PIMS V. 5.3 ADT Module User Manual
Security Officer Menu

Display User Access to Patient Record
Enter/Edit Patient Security Level
Purge Non-sensitive Patients from Security Log
Purge Record of User Access from Security Log
ISO - Sensitive Records Report-Export
ISO - Sensitive Records Report-Formatted Report

Revision History

Initiated on 8/5/05

Date	Description (Patch # if applic.)	Project Manager	Technical Writer
8/5/05	DG*5.3*666 Enhancements - add 2 options to Security Officer Menu	Zach Fain	Corinne Bailey
8/14/08	Minor Formatting Changes	Zach Fain	Corinne Bailey

Overview

This menu 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. The following is a list of the options contained in the Security Officer menu and a brief description of their major function.

DISPLAY USER ACCESS TO PATIENT RECORD
This option displays a listing of the users who accessed a sensitive record within a specified time frame. Users must hold the DG SECURITY OFFICER key.

ENTER/EDIT PATIENT SECURITY LEVEL
This option allows a level of security to be assigned/removed to a patient's records. Users must hold the DG SENSITIVITY security key in order to access this option.

PURGE NON-SENSITIVE PATIENTS FROM SECURITY LOG
This option allows entries of non-sensitive records to be purged from the Security Log. This is necessary for patients whose security level has been changed from sensitive to non-sensitive. Users must hold the DG SECURITY OFFICER security key.

PURGE RECORD OF USER ACCESS FROM SECURITY LOG
This option is used to purge user access from the DG SECURITY LOG file. Users must hold the DG SECURITY OFFICER security key.

ISO SENSITIVE RECORDS REPORT-EXPORT
This option produces a report (in downloadable format) of sensitive patient records accessed for a date range. Users must hold the DG SECURITY OFFICER security key.

ISO SENSITIVE RECORDS REPORT-FORMATTED REPORT
This option produces a report (in printable format) of sensitive patient records accessed for a date range. Users must hold the DG SECURITY OFFICER security key.

Display User Access to Patient Record

The Display User Access to Patient Record option displays a listing of the user(s) who accessed a selected sensitive patient record within a specified date range. The list can be run for a particular user or all users.

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.

Only holders of security key DG SECURITY OFFICER may access this option.

Enter/Edit Patient Security Level

The Enter/Edit Patient Security Level option is used to assign/remove a level of sensitivity to a patient record. 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. The DG SECURITY LOG file also contains the name of the person who assigned the security and when the security was assigned.

With the initialization of ADT V. 3.6, all existing patients with an eligibility code of EMPLOYEE were automatically entered into the security log as sensitive by the system. This is not automatic, however, for employee patients subsequently entered into the system.

Accessing a sensitive patient record can trigger different messages and bulletins being sent.

Only holders of the security key DG SENSITIVITY may access this option.

Purge Non-sensitive Patients from Security Log

The Purge Non-sensitive Patients from Security Log option is used to purge patients with a non-sensitive security level from the security log. The user may 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.

Purge Record of User Access from Security Log

The Purge Record of User Access from Security Log option is used to purge user access from the DG SECURITY LOG file for a single patient or all patients for a specified date range. However, any access to a sensitive patient record must be kept in the security 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.

ISO Sensitive Records Report-Export

The ISO (Information Security Officer) Sensitive Records Report-Export option displays a listing of sensitive patient records accessed within a specified date range. The report is in a downloadable format and can be easily exported to a Microsoft Excel spreadsheet for auditing purposes.

If run for the previous day, this report will provide the same information contained within the nightly MailMan message which is sent to the members of the DG ISO SENSITIVE RCDS mail group.

Information provided on the report includes: patient name, name of user who accessed the record, title/alias/service of the user, date/time record accessed, option/protocol used to access record, and whether or not the patient was an inpatient at the time the record was accessed.

Only holders of security key DG SECURITY OFFICER may access this option.

ISO Sensitive Records Report-Formatted Report

The ISO (Information Security Officer) Sensitive Records Report-Formatted Report option displays a listing of sensitive patient records accessed within a specified date range. The report is in a printable format.

If run for the previous day, this report will provide the same information contained within the nightly MailMan message which is sent to the members of the DG ISO SENSITIVE RCDS mail group.

Information provided on the report includes: patient name, name of user who accessed the record, title, date/time record accessed, option/protocol used to access record, and whether or not the patient was an inpatient at the time the record was accessed.

Only holders of security key DG SECURITY OFFICER may access this option.