Medical Office System
Chapter 22: HIPPA Security & Privacy Menu

This chapter discusses

- output authorization control to protect the PHI data.
- managing the Security on the MOS.
- checking the data access of the users.
- managing the Privacy of PHI data.

Security and Privacy Changes to Comply with HIPPA

HIPPA will have a great impact on the Medical Billing industry. In order for your practice to better comply with the new regulations, we have added the following security, code selection options and privacy regulations.

Procedure & Diagnosis codes

Procedure and Diagnosis codes can be marked to be Not HIPPA Compliant. A question was added to make it possible to exclude any code by answering "N" to the HIPPA Compliant question. We also added an INACTIVE date field to deactivate a code as of a given date. This date is compared to the current system default date and if it is not blank and less than the default working date, the procedure or diagnosis is not displayed for selection in the browse formats.

Also, if a procedure code is supplied that is marked as not HIPPA compliant and the bill to party is "MC" or medicare, it will not accept the code.

This is not currently the case for the diagnosis codes. You may supply any code.

Privacy Changes

Who sees what and why are new considerations for HIPPA regulations. Your practice may be asked to provide this kind of history about any patient data viewed, printed, or stored. The records on your computer and printouts now are required to track this information. To allow this to work, a database of persons that information was "disclosed to" has been added. This is for persons other than your billing and treatment staff that might see patient health information (PHI). For example, a Transaction Review is sent to the accountant. That accountant would be listed as the disclosed to party and the name, address and phone number must be entered. Another example, is a request for information by a relative, police department, credit bureau, employer or other such party. The regulations will require permission from the patient, in writing for some of these, but all should be tracked. I know this sounds overwhelming but by adding some questions to every output, that will identify the purpose and therefore weed out the normal office routines, a proper tracking can be made of this information.

Definition

PHI (Patient Health Information) - All information that identifies a patient falls under this definition. An output that simply lists the name of the patient is considered part of the PHI data. Just the fact that a patient is listed on a certain practice patient list, might give very personal data to someone. For example, a practice that only treats HIV patients prints a list of patient birthdays. Just the fact that a patient is on this list, might suggest to someone that the patient has HIV. There are many such specialties that are specific enough to tell too much information.

Business Associates - (BA) - These are people that you would interact with for business purposes but are not employees, such as janitors or cleaning staff, accountants, investors, visitors to your office, family and friends, computer specialists, software vendors, etc. It is imperative that you

identify these people as they relate to your business and get a contract in place that states the appropriate control they should provide when viewing your **PHI** data. Sample contracts are available from CMS or your medical associations.

Patient Authorization - Patient authorized disclosures are also possible. With written permission from the patient, the **PHI** data might be disclosed to a family member, employer, insurance company, etc. A patient may revoke this permission, so tracking what was given to an authorized person, when and why is important to your practice. Also the permission dates and revocation dates must be respected to protect you from violation under these regulations.

Employees - Anyone working directly in the practice is a practice employee. All employees do not need access to all data stored in your computer. Each employee that would need access to the computer, would need a login and password to gain access. This login would limit access in different ways. This is the first line of defense and it is very important that each and every employee have a login and password that they use exclusively. This protects your data from unauthorized access and protects your employees from other staff members that might not be so honest.

Limiting Access to given to an Employee

Each employee can be granted access or limited access in a number of ways. Each employee should be assigned a login Identification and Password. This protects both the data and other employees by

1) restricting access to data the employee has no business seeing and
2) by tracking what each employee does in the system.

This can offer a way to know an employee is accessing data they have no business seeing, it can help the practice by catching fraudulent behavior or just offering better information to the management for training and employee development.

Each User can be granted access in many ways.

1) by the access level given to the employee that limits the data they may see.
2) by granting administrative access to see reports deemed sensitive by management.
3) by indicating an employee activation and termination date, the user can be restricted.
4) By indicating the type of access of PHI data the user is required to make to do their job.
5) Using the function passwords to limit access to functions that are sensitive.

(More details about setting up an Authorized User will follow.)

New Output Disclosure Tracking

An attempt has been made to allow each and every output function to collect and restrict access to information. Each report or output generated by the MOS has been cataloged with information about the PHI data contained on the report and the purpose for which the report is commonly used. This allows a comparison between the PHI Access of the user and the function of the report. If the user is marked as a Billing worker, then a report that would be used for Treatment or Medical History would not be accessible to that user. Likewise a report that is for Billing purposes, would only be available to a billing clerk.

