Defense Health Agency

Protected Health Information Management Tool

(PHIMT)

Training Reference: Regular User Guide
Version 3.0

March 2011

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

Last Edited: 3/8/2011

TABLE OF CONTENTS

1.0 INTRODUCTION TO PHIMT 3
1.1 PHIMT USER PERMISSIONS 3
1.2 PHIMT USER ROLES 4
1.2.1 PRIVACY SPECIALIST 5
1.2.2 REGULAR USER 5
1.2.3 USER ADMIN 5
1.3 PHIMT SYSTEM REQUIREMENTS 5
1.3.1 BROWSER REQUIREMENTS 5
1.3.2 PLUG-INS 6
2.0 ACCESSING AND USING PHIMT 6
3.0 UNDERSTANDING PHIMT SCREENS 9
3.1 SCREEN FEATURES 9
3.1.1 DATE 9
3.1.2 NAVIGATIONAL OPTIONS 9
3.1.3 STATUS BOX 9
3.1.4 ACTIVITY HYPERLINKS 10
3.1.5 PHIMT SCREEN TABS 10
3.1.6 SCREEN TITLE 10
3.1.7 DISPLAY SCREEN/APPLICATION WINDOW 10
3.2 PHIMT ERROR MESSAGES 11
4.0 MHS DATA REPOSITORY 11
4.1 ACCESSING PATIENT ACCOUNTS 12
4.2 DUPLICATE ACCOUNTS 13
4.3 PATIENT PROFILE 13
5.0 REGULAR USER FUNCTIONALITY 14
5.1 USER TAB ACTIVITIES 14
5.1.1 MY PROFILE 14
5.1.2 MY REQUESTS 16
5.1.3 MY WORKLIST 18
5.1.4 SWITCH ORGANIZATIONS 18
5.2 PATIENT TAB ACTIVITIES 19
5.2.1 PATIENT SEARCH 19
5.2.2 ADD A PATIENT RECORD 21
5.2.3 CREATE AN ALTERNATIVE PHONE NUMBER 23
5.3 REQUESTS TAB ACTIVITIES 24
5.3.1 RECORD A DISCLOSURE REQUEST 25
5.3.2 UPDATE PATIENT ADDRESS 31
5.3.3 RECORD A SIMPLE DISCLOSURE REQUEST 33
5.3.4 RECORD AN ACCOUNTING OF DISCLOSURES REQUEST 39
5.4 REQUESTER TAB ACTIVITIES 44
5.4.1 REQUESTER SEARCH 44
5.4.2 REQUESTER REQUESTS 46
5.4.3 REQUESTER PROFILE 47
5.4.4 REQUESTER SUMMARY 48
6.0 GLOSSARY 50
7.0 USER ROLE PERMISSIONS 54

1.0 INTRODUCTION TO PHIMT

The Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires covered entities to safeguard patients' medical records. The Department of Defense (DoD) regulation, DoD 6025.18-R, Health Information Privacy Regulation, implements the Privacy Rule for the Military Health System (MHS).

The Privacy Rule requires a covered entity to maintain a history of when and to whom disclosures of Protected Health Information (PHI) are made. The MHS, as a covered entity, must be able to provide an accounting of those disclosures to an individual upon request. Authorizations and Restrictions from an individual to a covered entity are included in the information required for tracking purposes.

In accordance with DoD 6025.18-R, military treatment facilities (MTFs), as covered entities within the MHS, must provide an accounting of disclosures within 60 days of a request. If the MTF cannot honor an accounting of disclosures within the 60-day period, it must provide information to the requester as to the reason for the delay and expected completion date. The MTF may extend the time to provide the accounting by no more than 30 days. Only one extension is permitted per request.

To comply with these requirements, Defense Health Agency (DHA) created an electronic disclosure-tracking tool. The Protected Health Information Management Tool (PHIMT) stores information about all disclosures, authorizations, and restrictions that are made for a particular patient. PHIMT has a functionality built into it that can provide an accounting of disclosures. This tool is available for MHS covered entities, including MTFs.

1.1 PHIMT User Permissions

Each user is assigned to one or more organization(s), which is defined as a logical or physical entity such as an MTF, a Military Service, or DHA.

PHIMT permissions are based on status-level relationships within Service Groups. These Service Groups consist of the Army, Navy, Air Force, and Coast Guard. Anyone in a given Service Group can be granted access to information required to perform his or her duties. Specific roles have corresponding permissions that determine who will have access to what information. Individuals with PHIMT roles have access to information required for job performance as well as access to information accessible to those roles with fewer permissions. No individual will be granted access to information needed to perform duties that require a higher set of permissions. Those in roles with the highest levels of permissions will have access to all information within their Service Group. An individual within any Service Group may not be granted access to information in any other Service Group.

For example, DHA, Group A the top tier, occupies those roles with the highest levels of permissions. Individuals in this group are granted access to all information within their Service Group. Individuals Group B the second tier, do not have access to the information accessible to those in the top tier since they occupy roles requiring a lower level of permissions. However,

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

Group B does have access to the information in Group C, comprised of roles requiring even lower permission levels. The third tier, Group C, is comprised of offices and command centers within the Service Groups. This tier can only access information necessary for the individual to complete his or her responsibilities. The individual does not have access to information within the higher tiers. There is absolutely no viewing of an individual's information outside of his or her own Service Group.

1.2 PHIMT User Roles

A role is a named collection of permissions. Roles allow users with the same permissions to be grouped under a unique name. PHIMT roles include Regular User, User Admin, Privacy Specialist, and Tool Admin.

- A Regular User is a general role with basic functionality. This role can create disclosures and authorization requests that can be routed on to a Privacy Specialist.
- A User Admin is a local administrator for a MTF or a designated Service. The e-mail account administrators will handle this role for each MTF or Service.
- A Privacy Specialist is the Privacy Officer or designee at an MTF or Service level. This role allows the user to maintain disclosure reporting, approve/deny disclosure requests, amend requests, restrict, and suspend disclosures, and to generate associated letters.
- A Tool Administrator has global access to the application and will be maintained by the PHIMT Help Desk. This role allows the user to configure roles within MTFs, and create permissions within the application.

Within an organization, each user can have one or more role(s). A user can have the same roles in multiple organizations, or different roles in multiple organizations. Roles are inherited through permission levels

NOTE: An individual's particular user role will determine the level of PHIMT activities he or she is authorized to perform. Different user roles are authorized to access different tabs in the tool.

The Privacy Office is responsible for granting PHIMT Users access to certain departments that manage PHI based on the user's degree of permissions. Some of the departments that the Privacy Officer may wish to grant access include, but are not limited to:

- Medical records
- Release of information
- Patient advocate
- Patient's rights
- Privacy office

Some or all individuals within these departments may also be designated as Regular Users or Privacy Specialists.

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

1.2.1 Privacy Specialist

In PHIMT, the Privacy Specialist is usually a Privacy Officer within the facility or a designee at an MTF or Service level. This role allows the user to maintain disclosure reporting, approve/deny disclosure requests, amend requests, restrict and suspend disclosures, and issue complaints.

The Privacy Specialist understands how the MTF manages disclosures. Disclosure requests may be routed from a Regular User to the Privacy Specialist or from one Privacy Specialist to another. This process helps establish working relationships between the different PHIMT users.

1.2.2 Regular User

The Regular User can create disclosure and authorization requests that can later be routed to a Privacy Specialist. He or she can review patient profiles, record an accounting of disclosure request, and revoke authorizations.

1.2.3 User Admin

The User Admin will create User-to-User Relationships as directed by the Privacy Officer. A collaborative effort is required to ensure the release of PHI is managed within PHIMT. Before establishing any relationships, the Privacy Officer will have an understanding of the way the MTF manages disclosures, the key individuals involved in the release of information and tracking of disclosures, and the approval process. A complimentary knowledge base will come from you and your understanding of how to create a workflow by routing the requests of a Regular User to a Privacy Specialist and from a Privacy Specialist to another Privacy Specialist, if necessary. Multiple User-to-User Relationships can be established throughout the facility.

1.3 PHIMT SYSTEM REQUIREMENTS

Before using PHIMT, it is necessary to understand and ensure the operating requirements are met. PHIMT has specific requirements for the operating system, browser, and plug-ins. In particular, PHIMT requires a Microsoft Windows operating system: Windows XP (home, professional), Windows 2000 (standard, professional, advanced), or Windows 98.

NOTE: Windows NT works with PHIMT in most cases, but some limitations may exist.

1.3.1 Browser Requirements

PHIMT requires the use of Microsoft Internet Explorer, version 6.0 or above.

NOTE: Cookies and JavaScript should be enabled (these items are enabled in a default browser installation).

1.3.2 Plug-Ins

PHIMT requires the use of Adobe Acrobat, version 6.0 or above. The application will also work with version 5.0 but the latest version is recommended.

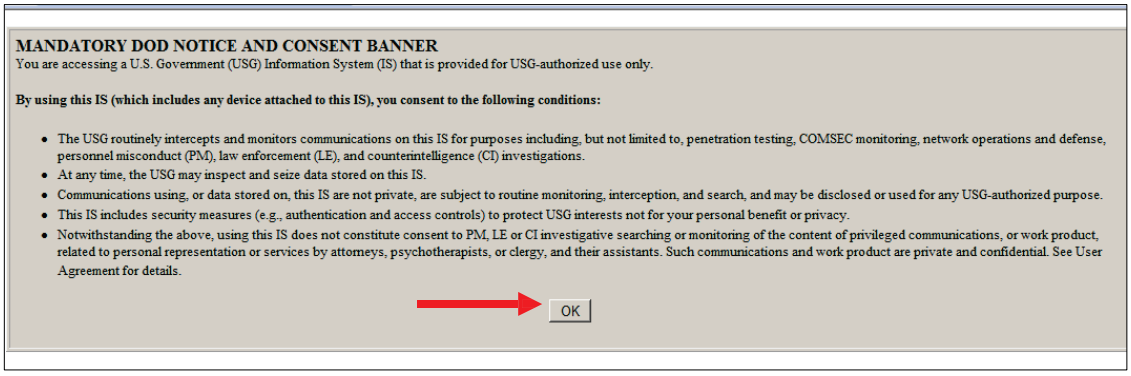
NOTE: To display the generated letters and reports in the browser, the Adobe Acrobat Plug-in is required. This is normally installed with Adobe Acrobat Reader. Download Adobe Acrobat for free at http://www.adobe.com.

2.0 ACCESSING AND USING PHIMT

Now that you have an understanding of why PHIMT was developed, are familiar with its capabilities and system requirements, and understand your role, you are ready to access the application.

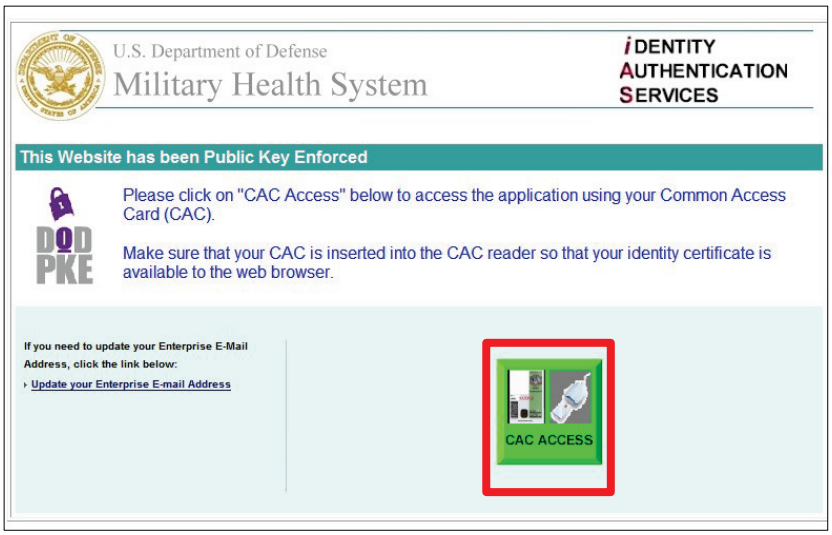
To login to the PHIMT application:

1. Enter the URL for PHIMT into the Web browser, https://tma-phimt.csd.disa.mil/hipaax



2. Read the DoD Notice and Consent Banner.

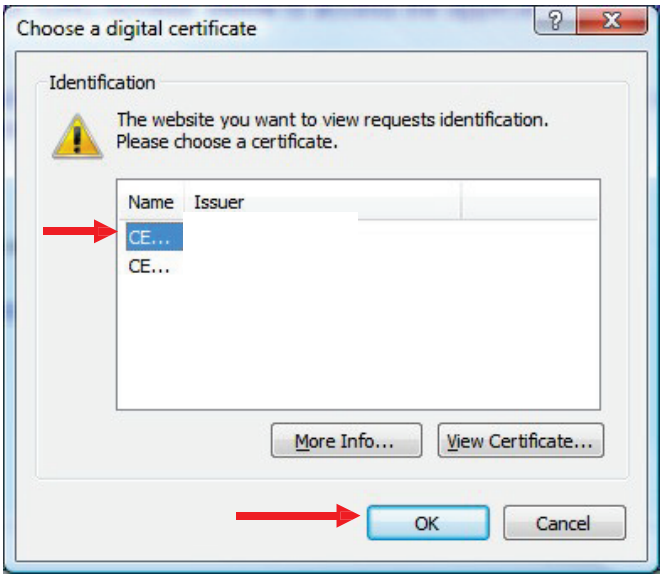
3. Click on the OK button.

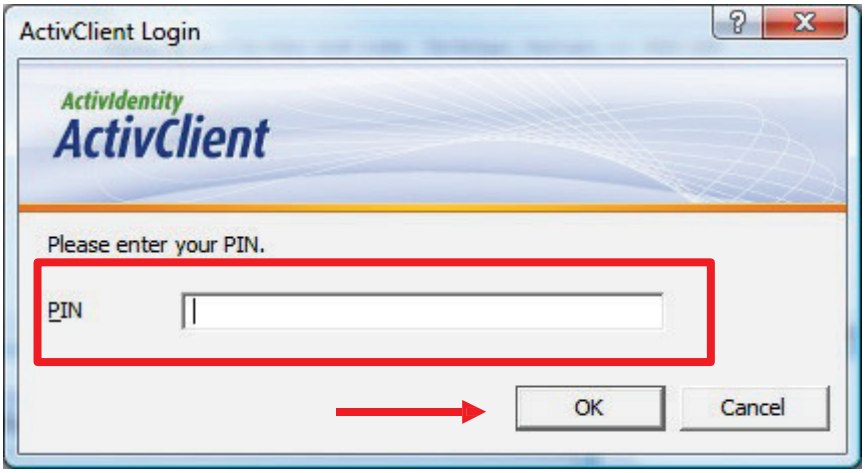


4. Click on the Green CAC Access button.

5. Select CAC Identification.

6. Click on the OK button.





7. Enter CAC PIN.

8. Click on the OK button.

9. Read the Notice and Terms of Use.

10. Click on the Accept button.

- Upon successful login you will be brought to the PHIMT User Tab.

3.0 UNDERSTANDING PHIMT SCREENS

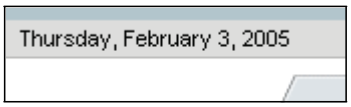
Each tab of the PHIMT screens contains some basic information that will be helpful to you when performing the various activities.

3.1 SCREEN FEATURES

There are many features to the PHIMT screen that you can use to navigate your way through the many disclosure activities you will perform. These features are discussed here.

3.1.1 Date

The date displays the current weekday, month, day, and year in the upper left corner of the PHIMT screen.

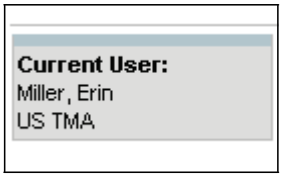


3.1.2 Navigational Options

Navigational options, such as logoff, provide directional hyperlinks that will help you to proceed through the PHIMT application. They are located in the upper right hand corner of the PHIMT screen.

3.1.3 Status Box

The gray status box shows current information and is located in the upper left hand corner of all PHIMT screens. The box displays the current user, user information such as organization and assigned role, patient information, and information about what disclosure activity is currently being performed. This information is updated when making inputs for various activities.



Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

3.1.4 Activity Hyperlinks

The activity hyperlinks are located under the status box, on the left hand side of the PHIMT screen. This listing consists of hyperlinks for activities that can be performed while in a specific "tab." The hyperlinks may include: My Profile, My Requests, or My Worklist; depending on which tab you are using. Your user role will determine specific hyperlinks listed.

3.1.5 PHIMT Screen Tabs

PHIMT screen tabs are labels that are located at the top of the display screen. The tabs serve as file folders for different groupings of activities. The specific tabs will vary depending on what role you are assigned.

- Privacy Specialist tabs includes: Patient, User, Admin, Requests, Requester
- Regular User tabs includes: Patient, User, Requests, Requester
- User Admin tabs includes: User, Admin. Each tab allows for different activities.

3.1.6 Screen Title

The screen title is located directly under the tabs and above the display screen. This is the title of the particular screen being displayed (ex. user worklist, patient search results).

3.1.7 Display Screen/Application Window

The display screen/application window is the PHIMT user's work area. These screens contain various fields in which to provide required information for proceeding through the PHIMT activities. To assist with data input, PHIMT provides text boxes, windows, calendar icons, and drop down menus. All features may not be on a particular user screen:

- Radio buttons – Radio buttons appear as black dots to indicate selection. You can toggle the buttons between selected and not selected.
- Check marks – Check marks are used to indicate a done or un-done status. You can toggle the marks between checked and unchecked.
- Drop down menus – Drop down menus provide the user with a list of possible selections from which to choose. Clicking on a particular selection causes it to be selected and appear in the "window." You can change a selection by clicking the arrow on the menu box and then clicking on a different item.
- Text boxes – Text boxes are empty fields in which you can provide information. At times, this data is requested as additional comments or for supplemental information.
- Calendar icons – Calendar icons are provided to make it easier for you to input required dates. Date inputs are specific dates chosen by you to clarify time limits on various PHIMT activities. Choose a date by selecting the arrow in the date window. A calendar icon appears for easy inputs. Click on the desired date or use the arrows near the month and year headings to display a date not currently shown. The date you select will appear in the date window.
- Action buttons – Action buttons are used to guide you through the PHIMT steps and processes. Click on these buttons to proceed through various activities. Examples of these buttons include: Next, Save, Create, and Update.

