printer (10 pages)

   Choose One:  (1-2): 1
```

Figure 9-2: Using sensitive patient tracking tutorial (Step 2)

3. The Sensitive Patient Tracking system on-line tutorial screen will be displayed (Figure 9-3).

4. Type the number of the option that you would like more information about at the "Select Help System Action or <Return>:" prompt. If you want to exit this screen press the Enter key.

```
                    SENSITIVE PATIENT TRACKING SYSTEM

 *** Welcome to the SENSITIVE PATIENT TRACKING System On-line Tutorial ***


        1. Introduction

        2. Implementation

        3. Maintaining Security Log

        4. Viewing Accessed Records

        5. Purging Log and Records

        6. Release Notes



  Press ENTER to exit or select a number to view that Section.

Select HELP SYSTEM action or <return>: 2
```

Figure 9-3: Using sensitive patient tracking tutorial (Steps 3–4)

5. Press the Enter key at the "Select Help System Action or <Return>:" prompt to exit the help option you selected.

```
                  Implementing Sensitive Patient Tracking

Upon installation, none of the new functionality of this module goes into
effect until turned on.  Here are the recommended Steps to implement these
new security measures:

1. Give the DG SECURITY OFFICER and DG SENSITIVITY keys to those
   individuals designated to maintain the system.

2. Place the BDG SECURITY MENU on the appropriate main menu for those
   given the aforementioned keys.

3. Use the Update Security Parameters option to customize this
   application for your facility.

4. Allocate the DG SENSITIVITY key to those staff members who do not need
   to see the warning message when accessing sensitive charts.  Try to
   keep the number of people holding this key down to a reasonable number.

5. If you restricted access to staff members' own patient records,
   allocate the DG RECORD ACCESS key to those individuals who ARE allowed
   access to their records.

Select HELP SYSTEM action or <return>: [ENT]
```

Figure 9-4: Using sensitive patient tracking tutorial (Step 5)

# 10.0 Glossary

**ADC**

Average Daily Census

**ALOS**

Average Length of Stay

**AMIS**

Automated Management Information System

**Attending physician**

Supervising physician who is responsible for the care of the patient. Non-affiliated hospitals may choose not to use this field.

**Breakeven**

A day on which the actual cost of care equals the estimated day allocation.

**CDR**

Cost Distribution Report

**Collateral visit**

A visit by a non-veteran patient whose appointment is related to or associated with a service-connected patient's treatment.

**Consistency checker**

Provides a method of assuring the accuracy of data contained in a patient file.

**Co-Pay Test**

A financial report used to determine if a patient may be exempted from pharmacy co-payments.

**DRG**

Diagnostic Related Group

**DXLS**

Diagnosis responsible for the major portion of a patient's stay.

**G&L**

Gains and Losses

**HINQ**

Hospital Inquiry

**Means Test**

A financial report used to determine if a patient may be required to make co-payments for care.

**PAF**

Patient Assessment File

**PAI**

Patient Assessment Instrument

**Primary care physician**

The health care provider with primary responsibility for the direct care of the patient. This may be the resident or intern in a teaching facility or the staff physician in a non-affiliated hospital.

**Purge**

To get rid of, remove, or delete

**PTF**

Patient Treatment File

**Routing slip**

When printed for a specified date, it shows the current appointment time, clinic, location and stop code. It also shows future appointments.

**RUG**

Resource Utilization Group

**Security code**

A code assigned to each user identifying them specifically to the system and allowing them access to the functions/options assigned to them.

**Security key**

Used in conjunction with locked options or functions.

**Special survey**

An ongoing survey of care given to patients alleging Agent Orange or ionizing radiation exposure. Each visit by such a patient must receive special survey dispositioning which records whether treatment provided was related to that exposure. This data is used for congressional reporting purposes.

**Stop code**

A three-digit number corresponding to an additional stop/service a patient received in conjunction with a clinic visit. Stop code entries are used so that medical facilities may receive credit for the services rendered during a patient visit.

**Third party billings**

Billings where a party other than the patient is billed.

**Trim point**

The expected Length of Stay range based on the LOS distribution for each DRG category.

**VADATS**

Veterans Administration Data Transmission System

**WWU**

Weighted Work Unit

# 11.0 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.

## 11.1 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, Pharmacy).

### 11.1.1 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.

### 11.1.2 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 polices and procedures prior to interconnection to or transferring data from RPMS.

### 11.1.3 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.

### 11.1.4 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.

### 11.1.5 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.

### 11.1.6 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).

### 11.1.7 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 lowercase 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 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.

### 11.1.8 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.

### 11.1.9 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

### 11.1.10 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.

### 11.1.11 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

### 11.1.12 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.

### 11.1.13 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.

## 11.2 RPMS Developers

### RPMS Developers Users 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.

## 11.3 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.

# 12.0 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