It is part of the HIPPA regulations that data be restricted to function and the least amount of PHI data be supplied for any request. That means that if an employer asks for a list of patients that see you, and the list is authorized to be sent, then the list should contain no more than the patient name.

Log Files

New logging capabilities have been added to the system. A log entry is made each time a user enters the system and each time the user activates or tries to activate an output that has PHI data and the party it is disclosed to is not automatically authorized to receive data. We have made every attempt to log each access as required and provide you with the appropriate data to check that users are using the system properly.

IF YOU DO NOT ACTIVATE THE AUTHORIZED USER DATA AND ADD LOGINS FOR EACH USER, this is worthless. The system will consider every access to be fully authorized and will allow all output functions. As of October, 2003, the authorized user feature will be activated permanently. We suggest you get familiar with it much before that time.

Each user must have a unique login and be taught to log off the system when they leave their computer unattended. Unless the computer is locked in a room with access limited to the operator, login control is very important. Remember, what you are trying to control is dishonest and nosey people from gaining access to information they have no business seeing. You do not always know who these people are in your practice, but if you have more than the doctor gaining access to the system, it is imperative.

For example, if you are a solo practitioner, and have your medical data billing software installed on your personal computer, but you allow other family members to use the computer. The login access is very necessary to protect you and the patient data in your care. I am sure you would not give access to your file cabinets to other family members, think of the computer as just such a thing. (I would most urgently suggest that a computer for your medical practice be segregated from the family computer. In other words, get two computers, one for work, one for play.)

SECURITY and PRIVACY LOGS

Two additional logs have been added to help us track both security of our data and the privacy of patients.

USER LOG

To properly provide security to your data, each office user is assigned a login and password. As they use that to access different functions, through the system a record of their activity is made. Each time they try to log in a note is made. Each time they access a report, a note is made. Each time the computer denies them access or they cancel the output, a note is made. This kind of log can tell you what each worker is doing or trying to do. It should be reviewed frequently for problems. This is one way you can control what the people who have access to the computer are doing. It should also make it more difficult for unauthorized persons to access the computer without your knowledge.

HIPPA LOG

This log will record each time a patient's PHI data is included in an output. It will note the report that the data appeared on and the time and to whom it was given. Don't panic, it is only necessary to track this log information, if the data is not to be used for billing, treatment or a few other very limited purposes. As you run a report, questions will ask you who you are, and why you are running the report. Most times in the course of normal business that will be the end of it. But in case this is the monthly reports for the accountant or you are printing information for a relative, you will be asked to provide the name of the business associate or person who requested the data. Simply supply the data and run the report as before. All the appropriate data will be logged for each patient included in the report.

If the patient asks for a list of who saw his data, what they saw and when they saw it, you will have it right at your fingertips.

MOS HIPPA Security Menu

This new menu appears on the MOS REPORTS Menu choice. Press 5 7 from the Main Menu.

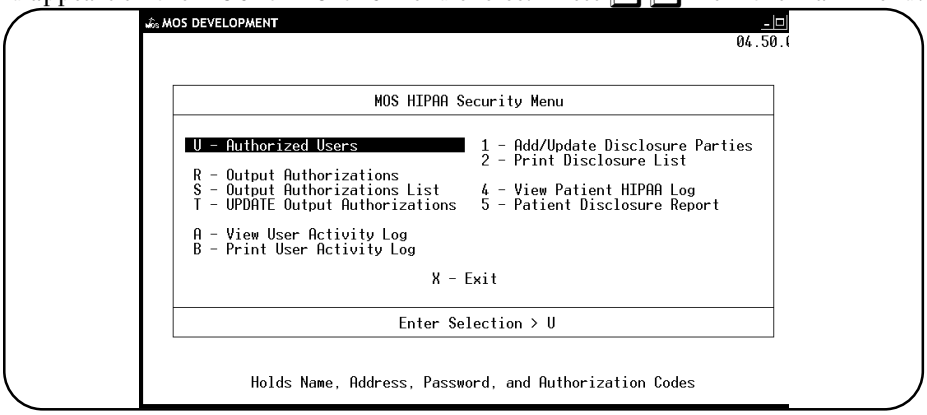


Figure 22-1:MOS HIPPA Security Menu

This new menu gives access to security functions and reports. This should make it easier to manage the overall Security on the system.