NOTE: These features will be discussed when they are used in an activity.

3.2 PHIMT ERROR MESSAGES

PHIMT issues error messages when an entry or selection is not appropriate or complete. The message begins "Error(s) have occurred" and then follows with a bulleted list of the errors. For example, if you try to route an activity to someone who does not have access to that information, or you are not authorized to route the information to that particular person, PHIMT will display a message indicating that you do not have the authority to perform that task. If you have not provided information for all the required data fields, PHIMT will issue a message indicating that information is missing. Once the error has been corrected, you can proceed to the next step in the PHIMT activity.

4.0 MHS DATA REPOSITORY

PHIMT has an automatic monthly upload of patient demographic information from the Military Health System (MHS) Data Repository (MDR). This avoids the need for Users to manually enter patient demographics information prior to recording a disclosure, thus significantly decreasing the time needed to record a disclosure. In addition, this capability decreases the likelihood of erroneous information entering PHIMT and increases the reliability and accuracy of the information it contains.

Now that the MDR data has been implemented in the PHIMT, the patient demographics will not need to be manually entered. When searching for a patient, all patient records in the MDR and PHIMT that meet your search criteria will be returned. The word "New" will appear next to all records that are from the MDR.

Test, Tonya	new	224414478 224664223 EDIPN:1046194728		1973-09-15	P.O. Box 42 Howardsville, VA 24562-0042
Test, Vanessa	121489	538394984 EDIPN:1086820702		1998-04-16	125 Granby Pl Portland, TX 78374-1407
Test, Virginia	62141	177308169 EDIPN:1034250320		1939-12-27	12475 Highgate Ln Gloucester, VA 23061-2649
Test, Weekend	62139	266090002 EDIPN:1268571627		1965-10-01	Undefined
Test, William	121488	318743051 EDIPN:1264557700	318743051	1982-07-01	527 I Ave Sheppard Afb, TX 76311-2502

Other options:
Adjust your search criteria and try again.
Create a new Patient record.

NOTE: When available, the address in the MDR will supersede the address in the PHIMT, unless the address in the MDR is blank. If the address in the MDR does not match the address in the PHIMT, the address in the MDR will be the default address. If there is not an address listed in the PHIMT, the address from the MDR Data will be used.

Once the patient record has been selected by clicking directly on the name of the patient, the record will be given a PHIMT Patient ID number, rather than being labeled as "New."

Monday, April 19, 2010 Patient Search Logoff

Patient | User | Admin | Requests | Requester

Current Patient:
Test, Rebecca
03/13/1984
EDIPN:1385132766

Summary
Requests
Record Disclosure
Accounting Suspensions
Disclosure Restrictions
Authorization
Notice
Patient Profile
Relationships
Generate Form

Patient Search

Patient Search Results

Search Results - Click on the name to select a person

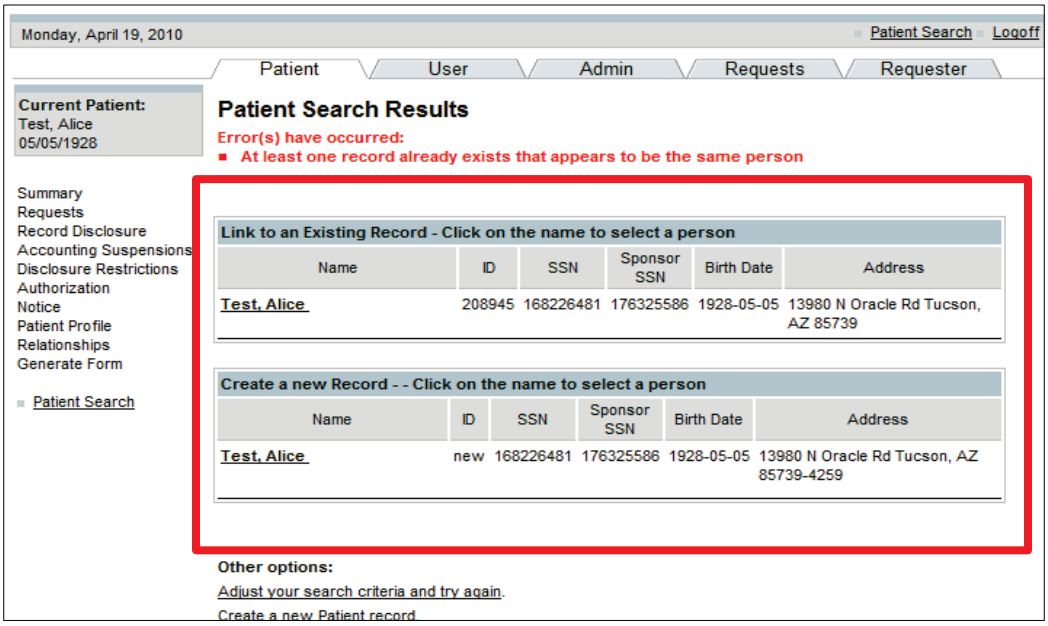
Name	ID	SSN	Sponsor SSN	Birth Date	Address
Test, Rebecca	208939	271905664	274864759	1984-03-13	1445 Beaver Creek Ln Kettering, OH 45429-3703
		EDIPN:1385132766			

Other options:
Adjust your search criteria and try again.
Create a new Patient record.

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

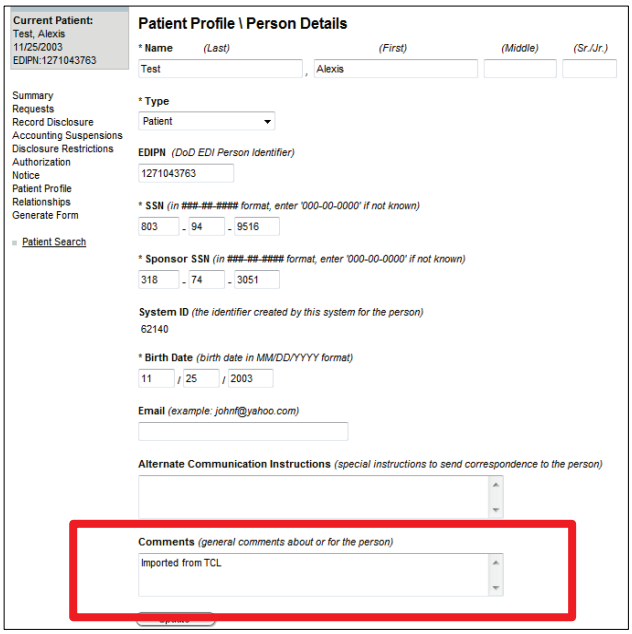
4.2 DUPLICATE ACCOUNTS

When using the PHIMT to access a patient's account, the EDIPN is used as the unique identifier. If there are two patients with the same SSN but different EDIPNs in the PHIMT and/or MDR data, both accounts will display, clicking on the patient name will select appropriate account.



4.3 PATIENT PROFILE

All patient profiles that are taken from the MDR will be labeled with "Imported from TCL" to show that the information has been imported.



Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

5.0 REGULAR USER FUNCTIONALITY

The following information will provide you with step-by-step instructions for recording requests and routing them to your Privacy Specialist for approval.

Your role as Regular User requires you to perform various PHIMT activities. The steps for performing these activities will be presented here and include the following:

- Record Disclosure Requests
- Record an Accounting of Disclosure Request
- Record Simple Disclosure Requests

5.1 USER TAB ACTIVITIES

The User tab provides you with various hyperlinks that allow you to perform "desk duties" such as accessing PHIMT User-related information, switching organizations, viewing past requests, and tracking tasks assigned to you. These hyperlinks include:

- My Profile
- My Requests
- My Worklist
- Switch organizations

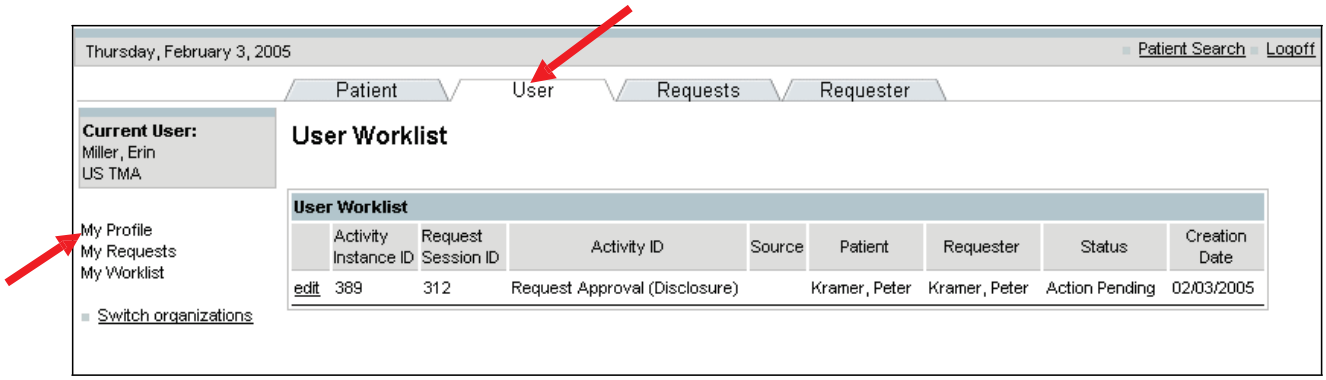
5.1.1 My Profile

NOTE: The My Profile hyperlink allows you to enter/update personal information and preference data.

To edit your profile:

1. Select the User Tab.

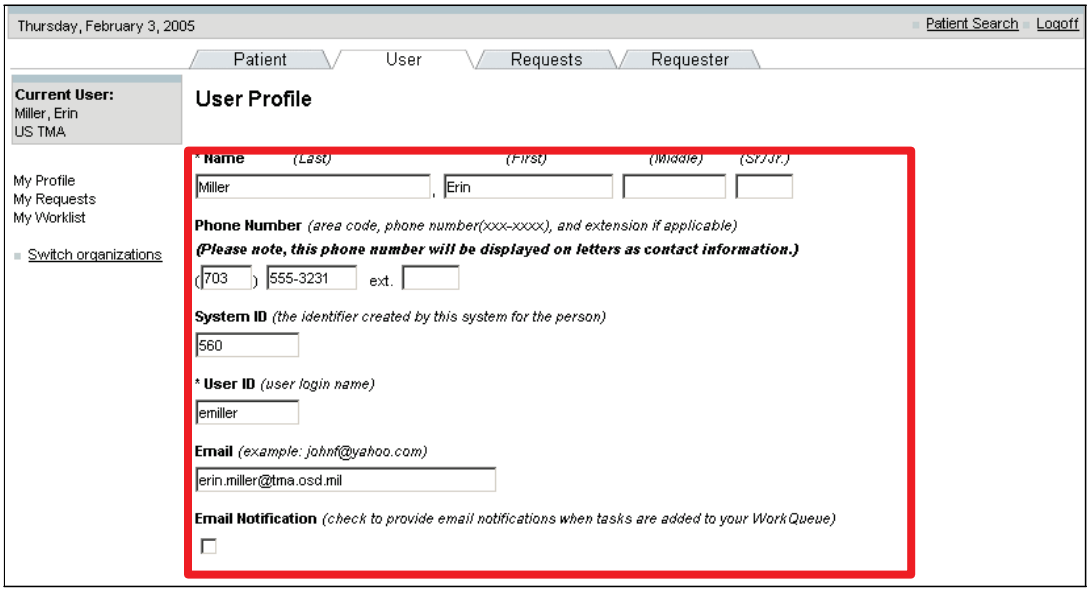
2. Select the My Profile hyperlink.



Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

3. Enter the updated information in the information fields.

   NOTE: You may update your name, phone number, email, password, signature block (ex. certification titles, educational titles), and add additional comments. You are not authorized to change the System ID or User ID, nor to access User Roles and User- to-User Relationships.

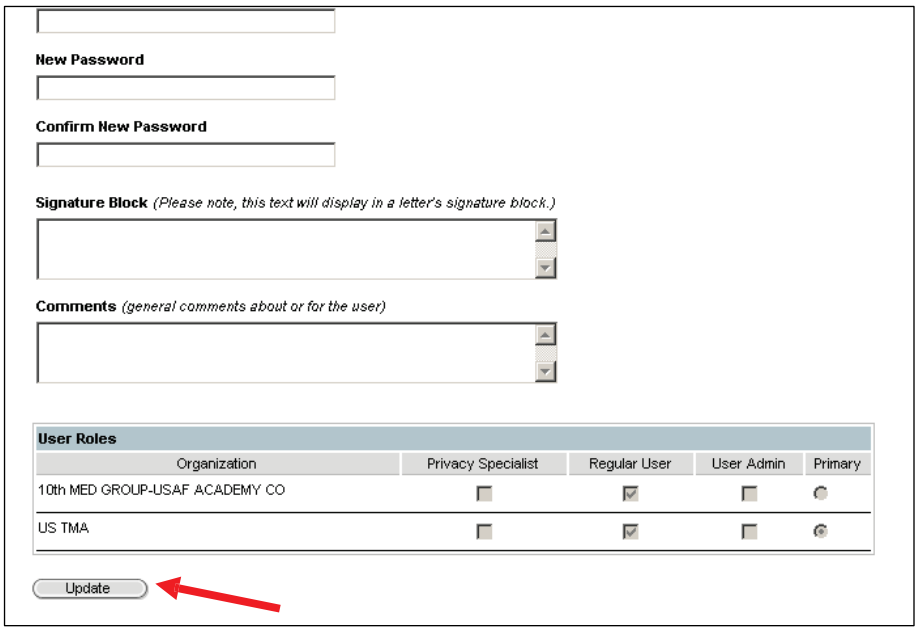


NOTE: All required fields are marked with an asterisk.

4. Scroll down to the bottom of the screen.

5. Click on the Update button.

- Your new information will appear in the appropriate fields.

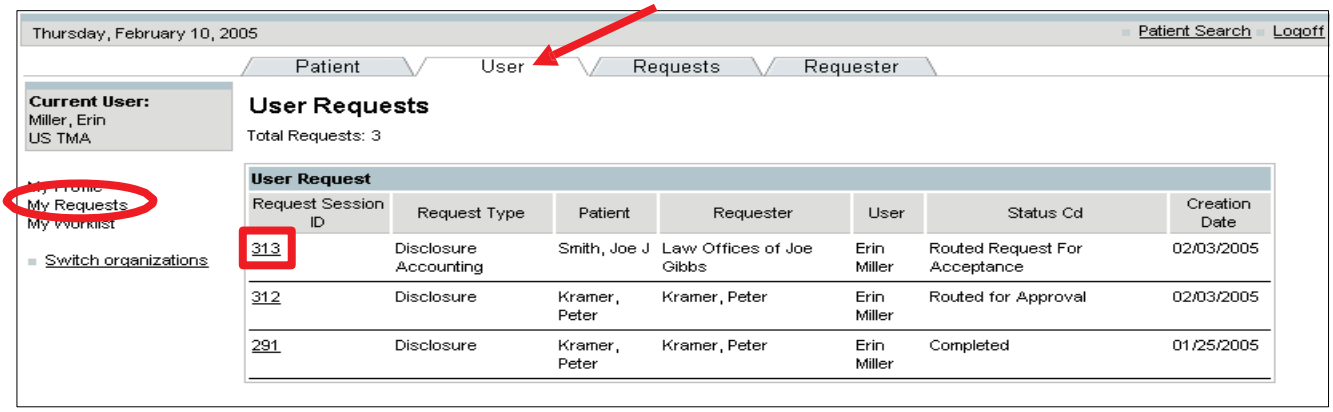


5.1.2 My Requests

NOTE: The My Requests hyperlink allows you to view the status of all requests that you have initiated.

To view your requests:

1. Select the User Tab.
2. Select the My Requests hyperlink.
3. Select the Request Session ID to view a specific request.



- A detailed summary of that particular request is displayed (as shown below).

NOTE: As a Regular User, you are not authorized to edit any information in the summary.

However, you can attach a document.

Thursday, February 10, 2005 Patient Search Logoff

Patient User Requests Requester

Current Request: Disclosure Accounting

Summary
History
Documents
Request Details
Request Action

Create New Request
Search for a Request

Edit Request

Request Activity History

Activity Instance ID	Request Session ID	Activity ID	Source	Patient Id	Requester Id	User	Status	Creation Date
390	313	Request Acceptance (Disclosure Accounting)		Smith, Joe J	Law Offices of Joe Gibbs	James Wilson	Action Pending	02/03/2005

Request Session Details Edit

Description	Details
Request Type	Disclosure Accounting
Details of the Request	requested by law firm
Start Date	08/10/2004
End Date	08/27/2004
Authority Verified	Requester has authorization
Verify Authority Text	requester has an authorization
Identity Verified	Patient Identifier
Verify Identity Text	identity verified
Route to Privacy Specialist	Yes
Request Classification	Life Insurance
Request Format	Received Request in Writing

Letters and Attached Documents Attach

ID	Date	Title

To attach a file to your request:

1. Click on the Attach button in the Letters and Attached Documents section.
2. Provide the document information.
3. Click on the Save button.

Thursday, February 10, 2005 Patient Search Logoff

Patient User Requests Requester

Current Request: Disclosure Accounting

Summary
History
Documents
Request Details
Request Action

Create New Request
Search for a Request

Attach File

You may attach any document, with file size not exceeding 2M

Document Title *(enter this document's title)*

Please select a file you wish to attach

Browse...

Save

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

5.1.3 My Worklist

NOTE: The My Worklist hyperlink allows you to view all tasks currently assigned to you. This feature serves as an electronic inbox.

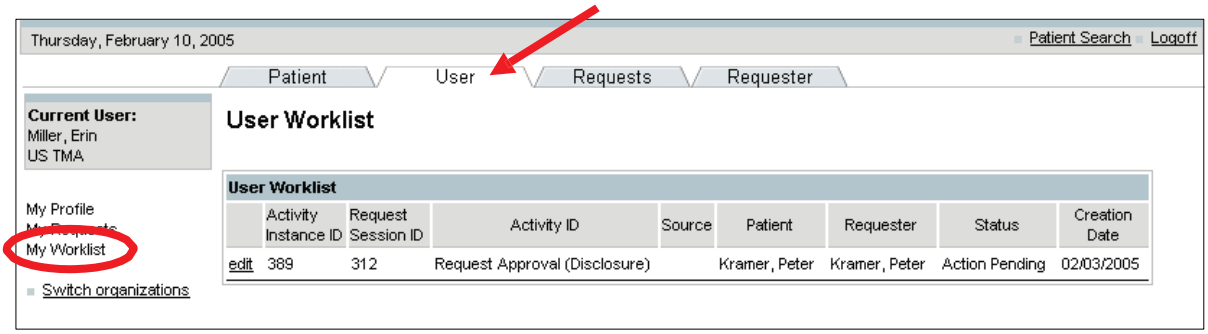
To view tasks in your worklist:

1. Select the User Tab

2. Select the My Worklist hyperlink.

- The Regular User can view and process all requests that have tasks currently assigned to them.

NOTE: To process a request, select that request and perform the action or route it for approval or denial.



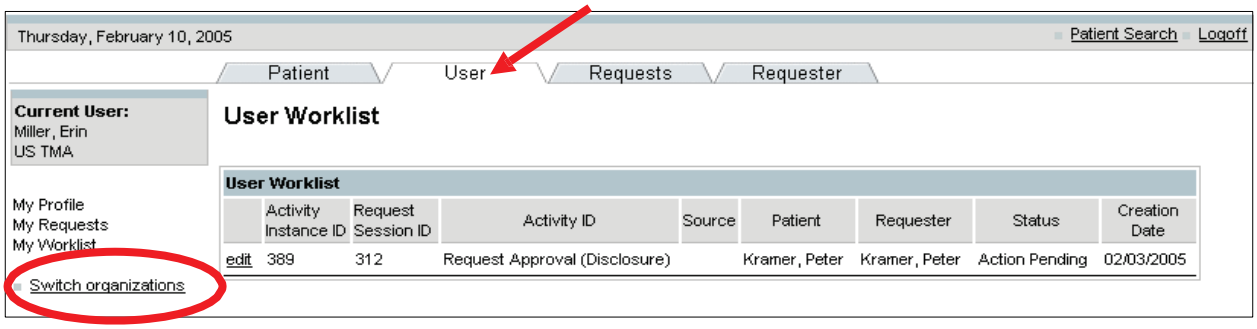
5.1.4 Switch Organizations

NOTE: The Switch Organizations hyperlink allows you to change your primary status between organizations, if you are assigned to more than one organization.

To switch between organizations:

1. Select the User Tab.

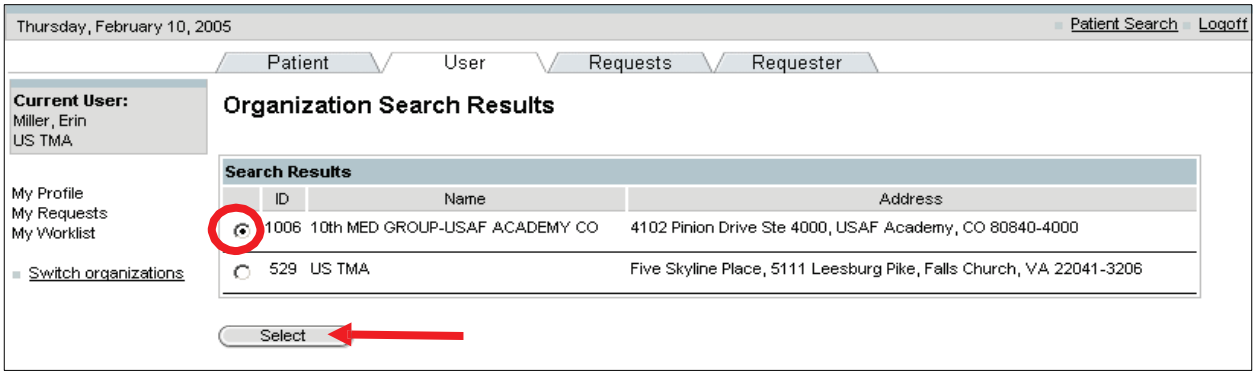
2. Select the Switch Organizations hyperlink.



Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

3. Select the new organization.

4. Click on the Select button.



5.2 PATIENT TAB ACTIVITIES

The Patient tab contains hyperlinks that allow you to perform patient-specific activities. These hyperlinks include:

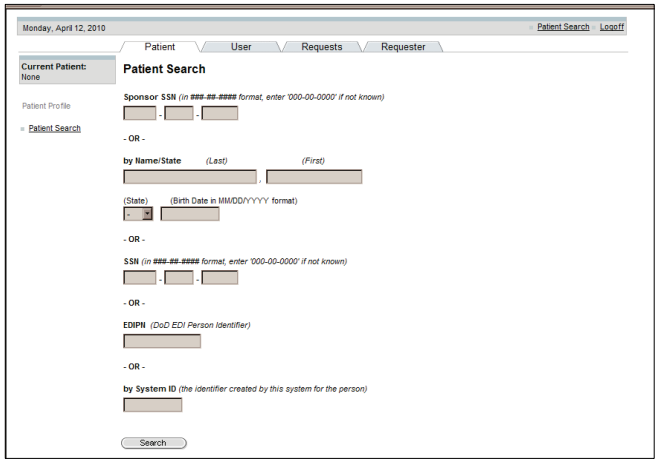
- Patient Profile
- Patient search

5.2.1 Patient Search

NOTE: The Patient Search hyperlink allows you to look for a particular patient in the PHIMT database.

To search for a patient:

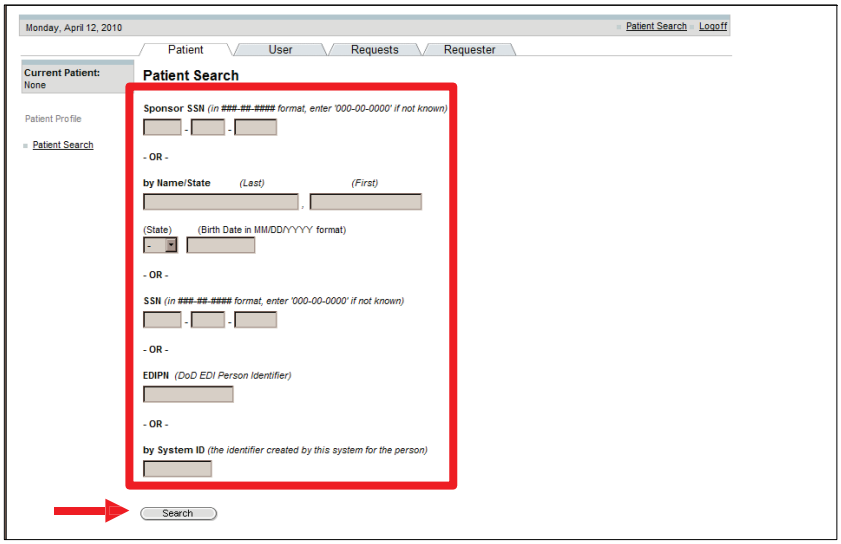
1. Select the Patient Tab.



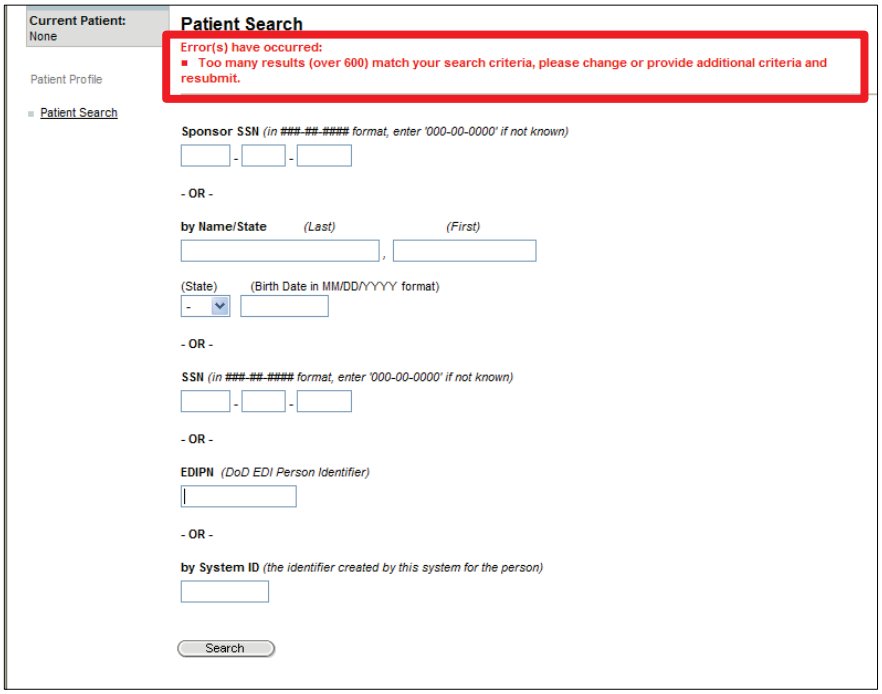
Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

2. Enter the Search Criteria (You can search for a patient by the Sponsor's SSN, by the patient's name/state, SSN, EDIPN or System ID).

3. Click on the Search button.



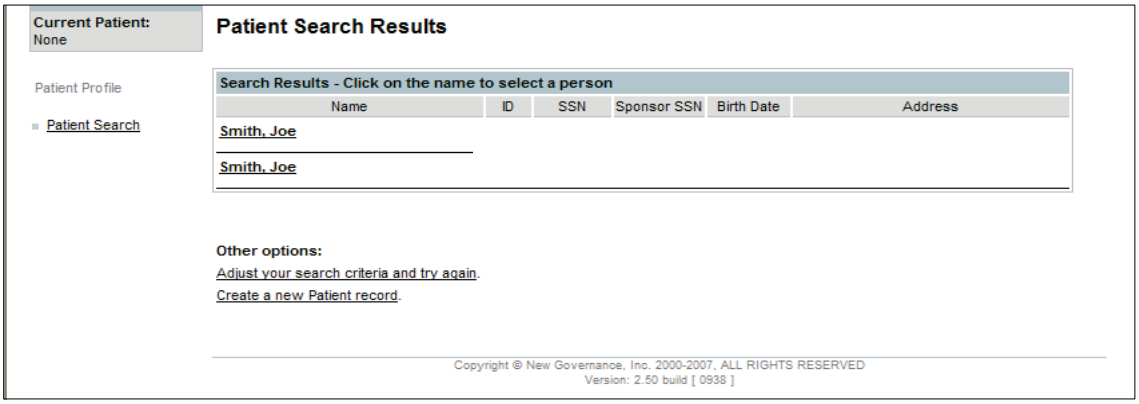
NOTE: The search limitation within the PHIMT is 600 records. This means that if your search results in over 600 records, you will have to narrow your search.



- Enter additional search criteria (if applicable)

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

- The Search Results screen will display.



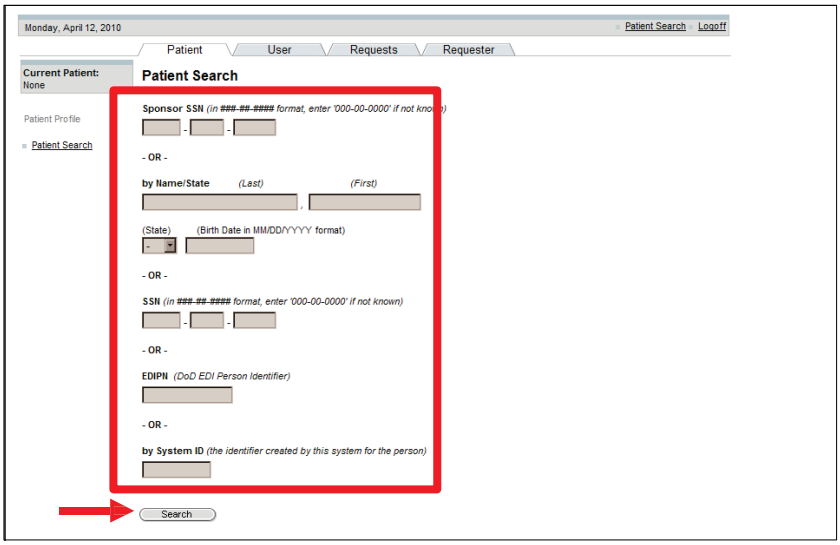
Since the MDR data has been added to the PHIMT, the instances where a patient will need to be added before entering a disclosure will be infrequent. If a patient does not exist in the PHIMT database or the MDR data, then the User must add a patient record. New patient records cannot be created without first searching the database. The Create a new Patient record hyperlink allows you to enter information for a new patient into the PHIMT database.

To add a patient record:

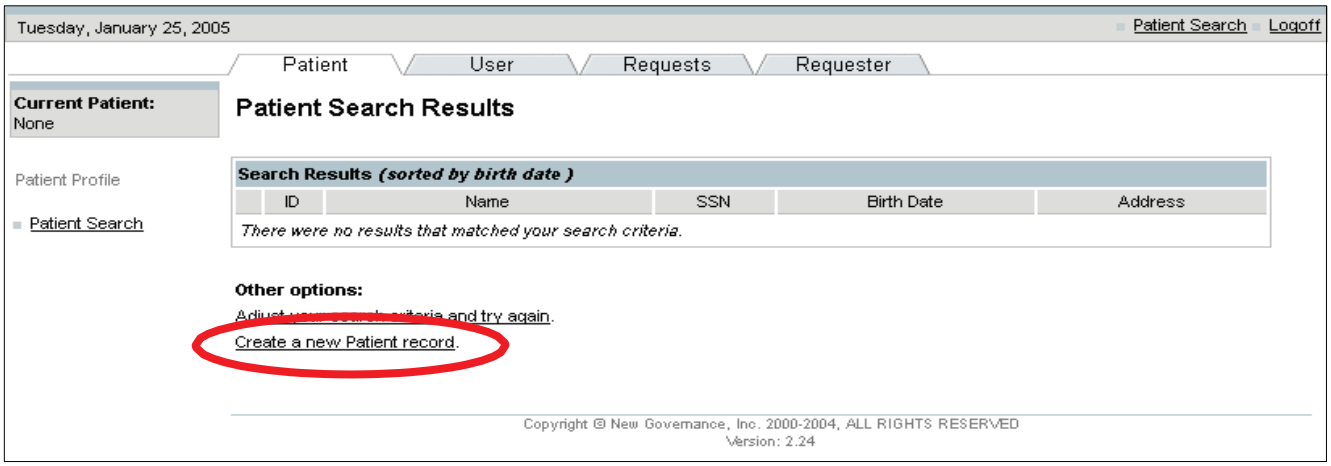
1. Select the Patient Tab.

2. Enter the Search Criteria (You can search for a patient by the Sponsor's SSN, by the patient's name/state, SSN, EDIPN or System ID).

3. Click on the Search button.



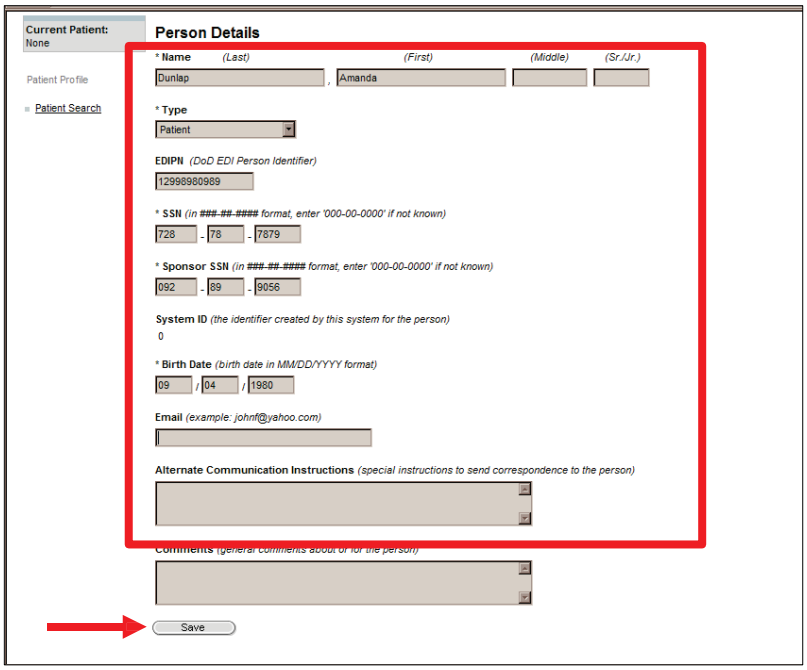
4. If no results matched your search, select the Create a new Patient record hyperlink.



5. Enter the patient's information: name, type, EDIPN, SSN, Sponsor SSN, birth date, email.

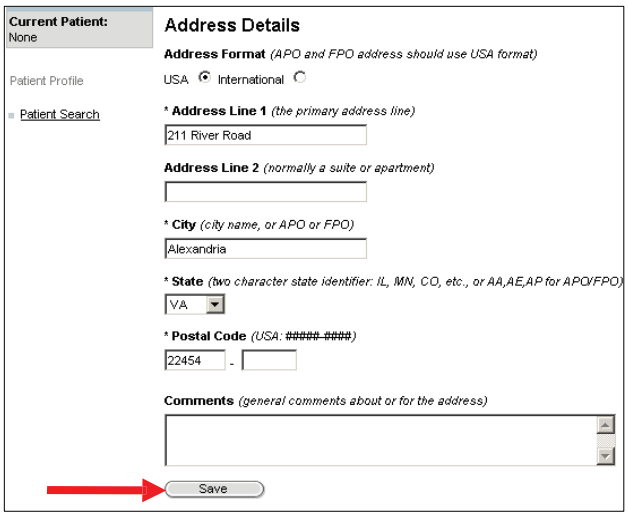
NOTE: All required fields are marked with an asterisk.