The first step necessary is to add each person that will have access to the computer to the Authorized User data file. This option also appears on the Support Files Menu and the detailed explanation of this can be found in Chapter 12, Authorized Users.

Once each user has been defined, with an appropriate access level to PHI data, then it is necessary to be sure the Authorized Users are active. This can be done in the Practice Information file found on the Support Files Menu.

Select Practice Information and a screen may appear with the Master Password HELP. If this appears on your system, press ENTER and then press Y. If the Practice Information pops right up, then press ESC P ENTER Y.

Then you will be asked for the current Master Password. This is a very important password and is the very highest level of security and access on your system. Enter the correct Master Password (if you first saw the Master Password Help screen, your password has not been changed from the default. It is still set to PASSWORD. This is the most secured level and knowing this password will allow access to all security features. Please assign a password to your system for proper control)

Guard this password well, write it down and put it in a very safe place, in case it is forgotten. It is required to access the Authorized Users and the System Passwords. Case is significant in most passwords so type the password properly.

Now the System Password screen appears:

To activate the User ID, type Y for that option. If your MASTER Password is still "PASSWORD", now is the time to change it. Protect it well and keep a copy in a safe place. (Write it down, put it in a sealed envelope, write on the envelope what it is and put in your safe or a safe place.)

The passwords are explained in Chapter 5, so I will not repeat that here.

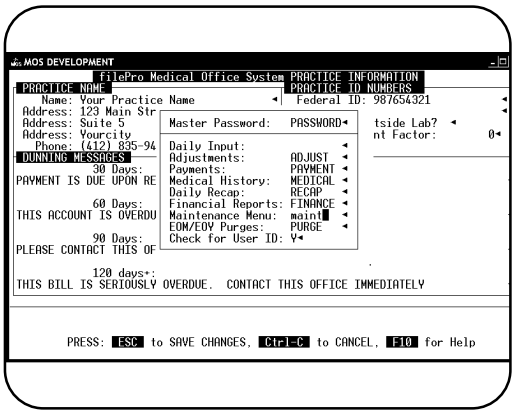


Figure 22-2: System Passwords

Press [ESC] to save the passwords. Your Authorized Users are now activated.

Adding Authorized Users

The next step necessary is to add authorized users to the system. This will create a User Login and Password for each user that should have access to the system. It will be necessary to assign access levels, PHI Authorizations and Activation dates. It is also necessary to include address and phone numbers.

To help you prepare, a page at the end of this chapter can be photocopied and filled in for each user.

R - Output Authorizations

This option will allow each output to properly allow users access, track PHI disclosures and generally secure your data from unauthorized access. This has been accomplished by defining access for each output possible.

Select [R] from the MOS HIPPA Security Menu and then enter the Master Password. Then it will be necessary to enter your User ID and Password. (A log entry is made indicating your access to this file, date and time. This is an important part of the security.)

This will bring you to the Choose Record Options Menu. To locate an existing output, select [4] [A]. Then press the keystrokes used to run the report from the main menu.

For example, to run the Diagnosis Report you would press [5] [1] [1]. As a way to help with this method, most new reports should print the keystroke sequence in the upper right hand corner. The only reports that do not follow this rule are things you would send to others, claims, statements, and letters.

Deletion is not allowed in this file. If you wish to control access, press U to update the record and enter NONE for the Security Level.

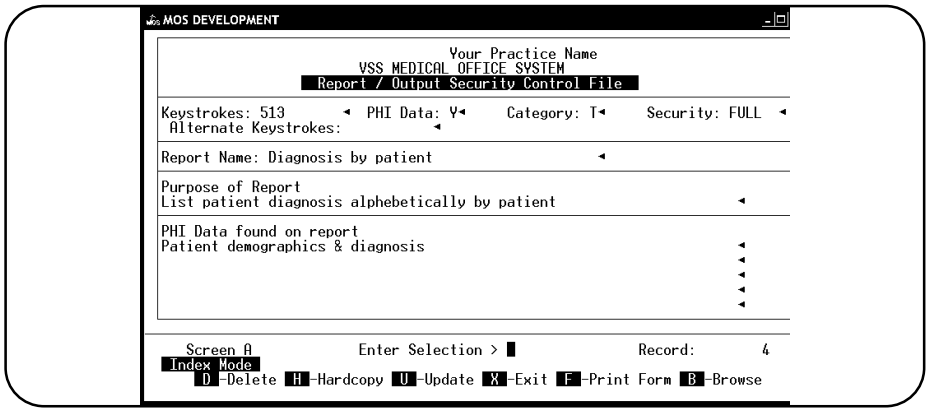


Figure 22-3:Output Authorizations

When defining the Output Authorizations, the output can be restricted as follows:

PHI Data (Y/N) An output marked with N does not require any additional security with regard to restrictions about PHI data. It will still be restricted by the Security Setting, however.