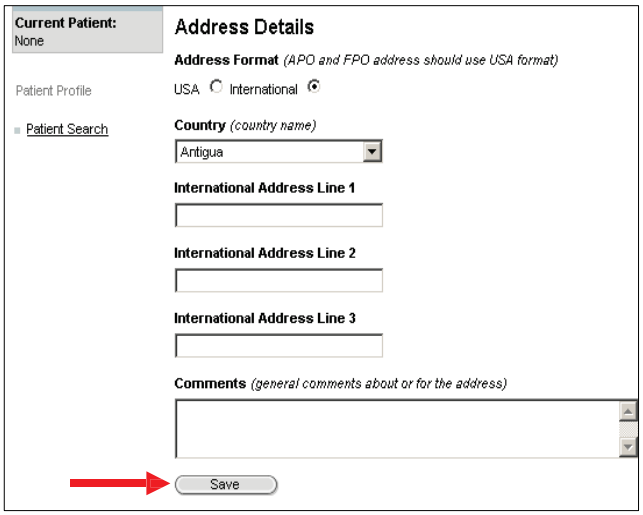
6. Click on the Save button.



7. Enter the Address Details (USA or International format).

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.





8. Click on the Save button.

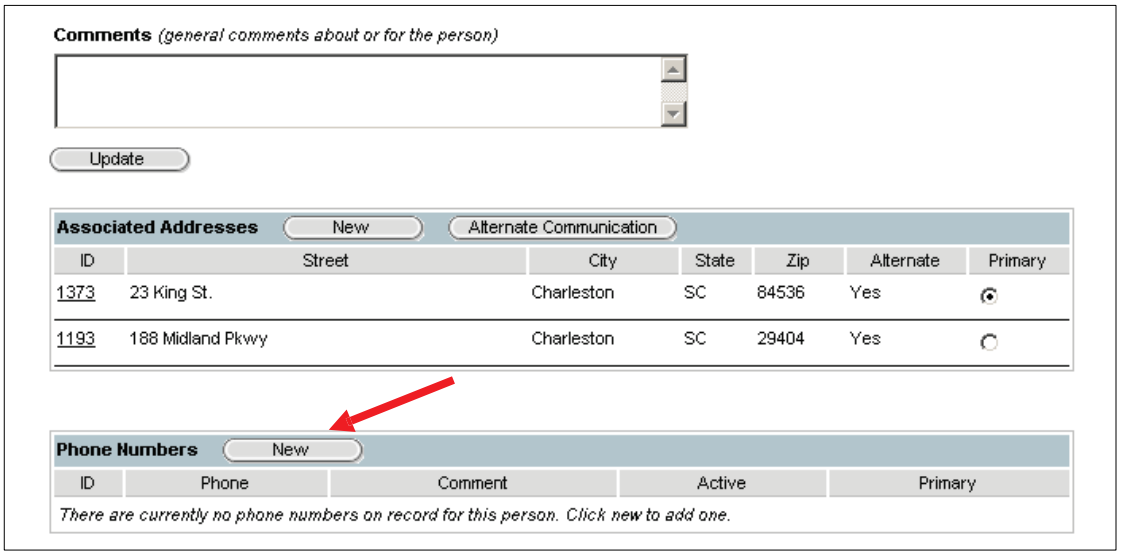
5.2.3 Create an Alternative Phone Number

Individuals have the right to request an alternative telephone number for receiving communications related to their PHI. An alternative telephone number can be created by Regular Users and Privacy Specialists.

To create an alternative telephone number:

1. Scroll to the bottom of the Patient Details screen.

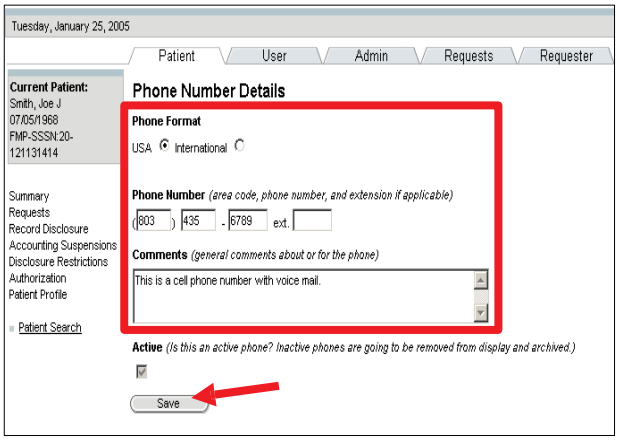
2. Click on the New button next to Phone Numbers.

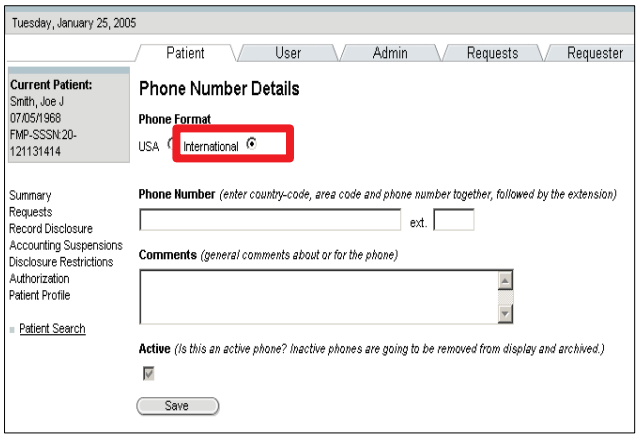


- The Phone Number Details screen will display (choose the USA or International format).

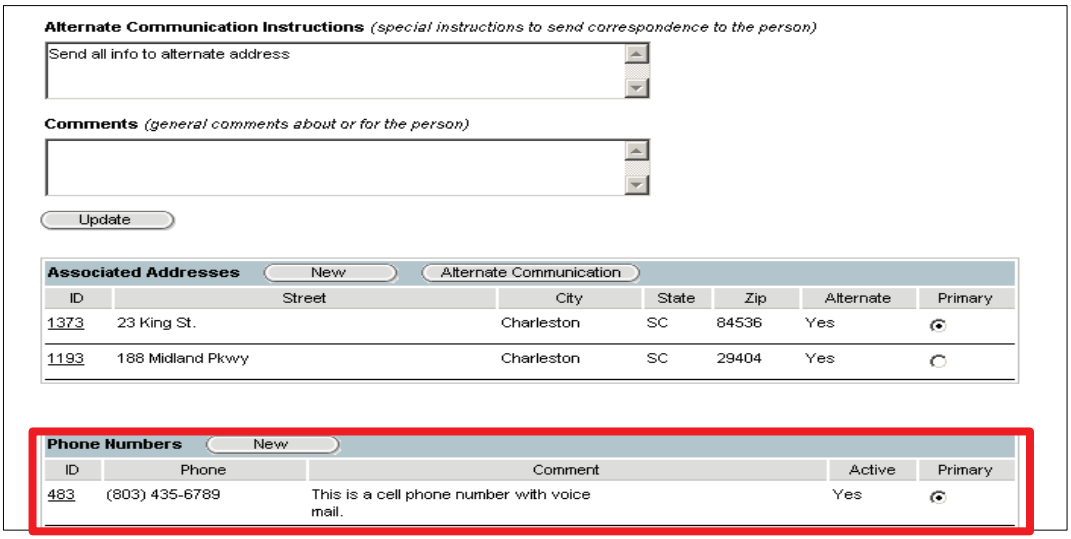
3. Enter the phone number and enter any comments.

4. Click on the Save button.





- The phone number you added will appear on the Patient Details screen.



5.3 REQUESTS TAB ACTIVITIES

The Requests tab allows you to access information about the activities requested by an individual or an organization. Requests tab activities include:

- Record Disclosure Requests
- Record an Accounting of Disclosure Request
- Record Simple Disclosure Requests

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

5.3.1 Record a Disclosure Request

NOTE: The Record Disclosure hyperlink allows you to record or document the release of PHI. This activity consists of five disclosure phases: patient selection, requester selection, detailed request, disclosure details, and request action.

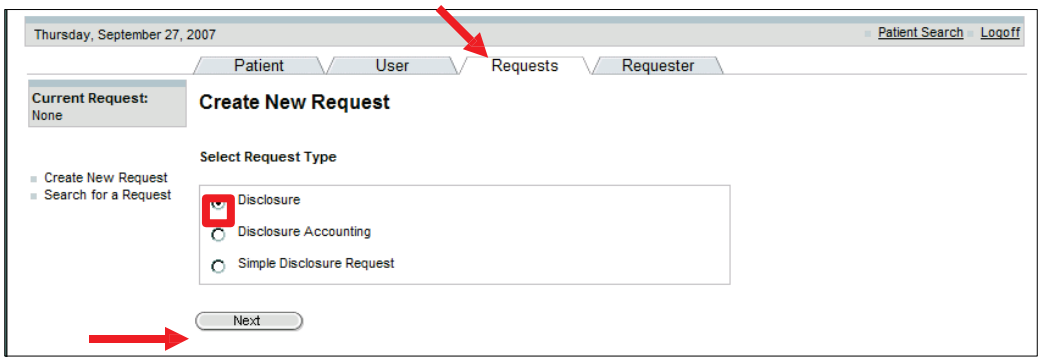
Disclosure requests allow you to forward it to a Privacy Specialist for approval or denial. Disclosure status will be set to Pending because as a Regular User, you are not authorized to approve disclosures. Entering the requested action allows you to route the disclosure request to your own worklist for further research or route to a Privacy Specialist.

To record a request for disclosure:

1. Select the Requests Tab.

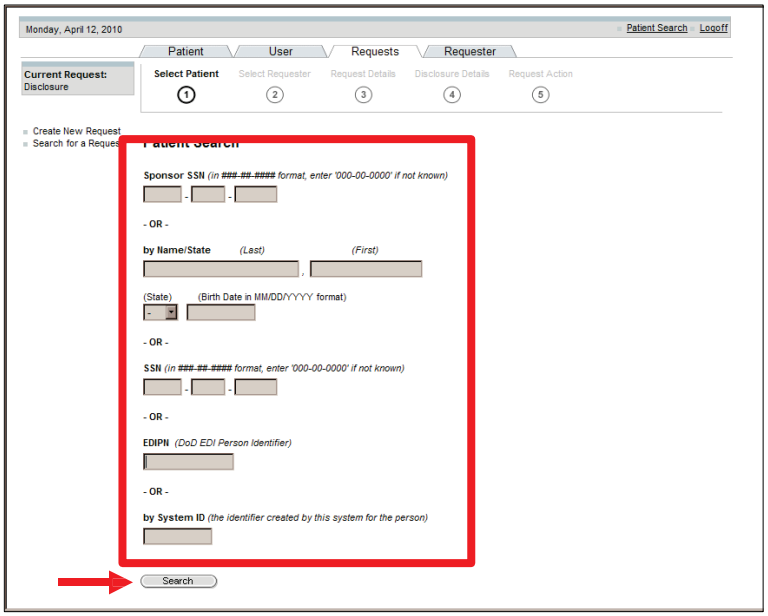
2. Click on the Disclosure radio button.

3. Click on the Next button.



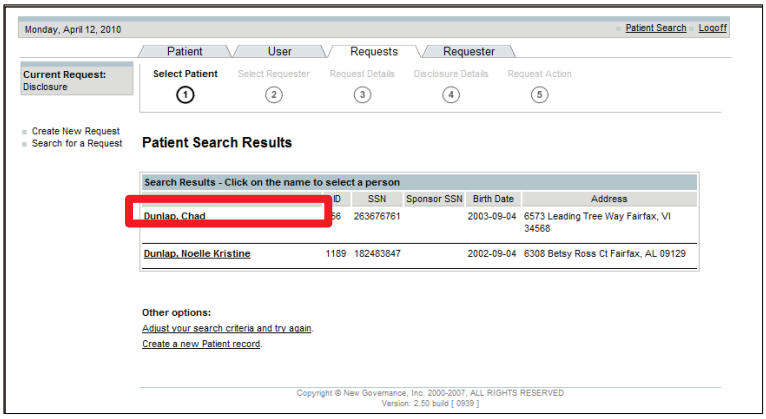
4. Enter the patient search criteria. (You can search for a patient by the Sponsor's SSN, by the patient's name/state, SSN, EDIPN or System ID).

5. Click on the Search button.

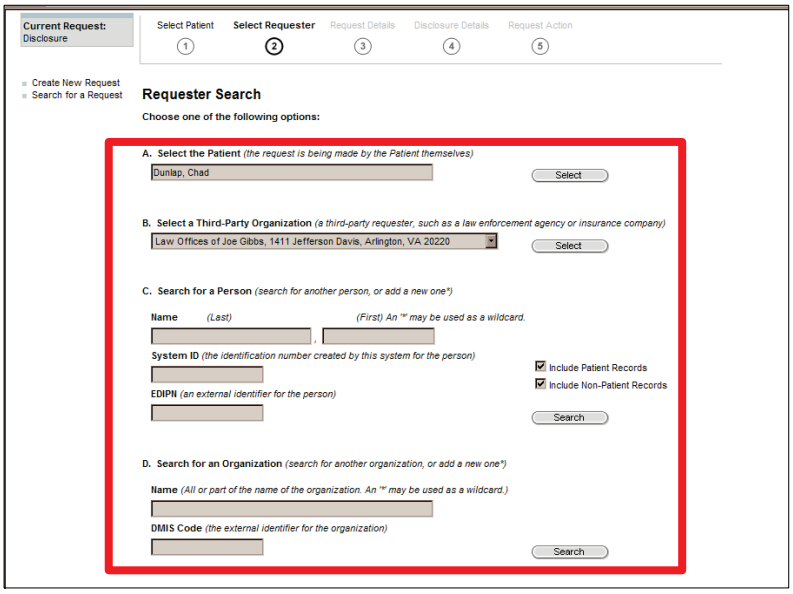


NOTE: If there were no results that matched your search criteria, you may select from two options: Adjust your search criteria and try again OR Create a new Patient record.

6. Select the correct patient by clicking on the name hyperlink.



- The Requester Search screen will appear.

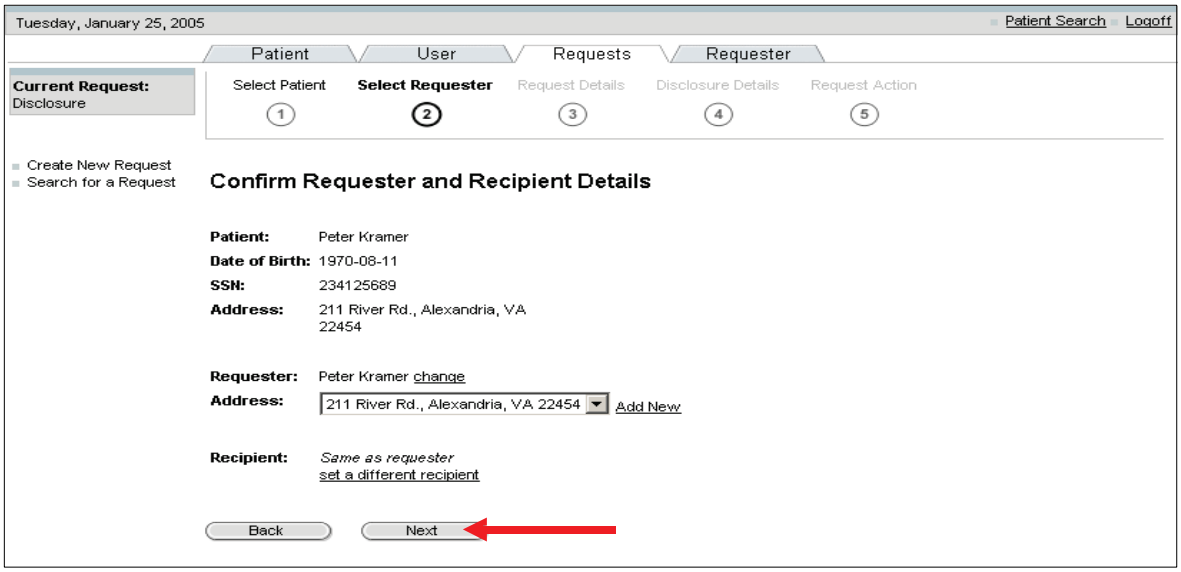


7. Enter the data into the information fields to search by patient, third party organization, person, or organization. (Complete only one field).

8. Click Select or Search (for that field).
   Example: If the request is being made by the patient themselves, click on the Search button next to the patient's name.

9. Confirm Requester and Recipient Details. Verify and/or enter the data into the information fields.

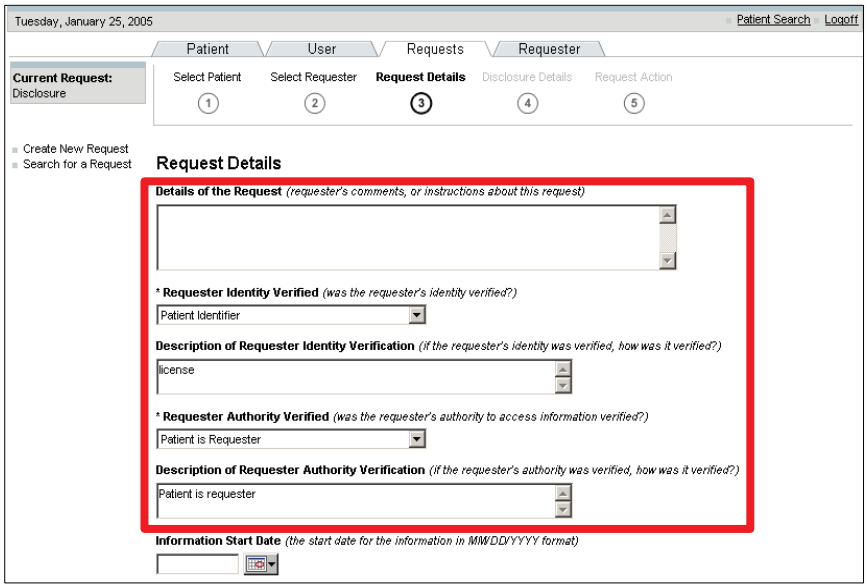
10. Click on the Next button.



Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

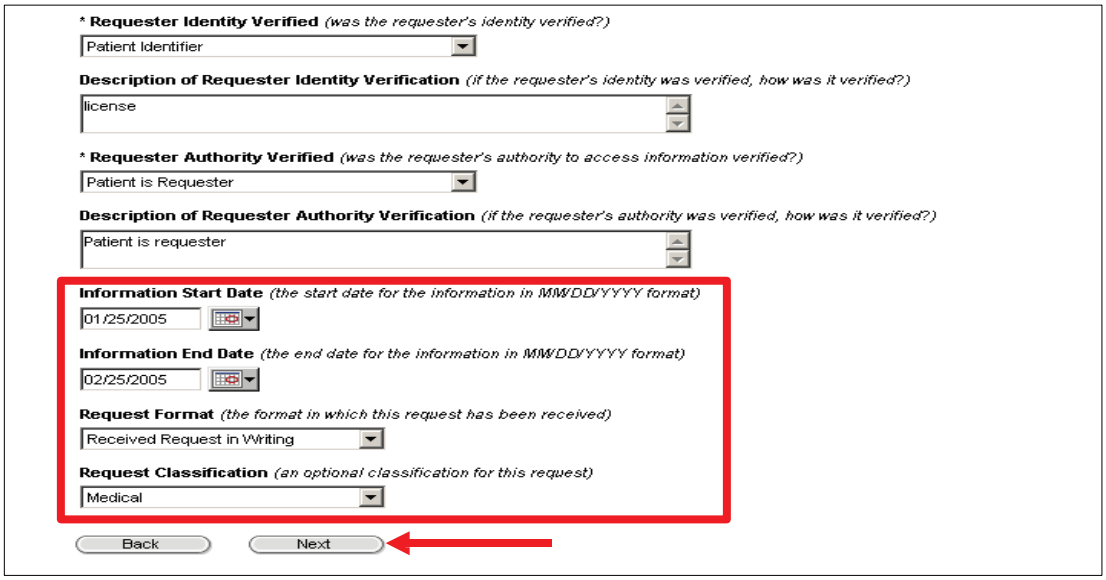
11. Enter the Request Details: details of the request, identity verification, and authority verification.

NOTE: All required fields are marked with an asterisk.



12. Scroll down the screen and enter: Information start and end date, request format, and request classification.

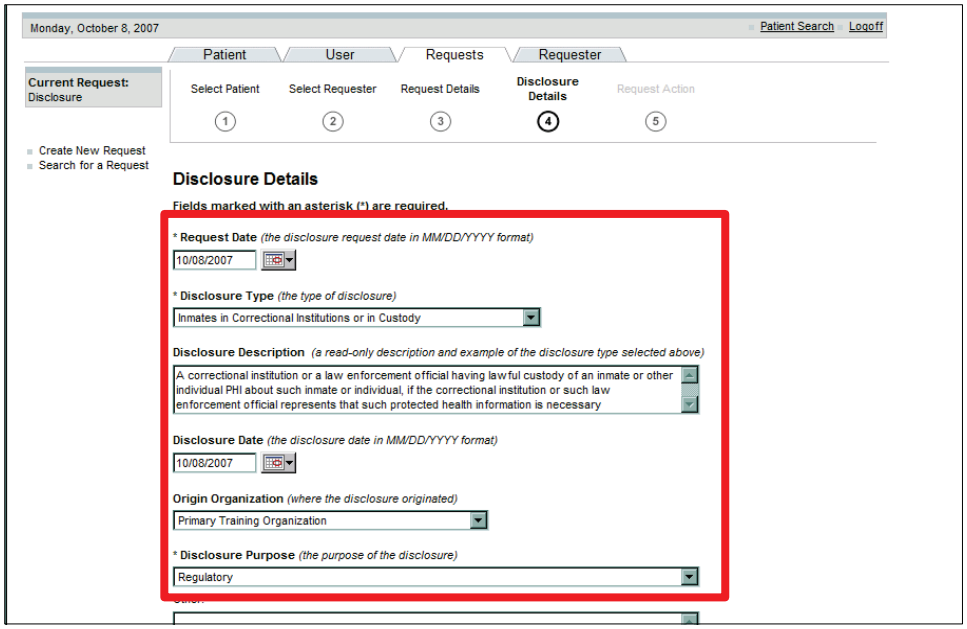
13. Click on the Next button.



Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

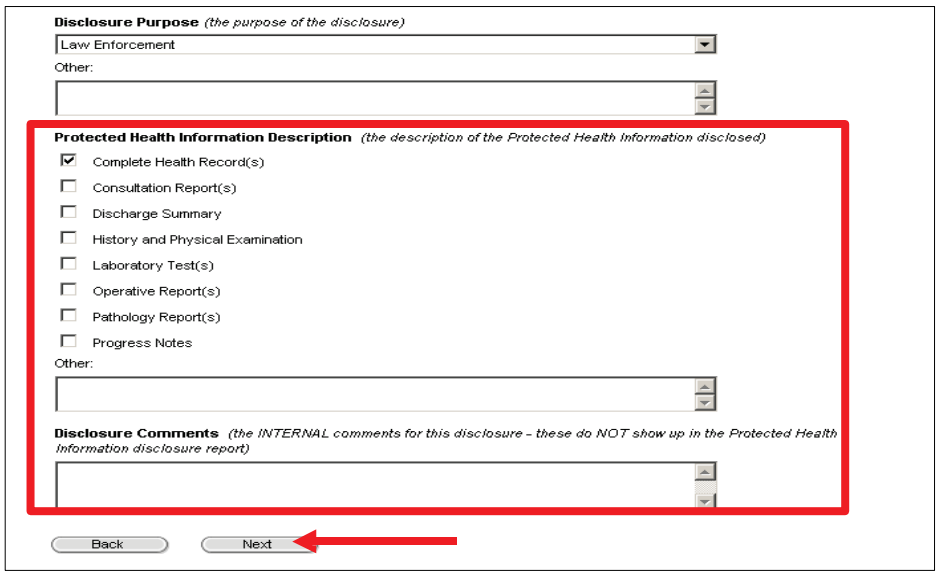
14. Enter the Disclosure Details: Request date, disclosure type, origin organization and disclosure purpose.

NOTE: The Disclosure description will be automatically populated once a disclosure type is selected.



15. Scroll down the screen and enter: PHI description and disclosure comments.

16. Click on the Next button.

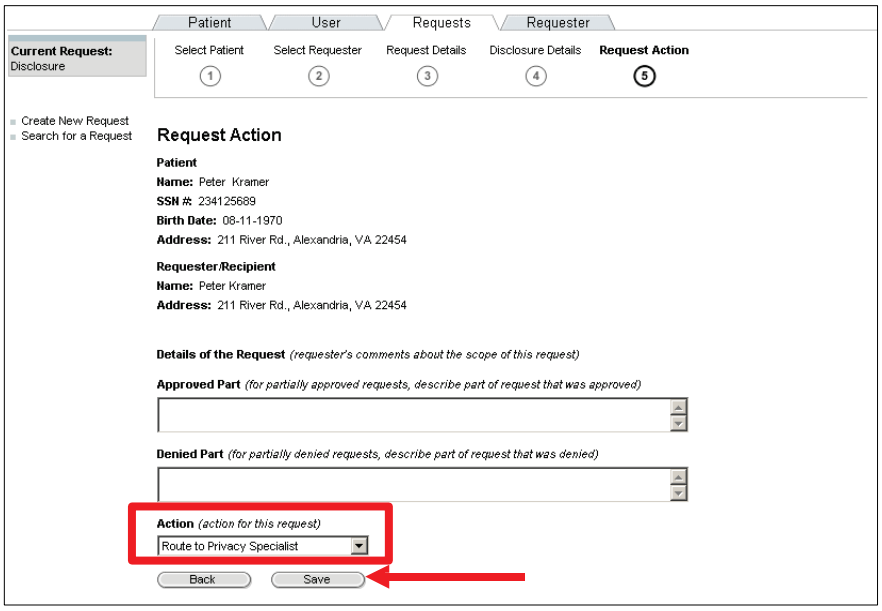


17. Enter the Request Action Details.

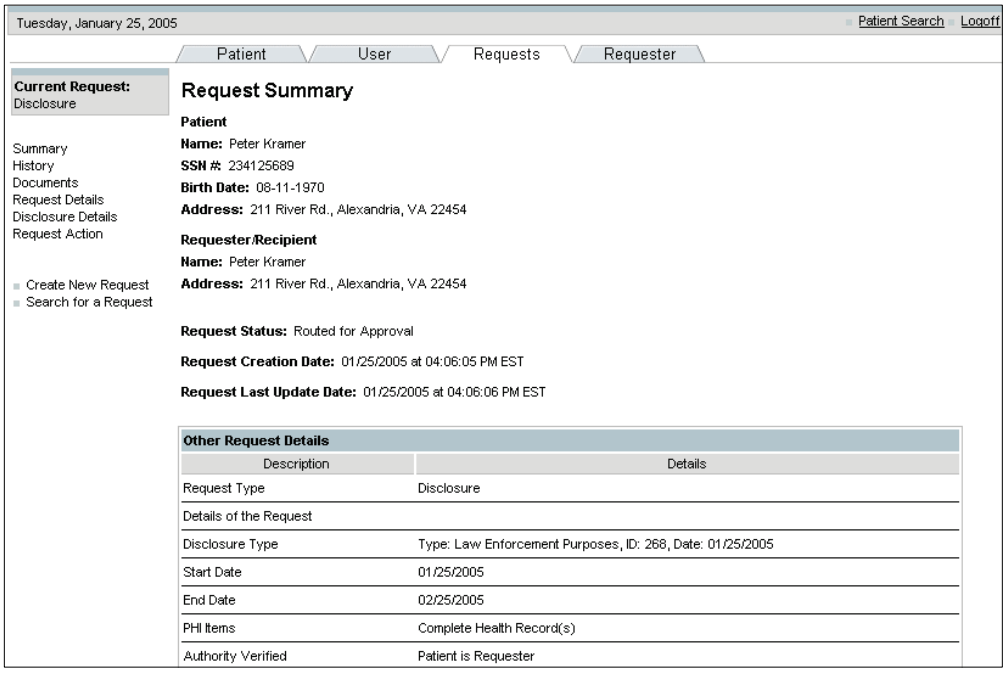
Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

18. From the Action drop-down menu, select the appropriate routing option (Privacy Specialist).

19. Click on the Save button.



- The Disclosure Request Summary will display.



Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

5.3.2 Update Patient Address

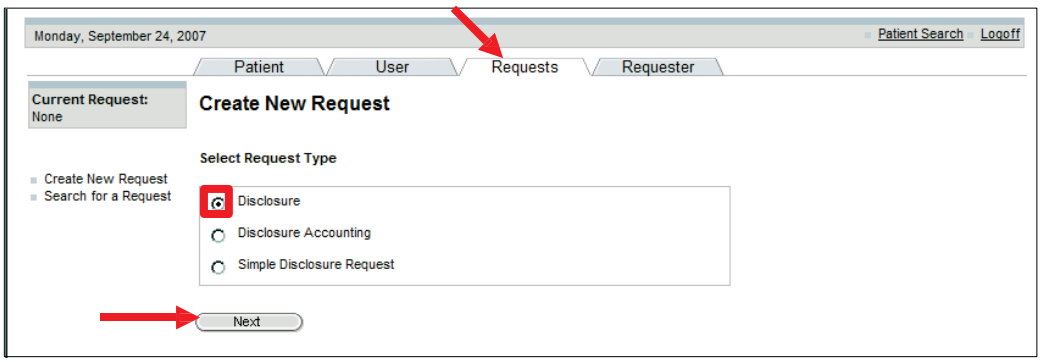
For a disclosure to be valid, a patient's address must be entered. The Regular User can update the patient's address in the middle of a disclosure request.

To update the patient's address:

1. Select the Request Tab.

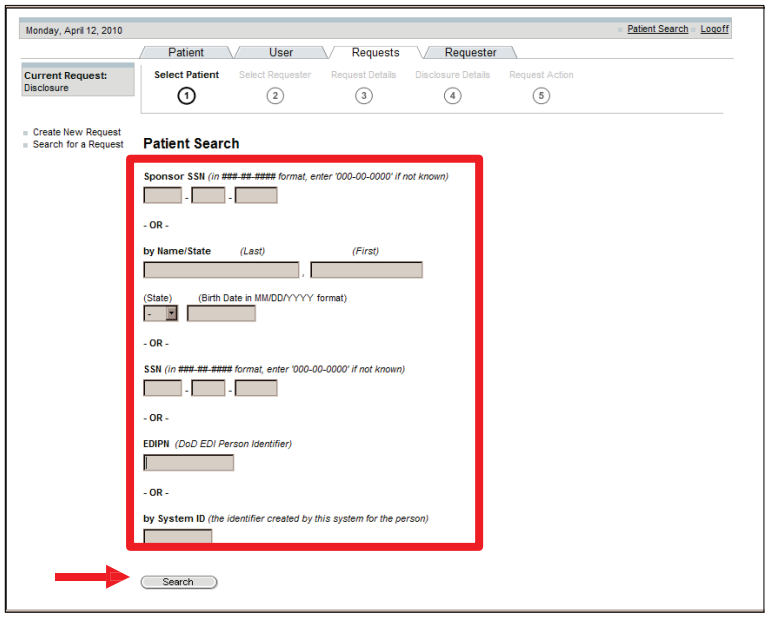
2. Click the Disclosure radio button.

3. Click on the Next button.



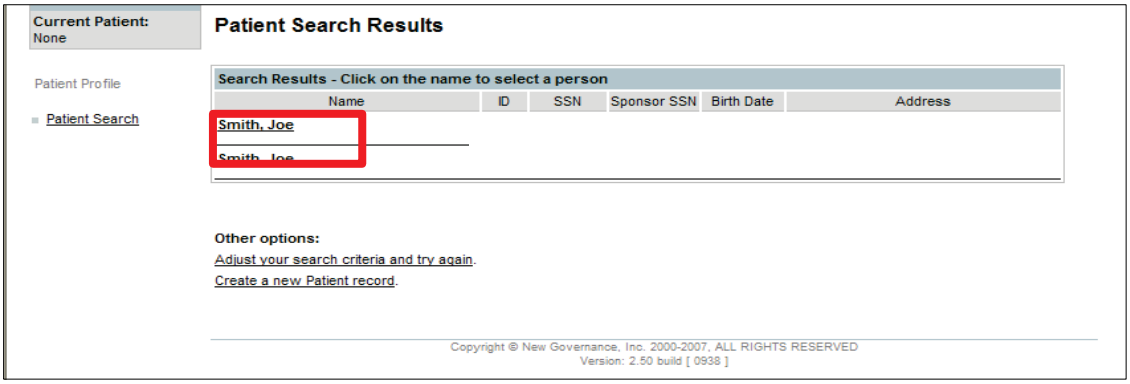
4. Enter the patient search criteria. (You can search for a patient by the Sponsor's SSN, by the patient's name/state, SSN, EDIPN or System ID).

5. Click on the Search button.



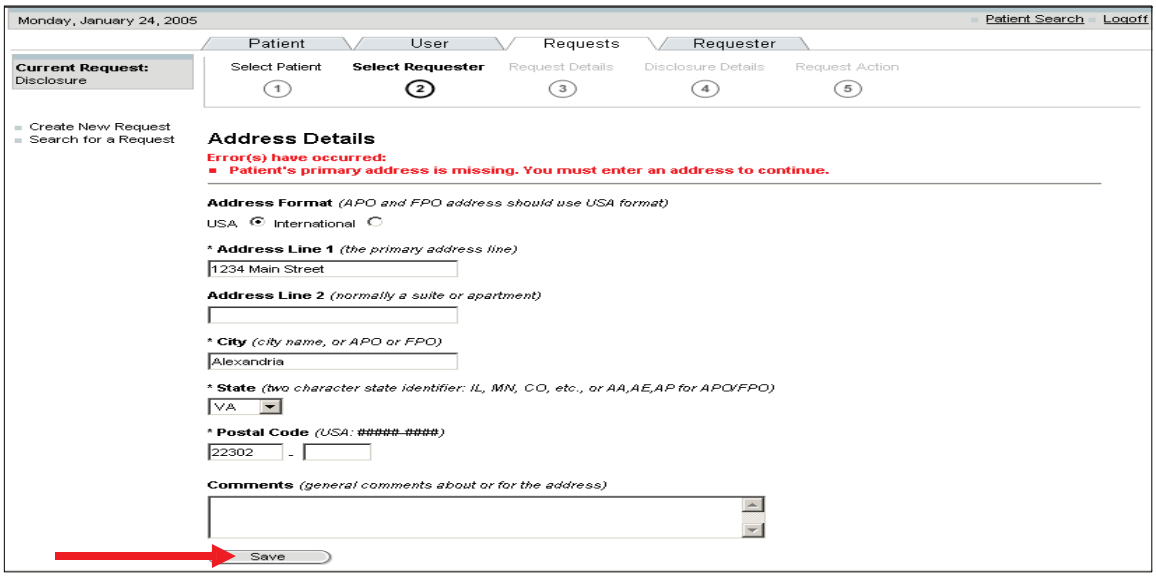
- If the patient does not have an address entered in the tool, "Primary Address not selected" will be listed next to the patient's name.

6. Select the patient.



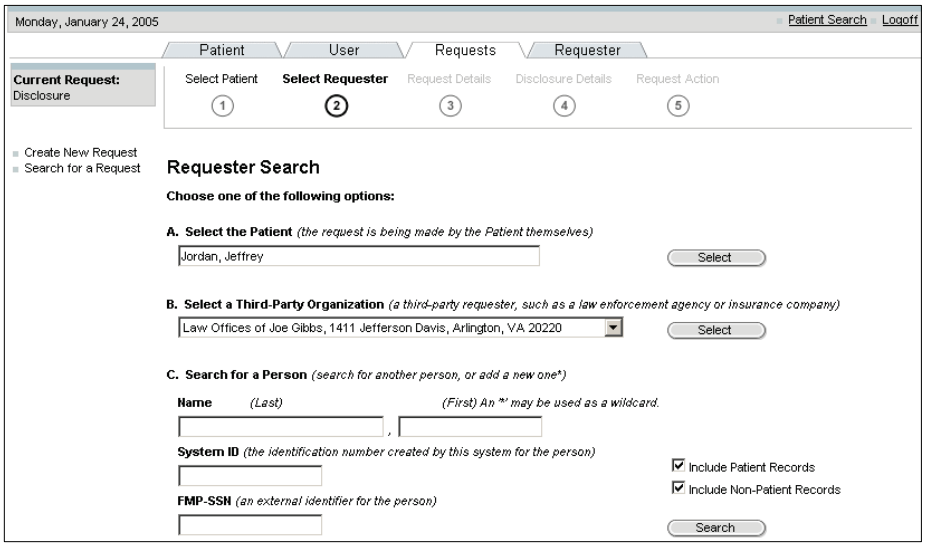
7. Enter the patient's address.