Category of output Type of office function that would require this report.

Billing Report

Treatment Report

Administration Report
Miscellaneous - all access but not classified as one of the above.

Report Security This can control any report and be used to restrict the access to specific personnel. This can be used to control access to logs, financial reports, etc. All reports are controlled by the PHI settings. These are in addition to those levels and can add another layer of security. In a small practice, where the Users need to have both treatment and billing access, this level can allow the office administrator to control some more sensitive reports and outputs.

FULL	This report only is restricted based on the PHI data and category information. No additional restrictions are made.
PASSWD	This requires a password to run. Each report can have a different password. This password is also required to change the security on the report. When the word PASSWD is supplied in this field, the prompt for the password appears when you press ESC . It is necessary to enter the password twice, to insure it is stored correctly. Whenever, you update an output authorization with a password, it may be changed when the record is saved.
ADMIN	This report requires an administration level access and a password. Using this setting is similar to the PASSWD setting but this would only be accessible to a user with administration access and will also use a password
NONE	This report may not be run by anyone. If any of the reports are to be locked down from any access, use this setting.

.

Report Name The name of the report as it appears on the menu.

Purpose of Report Reason for running this report This just needs to be a general explanation of the use of the report in your practice.

PHI Data PHI data found on this report. This would indicate the type of data the report contains about the patient. A list of data or a general accounting of what would be disclosed if this output were printed.

DEFAULT PASSWORDS: On a few outputs, the security level was set to ADMIN or PASSWD, to help you get familiar with the use of these permissions. The password we set is easy to remember and should be removed or changed if you wish the passwords to be secure. For an ADMIN password enter "ADMIN" and for a PASSWD item enter "PASSWD". Remember, the fact that I have printed them in the manual makes them useless as real security. As with all passwords they should be unknown to the people that need to be excluded. A good password should be something easy to remember but not easily connected to you. Never use your birthday, name, children's names, dog's name, etc. I might suggest things like this: med$bill, adm-only, no-way, not!allw - two words with a punctuation can be easy to remember but difficult to guess.

T - Browse Output Authorizations

Browse can offer a quick way to look at the output authorizations. Display one record and press B at the Enter Selection prompt. Highlight a particular item and press ENTER and that items full screen will be displayed.

It is then possible to update or review the information. To return to the browse list, just press B .

S - Output Authorization List

This report will list all the output authorizations. They page feed on the first keystroke so the items are sorted by the menu or functions.

Paper: This report requires 8 ½ x 11 paper.

Selection: All records are selected.

Procedure: This report will require a user name and password. Then the purpose of the report must be supplied.

Sample page shown below. Notice in the upper right the code for this report (57S). The columns can be explained by looking at the data fields above. Complete list can be found in Appendix F.

T - UPDATE Output Authorizations

This option also appears on the installation menu. This will add any new output authorizations to the list that might have been added in an upgrade. Since each and every output must have a record in this file or it will not be able to be executed, it is necessary to add new ones whenever we add an new report or output to your system.

All you need to do is to select this, a prompt will remind you that current authorizations are not changed only new ones will be added. Be sure the answer is Y and press ENTER .

When it is finished, a prompt will display that indicates how many new items were added.

Activity Log

This item is used by administrators or managers to review the access requested by users. It is important to see who is doing what, when and why.

Reasons to review this data.

1. It might be important to see that a user repeatedly attempted to log into a report and was denied access.

2. Look for users running outputs that fall outside their job descriptions.

3. Look for repeated requests for the same output, where someone may be making a copy for personal use.

4. Look at denied items or cancelled items for attempts to access data that is not allowed.

Press A from the menu. This requires the master password, user name and password.

Then the index selections appear:

Depending on what you want to know select the correct index.

A - User Login Name, Date, report key

B - Report Key, User Name

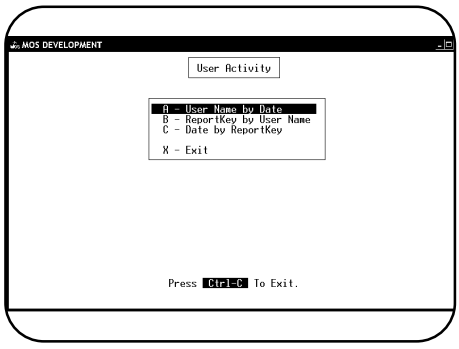


Figure 22-4:User Activity Indexes

C - Date, Report Key

If you want to see what happened today, select index C, and enter today's date. Then all items for today are displayed.

If you want to see what was done by a User, select index A and enter a User name .

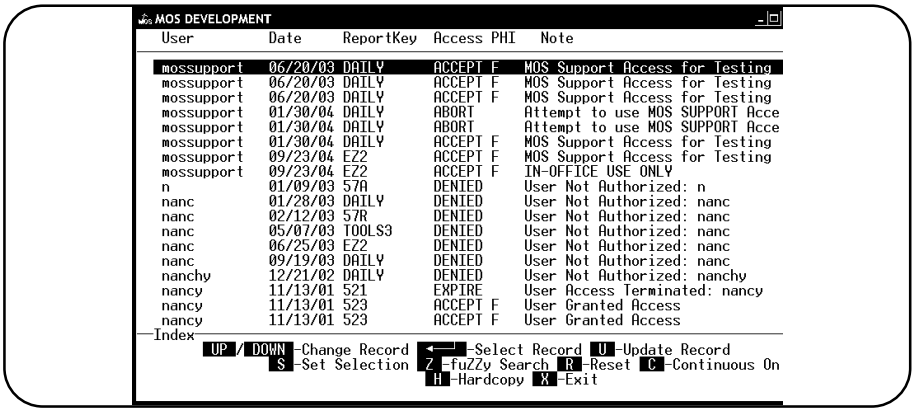


Figure 22-5: Browse User Activity by User

Notice 3 items with no user, these options were canceled without proper login. Notice the billing user tried to print report 528 twice and was denied because they did not have access to that type of output.

Notice 2 items where the billing2 user tried to run an ADMIN report 523 and was denied. Use the menus or a reference printout of the Output Authorizations, to see what report the user was attempting to access.
the practice responsibility, to protect the PHI data and this information can help control who is doing what.

B - Print User Activity Log (572)

This selection will allow the information in the User Activity Log to be printed in various ways. Select this item and supply your user name and password.

Then a selection menu appears.

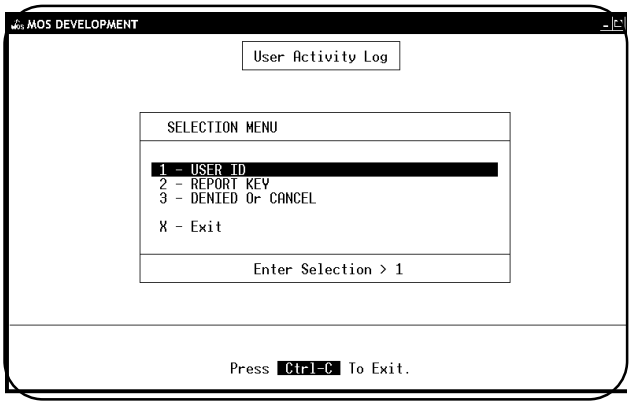


Figure 22-6: User Activity Log Selection Menu

User ID

Enter a User ID, then a prompt for Start Activity Date and End Activity Date. This will allow a data range selection.

The output is sorted by reportkey then date.

Report Key

Enter the report key that is of concern. A data range can then be supplied.

```
                    Your Practice Name                                                    (57B)
                          VSS Medical Office System
Sort by: Dummy field          User Activity Log                          Printed: Mar 19, 2003
                         Date
  Page: 1
User Name    Time     Report     Result     Note
-------------------------------------------------------------------------------------------
nancy        08/08/02 520        ACCEPT    User Granted Access
                  08:11:35  Missed recall report

nancy        08/08/02 520        ACCEPT    FOR TREATMENT PURPOSE
                  10:12:34 Missed recall report

nancy        08/08/02 520        ACCEPT    User Granted Access
                  10:45:20  Missed recall report

nancy        08/08/02 520        ACCEPT    FOR TREATMENT PURPOSE
                   13:12:33 Missed recall report

nancy        08/08/02 520        ACCEPT    User Granted Access
                   14:22:45 Missed recall report

nancy        08/08/02 520        ACCEPT    FOR TREATMENT PURPOSE
                   20:11:20 Missed recall report

UNKNOWN 03/14/02 520        ACCEPT    NO AUTHORIZED USERS ACTIVE
                   09:11:34   Missed recall report
```

Denied or Cancel Select this to see the entries for any transaction that was denied or canceled. This should zero in on any faults or access attempts. Remember it is normal that on occasion a person would select an incorrect menu choice or make a mistake typing in their login or password. Repeated attempts, in a very short time, or at times that are outside of business hours would be a red flag.