8. Click on the Save button.



- After saving the address, you can continue with the Disclosure Request where you left off.

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.



- The Request Summary for that person will be displayed.

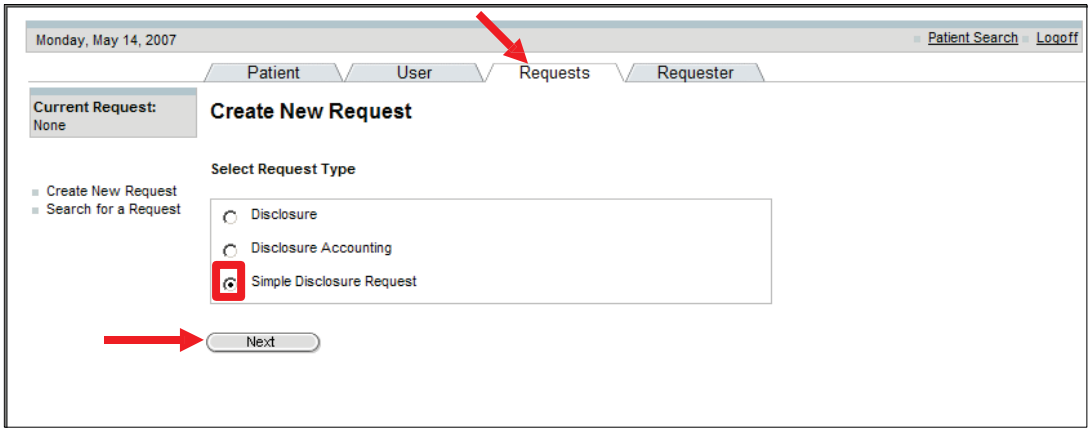
5.3.3 Record a Simple Disclosure Request

A Simple Disclosure Request provides the ability for Multiple Disclosure Accounting. A covered entity may account for multiple disclosures with a single entry if the MTF has made multiple disclosures of PHI to the same person or entity for a single purpose. Some examples include: a series of disclosures that occur on a periodic basis such as monthly medical readiness status, dental class reports, or pre-deployment preparation reports to a commander or the commander's designee(s). Multiple disclosure is primarily used when the same disclosure occurs in a specific time period. This will allow for better tracking of multiple disclosures and Users will not have to create separate single disclosures.

1. Click on the Requests Tab.

2. Click on the Simple Disclosure Request radio button.

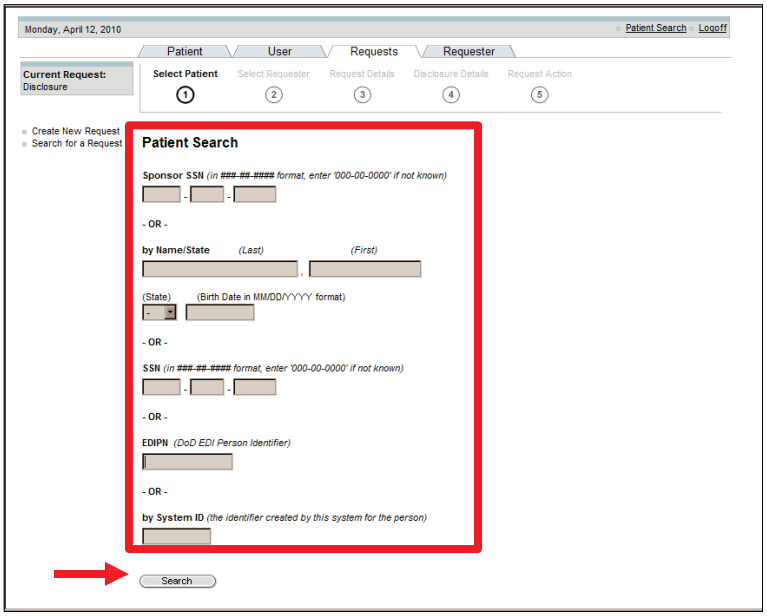
3. Click the Next button.



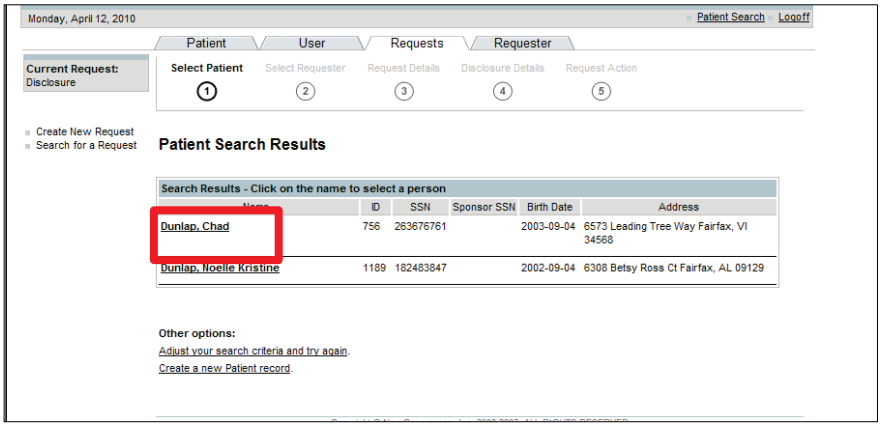
Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

4. Enter the patient search criteria. (You can search for a patient by the Sponsor's SSN, by the patient's name/state, SSN, EDIPN or System ID).

5. Click on the Search button.



6. Select patient from the Patient Search Results screen.



7. Click on the Multiple Disclosures for the same Purpose radio button. (The disclosure frequency was added to differentiate between single and multiple disclosures. It is defaulted to single).

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

Create New Request
Search for a Request

Disclosure Details

Fields marked with an asterisk (*) are required.

* **Patient** *(the Patient to whom the disclosure applies)*
Name: Dhel Test
SSN #: 108693548
Birth Date: 10/28/1930
Address: Ahruntep1277 Vinton, VA 24179-1036

* **Disclosure Frequency** *(the frequency, periodicy, or number of disclosures made)*
Single Disclosure Multiple Disclosures for the same Purpose

* **Requester** *(the organization or person requesting the disclosure)* Change
Name:
Address:
Phone:
Contact Person:

- The Disclosure Frequency fields will appear.

8. Select the occurrence, start date, and end date. (Users can select from the drop-down menu, which includes: weekly, monthly, or annually, or they have the option to put how many times the disclosure occurs in a specified time period.)

9. Click on the Change button.

Create New Request
Search for a Request

Disclosure Details

Fields marked with an asterisk (*) are required.

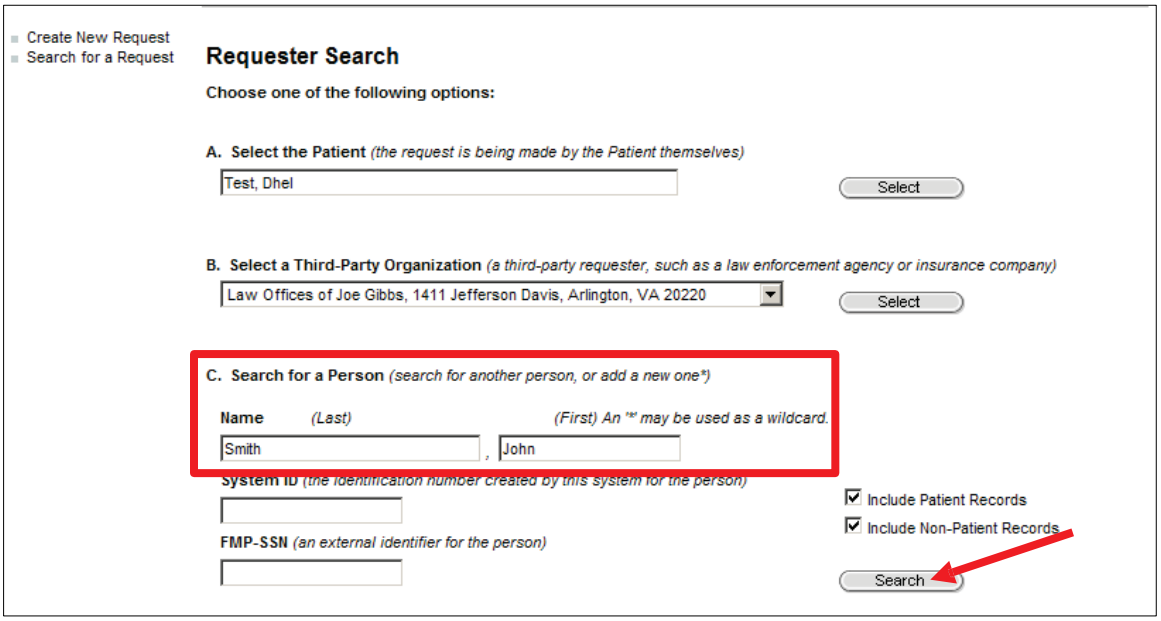
* **Patient** *(the Patient to whom the disclosure applies)*
Name: Dhel Test
SSN #: 108693548
Birth Date: 10/28/1930
Address: Ahruntep1277 Vinton, VA 24179-1036

* **Disclosure Frequency** *(the frequency, periodicy, or number of disclosures made)*
Single Disclosure Multiple Disclosures for the same Purpose
Occurs once Weekly or 0 times from 05/14/2007 to 06/14/2007

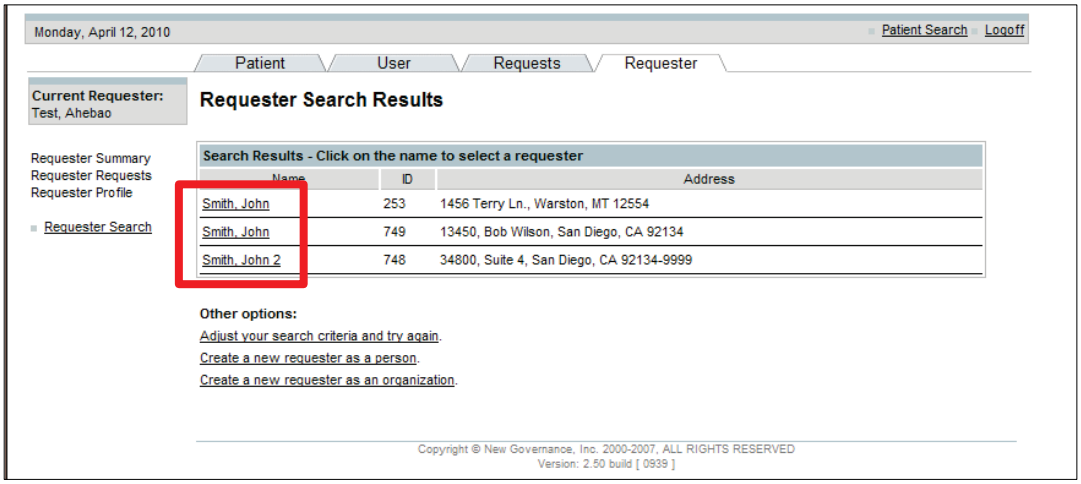
* **Requester** *(the organization or person requesting the disclosure)* Change
Name:
Address:
Phone:
Contact Person:

10. Select the Requester: either a) select by the default patient or third party organization or b) enter the information into the data entry fields, to search by person or organization. Complete only one field.

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

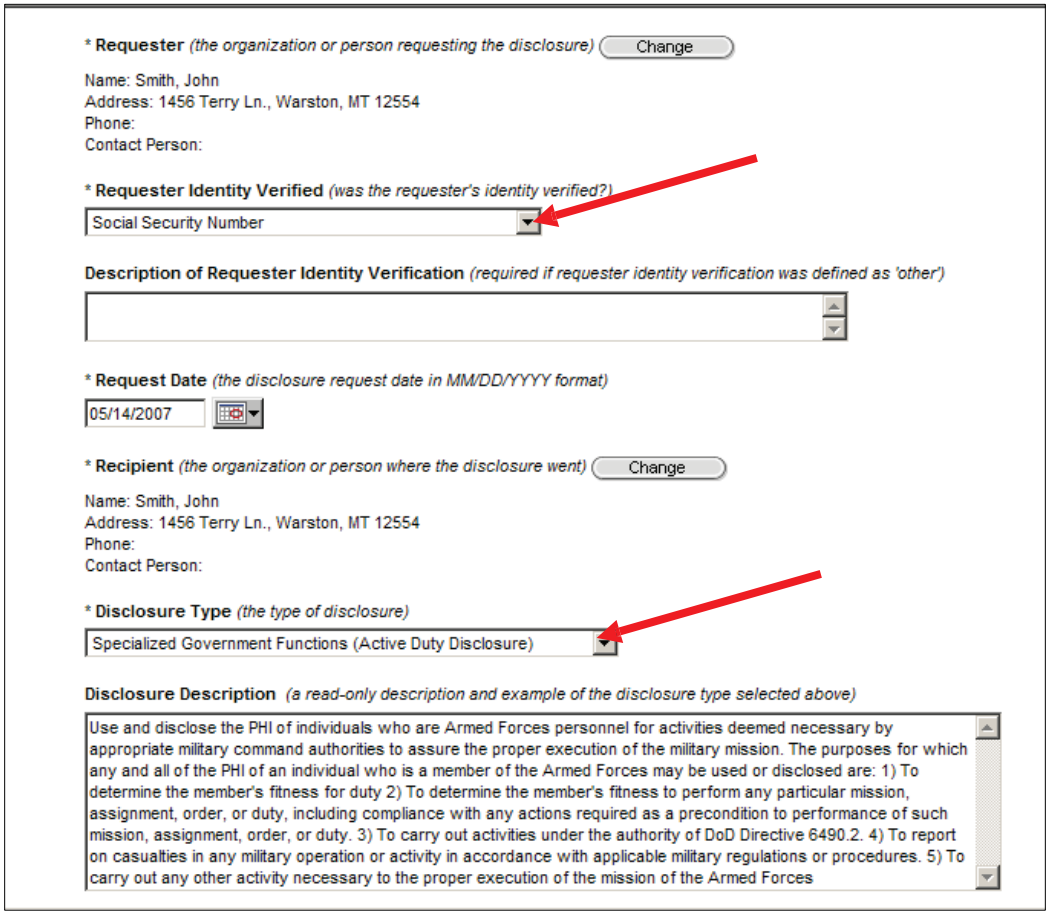


11. Confirm the requester details. Click the Search button and/or Select the Requester.



12. Select the Requester Identity Verified and Disclosure Type from their respective drop-down menus.

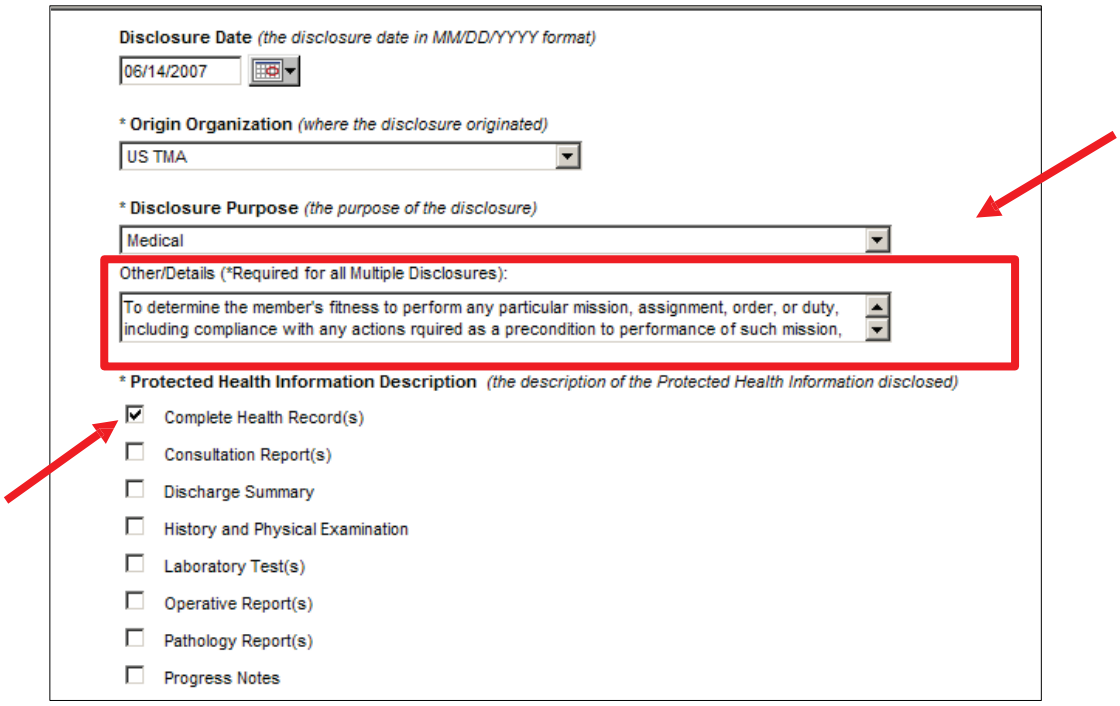
NOTE: The Disclosure description will be automatically populated once a disclosure type is selected.



13. Select the Disclosure Purpose from the drop-down menu.

14. Enter the data into the "Other/Details" text box. (For multiple disclosures, the purpose details box must be filled in for the disclosure to be complete.)