1 - Add/Update Disclosure Parties

This option can be used to add or modify the parties that might receive Patient Health Information other than the patient. This might contain the name and address of your accountant, Virtual Software Systems, Employers, Law Enforcement or a Patient's friend, or relative. When disclosing information, if it must be tracked for HIPPA regulations, the name and address of the person or Business Associate that receives the information must be stored.

To speed data entry, the names are categorized by areas so that once the purpose of the output has been given, the people in that category are displayed. For example, if you indicate that the output will go to a lawyer, then all the lawyers are displayed for your selection. When creating an output, the disclosure party can be added then or added to this file from here.

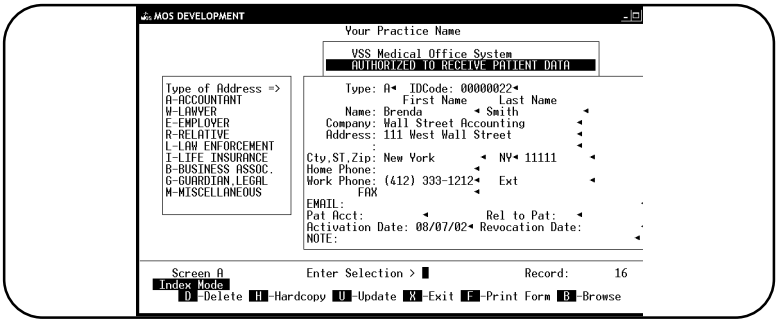


Figure 22-7:Disclosure Party Screen

Type Enter a type code from the chart at the left of the screen.

IDCode Enter an identifying code for this party. Initials, abbreviations of the company name, or other such codes might be helpful.

Name & Address Enter the name and address, phone numbers and extensions for the party. It is important to make this as complete as possible.

Email/Fax A sign of the times, many people communicate by email or fax and this might be helpful.

Pat Acct This will contain the patient account number when the party is a patient related party, such as a relative or legal guardian. This connection can be made by adding these parties from the patient record, but it will work just fine from here.

Rel to Pat Enter the relationship of this party to the patient. This uses the normal codes you are familiar with in Insurance relationships.

Activation Date Enter the date the permission was given from the associated patient, if it is associated with a patient, or the date you entered into a Business Associates agreement. Some parties entered here, may be covered by the HIPPA regulations as a valid party for disclosure such as a Medical Consultant, Collection Agency, but I think you might want to track disclosures to them and track your agreement by entering them in this file.

Revocation Date If the permission given to disclose to this party is revoked by the patient or other party, enter the date that disclosure should be denied.

Since Patients can give and take back permission you will need to start a new disclosure party if the disclosure permission is given again. It is important to track the time when permission was given, so you can show that any disclosure made to that party was in the time you had permission to do so. This is your protection.

Note This is available for any notes you might like to make about this party.

2 - Print Disclosure List (572)

This option will print a list of the data in the disclosure parties data base.

The selection and sort options are open to allow those items to be varied as necessary. Using the sort defaults will sort the addresses by type.

Procedure: Select 2 from the HIPPA Security Menu. Enter your selection and sort options, if you want all items just press ENTER ESC Y Then prompts will request your User ID & Password.

This report requires 8 ½ x 15" paper or a printer capable of 12 pitch.

4 - View Patient HIPPA Log

This log is part of the required HIPPA disclosure information. Each time an Patient Health Information (PHI) is included in output functions used for things other than billing or treatment, it is necessary to track the destination of that information. Who you sent it to, why and what kind of information was included about the patient. In order to accomplish this, each output now knows if it contains PHI data, what kind of data is included, what the output should be used for in your practice and possible security to protect the data.

This file will grow, however, it is only necessary to track things that are not for billing or treatment, and that shortens the list considerably.

Select 4 from the HIPPA Security & Privacy Menu. Then enter the Master Password. Since this data is required and must be protected, great amounts protection have been applied. The data in this file can not be changed, or deleted. A log entry is made when you access this file. Only Users with Administration Access are permitted to access this file.

The first screen displayed is:

Select the best option for what you are looking to find in this file and then enter the key data. It is not necessary to enter all the key data, just the first item is enough to start the search. If you have more specific information, supply as much as you know.

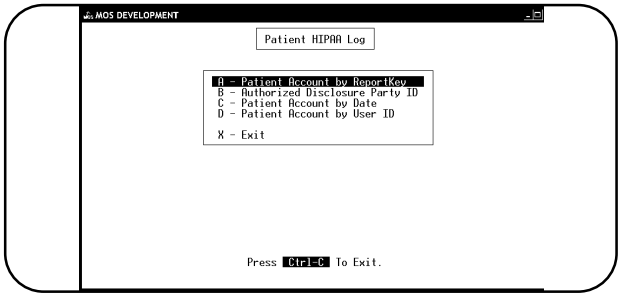


Figure 22-8:Patient HIPPA Log Indexes

For example, if you want to see everything sent to your accountant, then select index B and enter the ID for the accountant. When the screen is displayed, press [B] to browse down the list. To see the full screen for any item in the browse, highlight the item then press [ENTER] .

The full screen display will show the following.

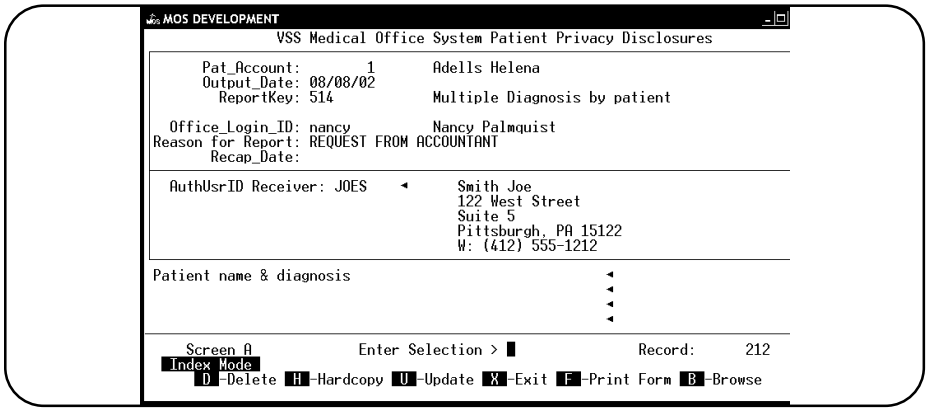


Figure 22-9:Patient Privacy Disclosures Screen

This screen has collected information form a number of files. It displays the patient name, the user that ran the report, the name of the report, the name, address and phone number of the disclosure party. It also shows the data that would be included on this output.

5 - Patient Disclosure Report

Purpose

This report will print the disclosed items for a patient between given dates. The report is installed with the Administration Password set to "admin". This can be changed in the Output Authorization.

Paper

8 ½ x 15" paper or a laser printer with 16.5 pitch fonts.

Sort

By patient, then by disclosure date.

Selection

One patient, between given dates.

Procedure

Select 4 from the HIPPA Security Menu. Supply the security information.