15. Scroll down the screen and enter: Protected Health Information Description and Disclosure Comments.



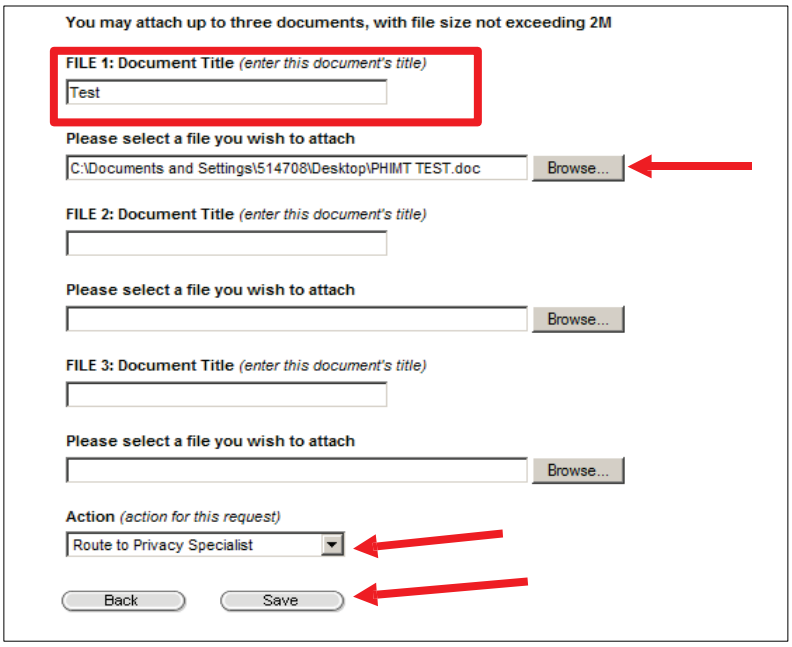
If you need to attach a document to the disclosure request, follow these steps:

16. Enter the document title. (If applicable)

17. Click on the browse button to attach the document. (If applicable)

18. Select Route to Privacy Specialist from the Action drop-down menu.

19. Click on the Save button.



Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

- The Request Summary screen will display.

Monday, May 14, 2007 Patient Search Logoff

Patient User Requests Requester

Current Request: Simple Disclosure Request

Summary
History

Create New Request
Search for a Request

Request Summary

Patient
Name: Dhel Test
SSN #: 108693548
Birth Date: 10-28-1930
Address:

Requester/Recipient
Name: John Smith
Address: 1456 Terry Ln., Warston, MT 12554

Request Status: Routed for Approval

Request Creation Date: 05/14/2007 at 03:51:49 PM EDT

Request Last Update Date: 05/14/2007 at 03:51:49 PM EDT

Other Request Details

Description	Details
Request Type	Simple Disclosure Request
Disclosure Type	Type: Specialized Government Functions (Active Duty Disclosure), ID: 676, Date: 06/14/2007
Route to Privacy Specialist	Yes
Identity Verified Text	Social Security Number

5.3.4 Record an Accounting of Disclosures Request

NOTE: The Disclosure Accounting hyperlink allows you to process a request for a report of all disclosures that have been made for a particular patient. This activity consists of four accounting of disclosure phases: Patient Selection, Requester Selection, Request Details, and Request Action.

A patient may ask for an accounting of disclosures at any time. PHIMT allows for a quick reporting of this information.

NOTE: Request Action allows you to route the request to your Privacy Specialist for approval or denial or to your own worklist if you need to research it further.

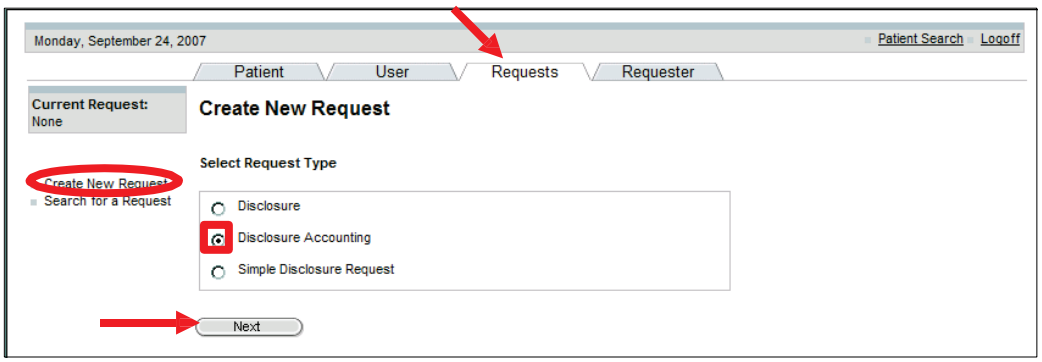
To record a request for an accounting of disclosures:

1. Select the Requests Tab.

2. Select the Create New Request hyperlink.

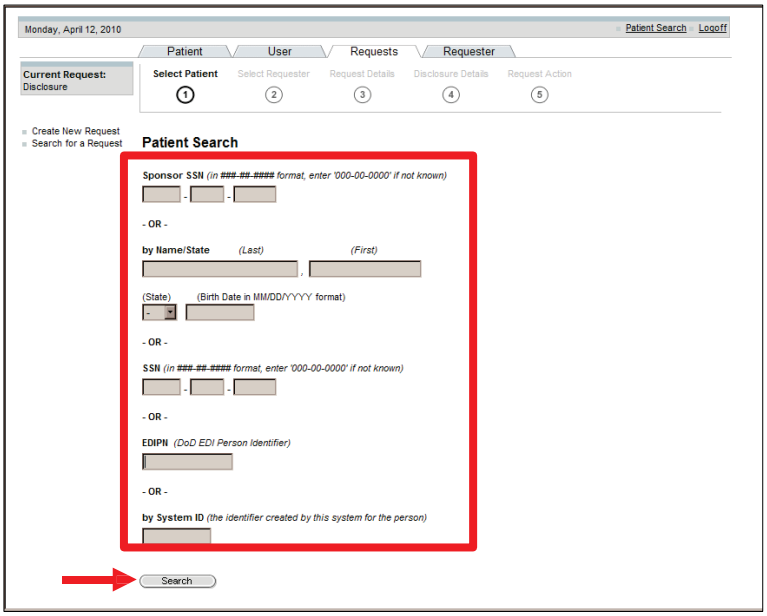
3. Click on the radio button for Disclosure Accounting.

4. Click on the Next button.

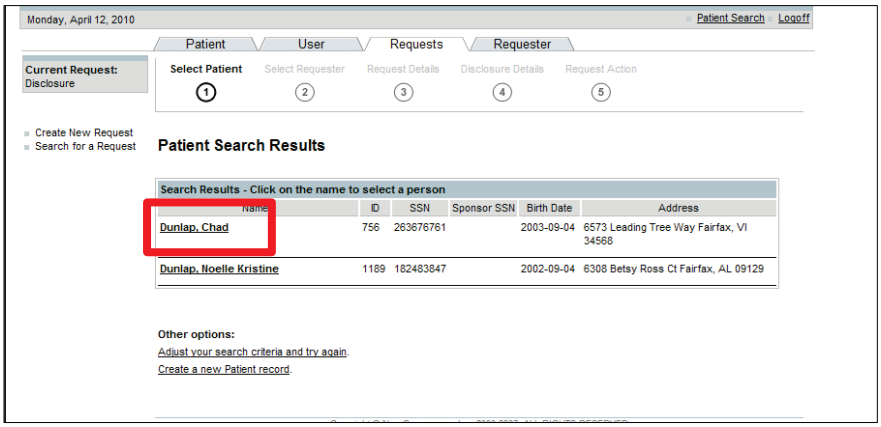


5. Search for the patient (You can search for a patient by the Sponsor's SSN, by the patient's name/state, SSN, EDIPN or System ID).

6. Click on the Search button.



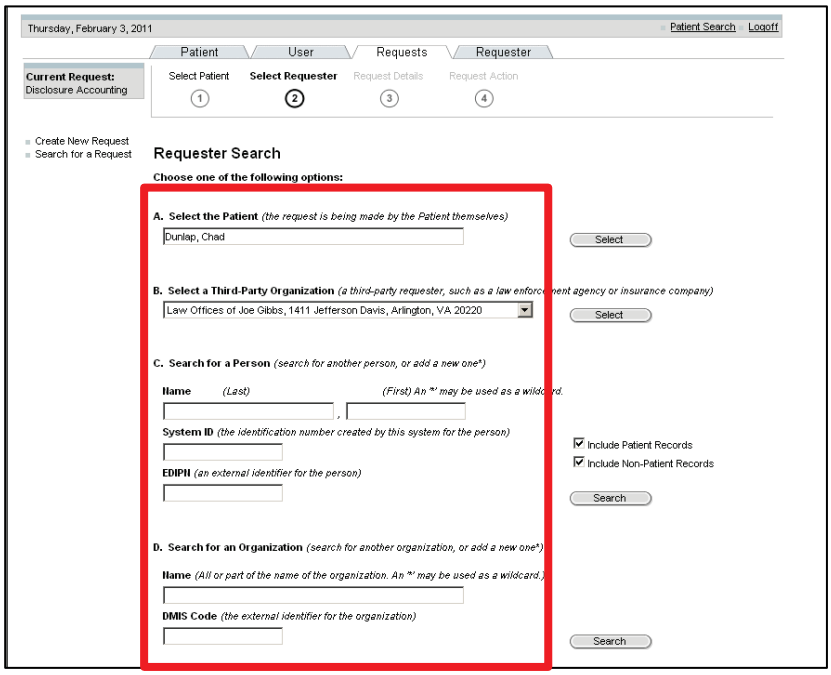
7. Select the patient from the Patient Search Results screen.



Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

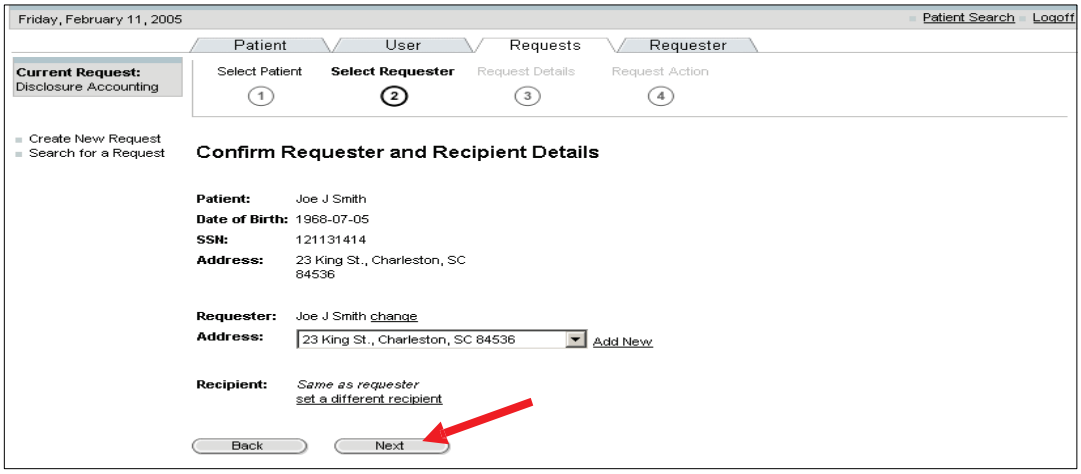
8. Select the Requester: either a) select by the default patient or organization displayed, or b) enter the information into the data entry fields, to search by patient, third party organization, person, or organization. Complete only one field. (For this User Manual, the patient is selected).

9. Click Select, or Search (for that field).



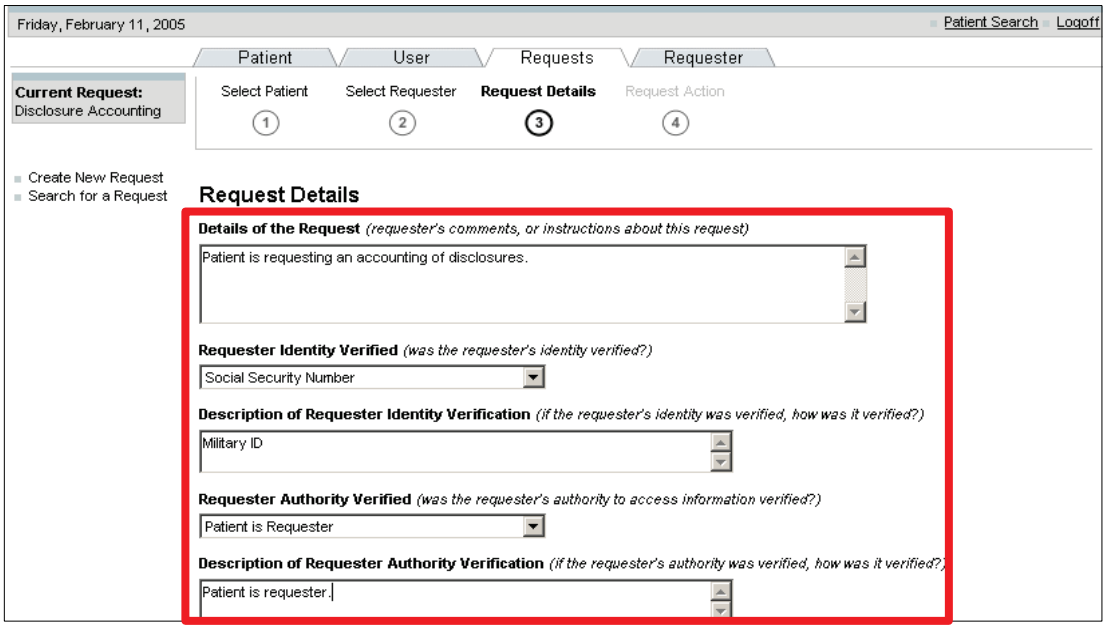
10. Confirm the requester and recipient details. Verify that the information is correct and/or enter the data into the information fields. (If changes are necessary, select Back, and make the changes).

11. Click on the Next button.



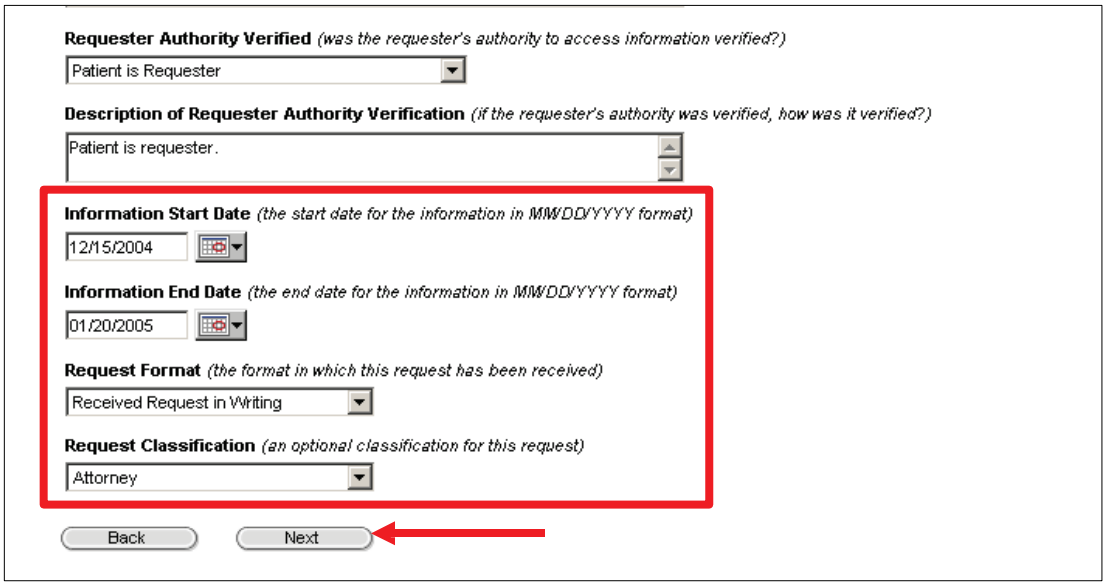
Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

12. Enter the Request Details: details of the request, identity verification (with description), and authority verification (with description).



13. Scroll down the screen and enter: Information start and end date, request format, and request classification.

14. Click on the Next button.



15. Enter the Request Action details.

16. From the Action drop-down menu, select the appropriate person to route the request to. (The Regular User would route the request to the Privacy Specialist or to their worklist).

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

17. Click on the Save button.

Friday, February 11, 2005 Patient Search Logoff

Patient User Requests Requester

Current Request: Disclosure Accounting

Select Patient (1) Select Requester (2) Request Details (3) Request Action (4)

Create New Request
Search for a Request

Request Action

Patient
Name: Joe Smith
SSN #: 121131414
Birth Date: 07-05-1968
Address: 23 King St., Charleston, SC 84536

Requester/Recipient
Name: Joe J Smith
Address: 23 King St., Charleston, SC 84536

Details of the Request *(requester's comments about the scope of this request)*
Patient is requesting an accounting of disclosures.

Approved Part *(for partially approved requests, describe part of request that was approved)*

Denied Part *(for partially denied requests, describe part of request that was denied)*

Action *(action for this request)*
Route to Privacy Specialist

Back Save

- The Request Summary screen will display.

NOTE: The current disclosure accounting appears in the status box.

Friday, February 11, 2005 Patient Search Logoff

Patient User Requests Requester

Current Request: Disclosure Accounting

Summary
History
Documents
Request Details
Request Action

Create New Request
Search for a Request

Request Summary

Patient
Name: Joe J Smith
SSN #: 121131414
Birth Date: 07-05-1968
Address: 23 King St., Charleston, SC 84536

Requester/Recipient
Name: Joe J Smith
Address: 23 King St., Charleston, SC 84536

Request Status: Routed Request For Acceptance

Request Creation Date: 02/11/2005 at 01:05:04 PM EST

Request Last Update Date: 02/11/2005 at 01:05:06 PM EST

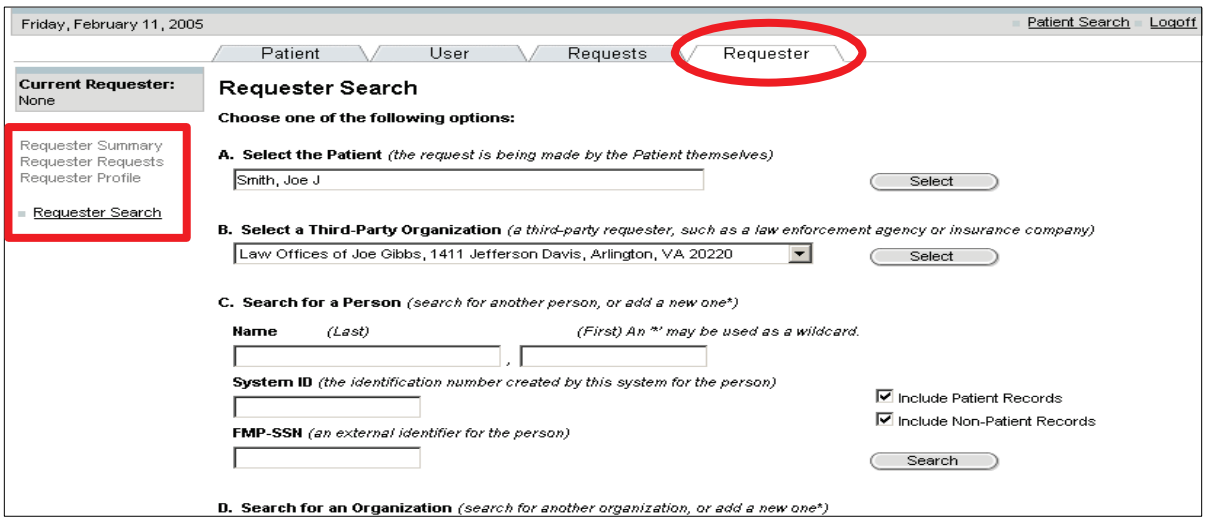
Other Request Details

Description	Details
Request Type	Disclosure Accounting
Details of the Request	Patient is requesting an accounting of disclosures.
Start Date	12/15/2004
End Date	01/20/2005
Authority Verified	Patient is Requester
Verify Authority Text	Patient is requester.