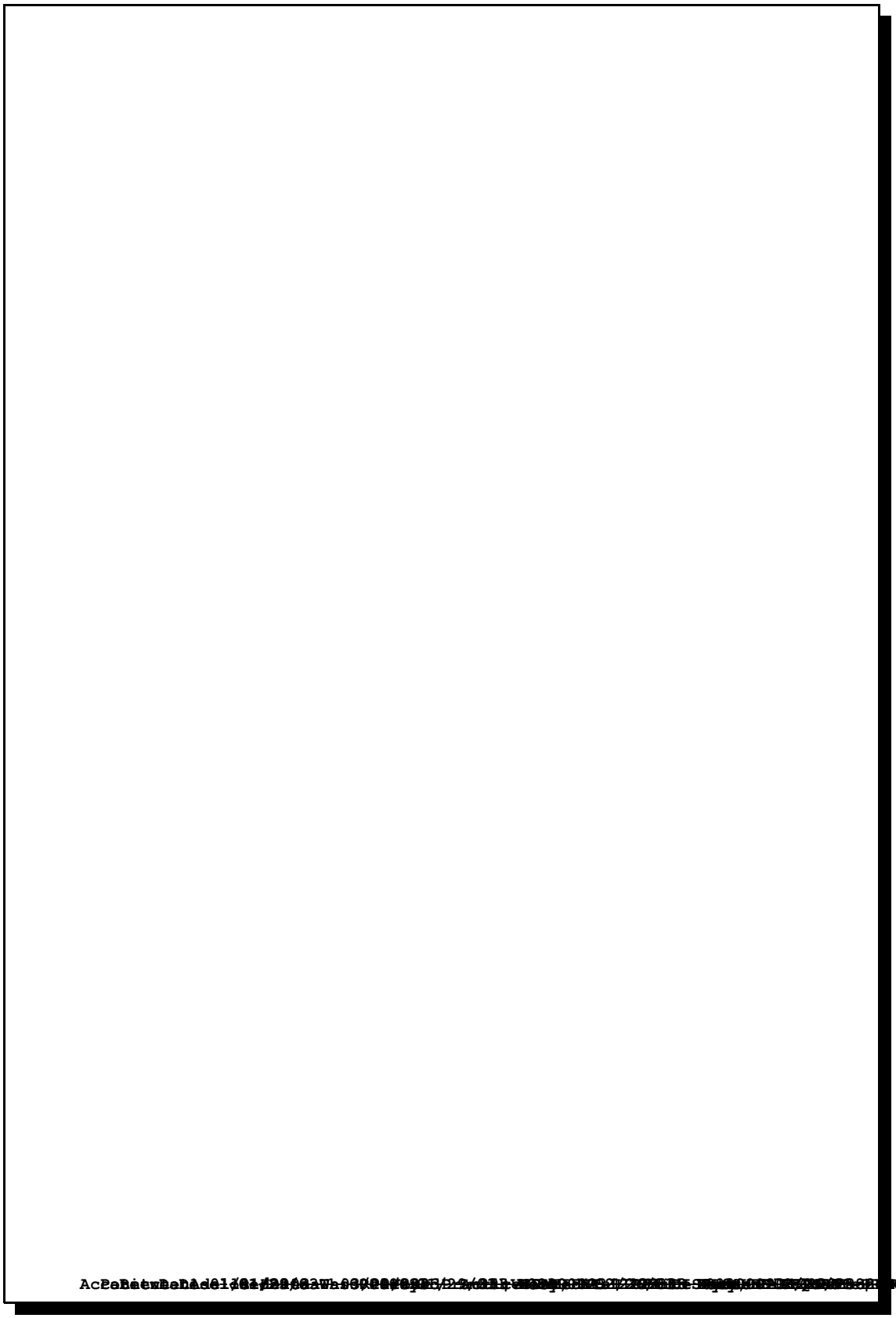
Enter the Patient Account Number that should be printed.

Enter the Starting Date to select. The default is the lowest date in your 100 year range.

Enter the Ending Date to select. The default is today's date.

A REDO prompt is displayed. Press ENTER or N to continue to generate the report.

A sample of the report is shown on the next page.



AUTHORIZED USER Questionnaire

File this as part of your HIPPA policy.

User First Name:_____ **User Last Name:**_____

Address:_____

Address:_____

City:_____ **State:** _____ **Zip:** _____

Phone: (_____) _____ - _____

User Login Name (12 characters max, case is not significant) _____

For security, when the user is added, have them type the password when the question appears. Then it will be known only to them. It is typed twice to make sure it is stored correctly.

Activation Date:_____ Date the user is first allowed to access the data

Termination Date: _____ Date the user is no longer allowed to access the data.

Access Level Check one

_____ F Requires Full access to all functions. If only one person uses the computer, select this.

_____ I Only requires Inquiry access, this user may not change data.

_____ A User will make appointments and Inquire in other areas. Only able to add patient name and phone number, in order to establish an appointment.

_____ R Receptionist - Add patients, update patient address screen, make appointments. This user will also be able to manage appointments.

PHI Level- Check One

_____ B This user only does billing functions.

_____ T This user only needs access to treatment history and medical notes.

_____ F Full access to both billing and treatment is necessary for this user.

_____ N No access is ALLOWED. At any time a user should be made inactive this would do it.

Does this user need access to areas indicated restricted to Administration?
YES NO

It is also important to restrict access to the computer by establishing a computer login/password and Screen Savers with passwords that activate when the computer is inactive for a time.