5.4 REQUESTER TAB ACTIVITIES

The Requester tab (shown below) provides access to all PHIMT Requester data and allows you to access information about the individual or organization making the disclosure request. You must first identify an organization or individual as the requester. This can be accomplished on the Requester Search screen. The hyperlinks become active on the Requester Summary screen once a requester has been designated. Access to requester data is provided by these hyperlinks:

- Requester Summary
- Requester Requests
- Requester Profile
- Requester Search



5.4.1 Requester Search

NOTE: The Requester Search hyperlink allows you to search for a particular requester. (You are searching for a patient in the database).

To search for a particular requester:

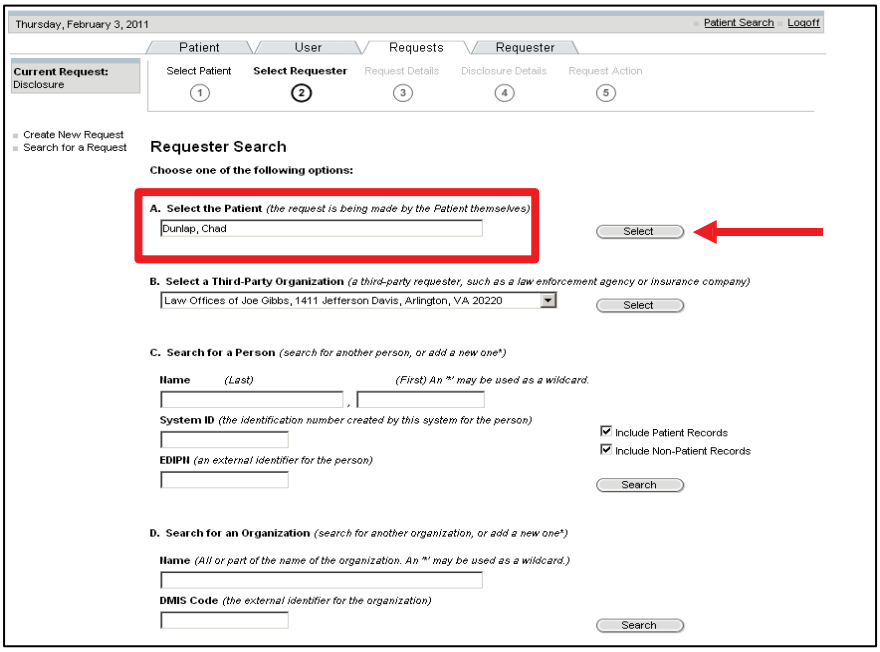
1. Select the Requester Tab.

2. Select the Requester Search hyperlink.

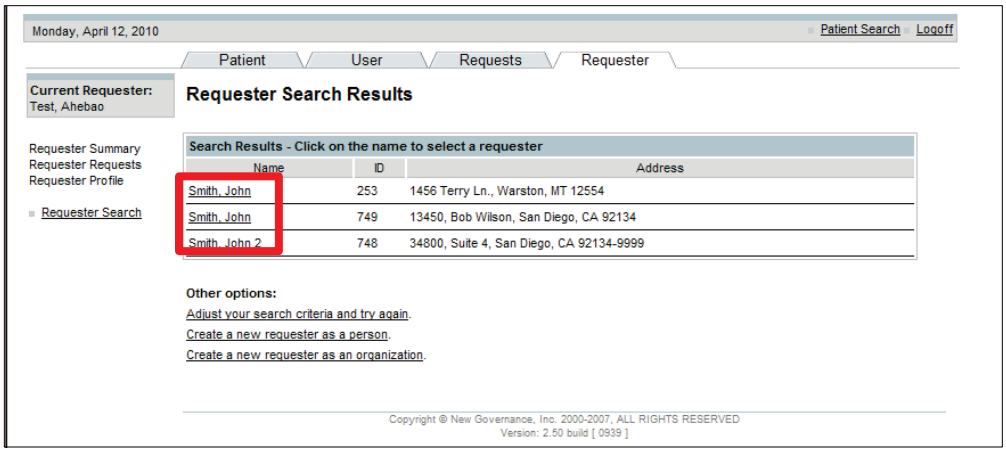
3. Enter the person's name for the search.

4. Click on the Search button.

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.



5. Select the patient from the Requester Search Results screen.



- The Requester Summary screen will display. The Regular User can display reports and/or letters by clicking the Display button or accessing another hyperlink.

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

5.4.2 Requester Requests

NOTE: The Requester Requests screen displays the status of all requests that were generated by a particular patient or organization.

To view the status of requests:

1. Select the Requester Tab.

2. Select the Requester Search hyperlink.

3. Enter the person's name for the search.

4. Click on the Search button.

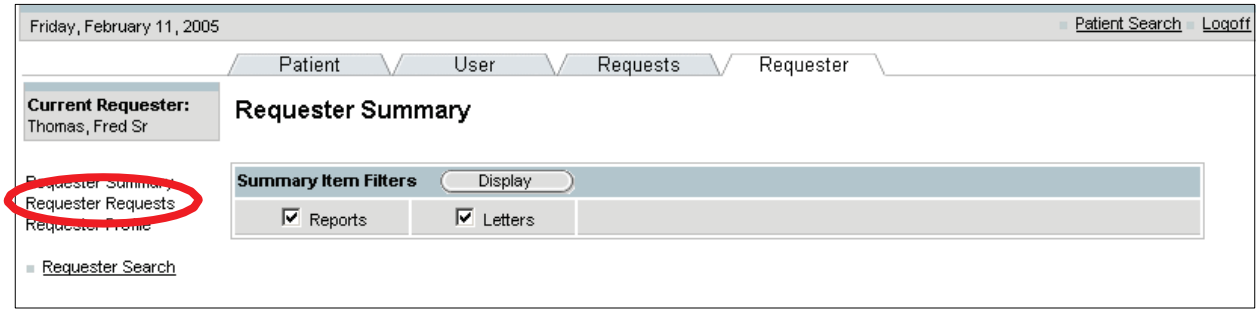
5. Select the patient from the Requester Search Results screen.

6. Click on the Select button.

   - The Requester Summary screen will display.

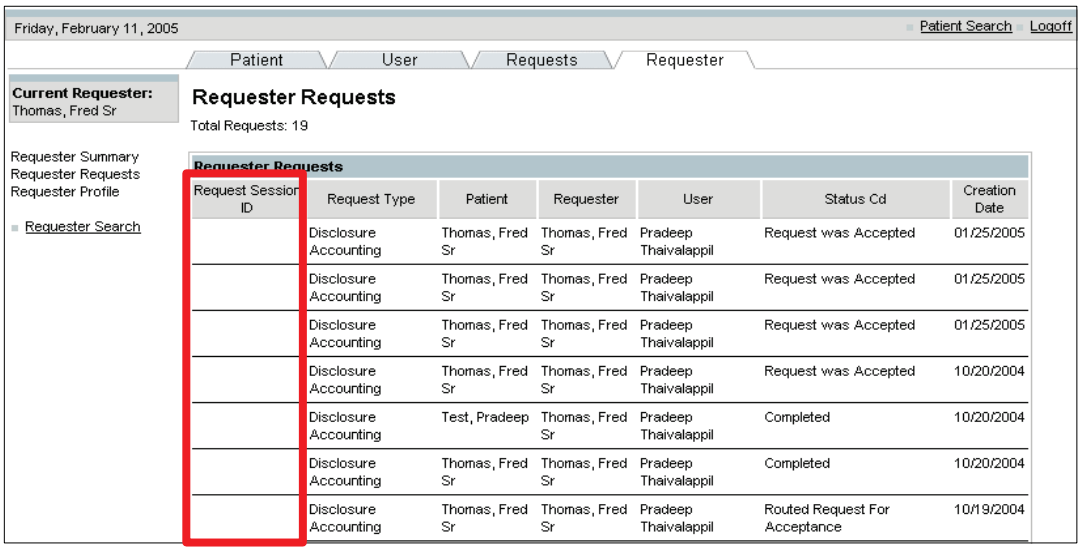
NOTE: Steps 1-6 for Requester Requests are the same as those for Requester Search,5.4.1. Refer to steps 1-6 in 5.4.1 for screen display information.

7. Select the Requester Requests hyperlink.



- The Requester Requests screen will display. All requests for that particular patient or organization and the status of those requests will be displayed. (Regular Users can view the status of a disclosure; however, they cannot view the details of the disclosure. They do not have access to the Request Session ID).

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.



5.4.3 Requester Profile

NOTE: The Requester Profile hyperlink allows you to view information about the individual or organization making the request.

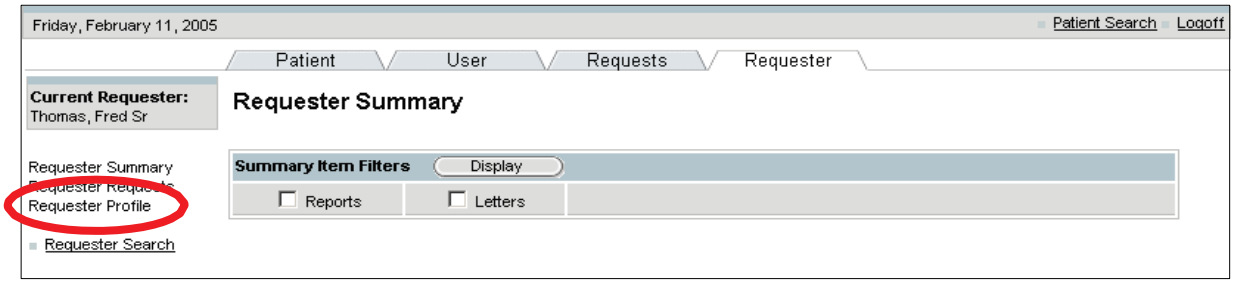
To edit the requester's profile:

1. Select the Requester Tab.
2. Select the Requester Search hyperlink.
3. Enter the person's name for the search.
4. Click on the Search button.
5. Select the patient from the Requester Search Results screen.
6. Click on the Select button.
   - The Requester Summary screen will display.

NOTE: Steps 1-6 for Requester Profile are the same as those for Requester Search, 5.4.1. Refer to steps 1-6 in 5.4.1 for screen display information.

7. Select the Requester Profile hyperlink.

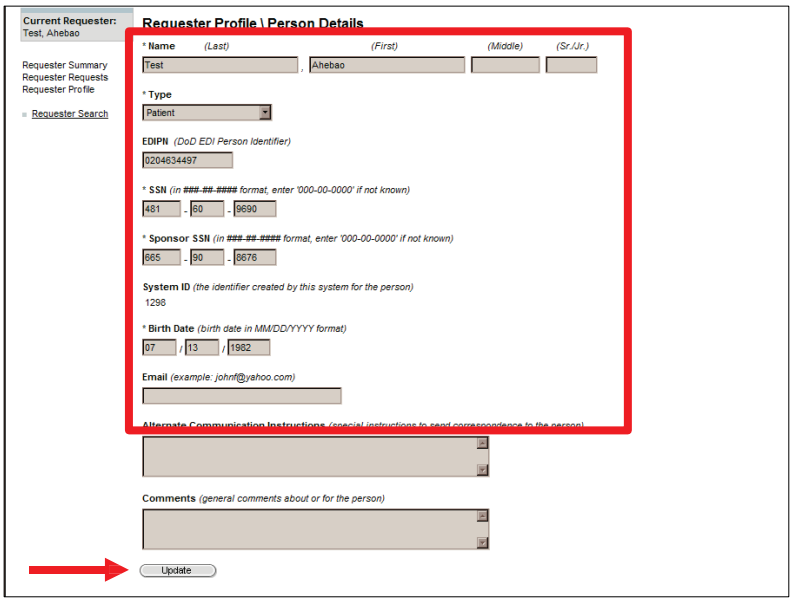
Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.



8. Enter the required information: name, requester type, EDIPN, SSN, Sponsor SSN, birth date of the requester. Use drop-down menus where applicable.

NOTE: The required fields are marked with an asterisk.

9. Click on the Update button.



5.4.4 Requester Summary

NOTE: The Requester Summary hyperlink allows you to display all the letters and reports that were requested.

To view a summary of all disclosure letters and reports:

1. Select the Requester Tab.

2. Select the Requester Search hyperlink.

3. Enter the person's name for the search.

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

4. Click on the Search button.

5. Select the patient from the Requester Search Results screen.

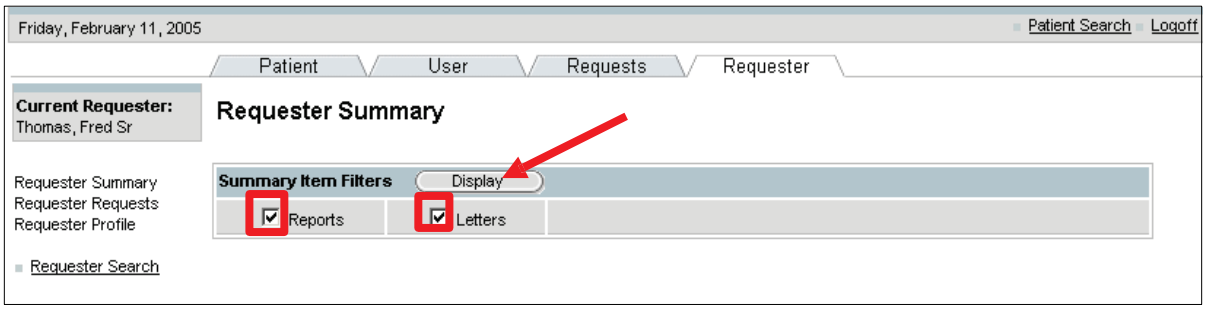
6. Click on the Select button.

   - The Requester Summary screen will display.

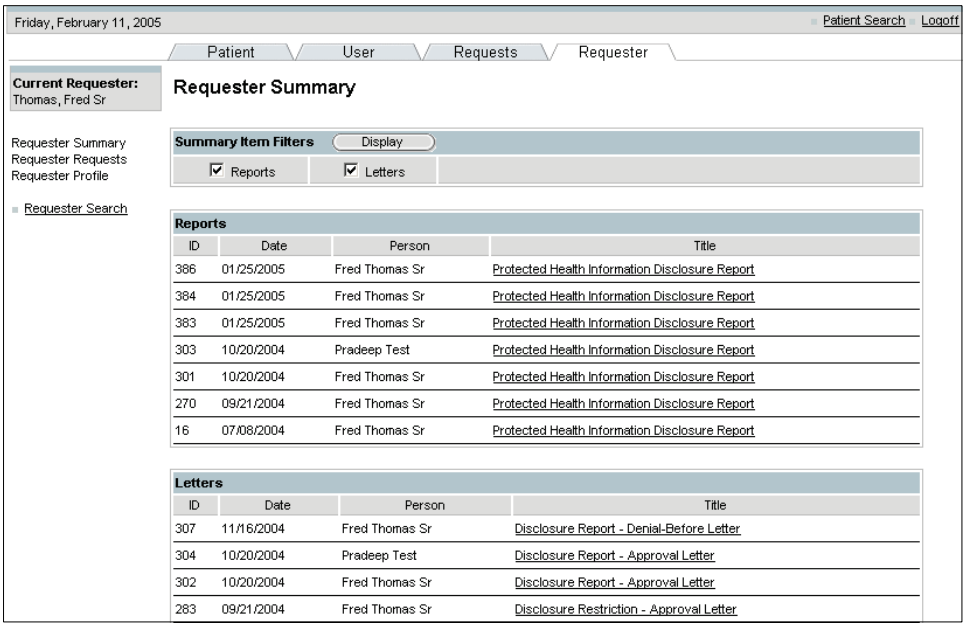
NOTE: Steps 1-6 for Requester Profile are the same as those for Requester Search, 5.4.1. Refer to steps 1-6 in 5.4.1 for screen display information.

7. Select Letters or Reports (or both) by placing a check in the checkboxes.

8. Click on the Display button.



- A summary of all letters and reports of disclosures made by that requester will be displayed.



Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

6.0 GLOSSARY

To facilitate clarity the following terms will be used throughout the document and are defined as follows:

TERM	DEFINITION
Accounting Suspension	An action that results in the temporary postponement of a previously approved disclosure. The suspension can be either specific (referring to a particular disclosure) or type (referring to a disclosure of a particular type). Suspensions can be oral, lasting for up to thirty days, or written, lasting up to six months.
Action	A specific activity that requires a response to a request.
Add Organization	A hyperlink on the Admin Tab that allows the User Admin to enter new user facilities to the current listing
Add User	A hyperlink on the Admin tab that allows the User Admin to enter a new user into the database.
Admin Tab	One of two label tags that provide access to a set of User Admin activities that regulate administrative functions of the PHIMT database. These activities include: maintaining disclosure types and organizations, and creating/modifying users.
All User's List	A hyperlink on the Admin tab that provides a listing of all users in the database. This hyperlink makes user management available.
Attach	An option that allows the User to send documentation or files with a disclosure.
Authorization	A hyperlink on the Patient tab that allows the User to process an approval for a disclosure.
Back	A navigation button that allows the Regular User to return to the previous screen.
Complaint	Activity that allows a user to file a HIPAA grievance against a person or organization.
Create	An option that allows the Regular User to initiate a new activity.
Create New Request	A hyperlink on the Requests tab that allows the Regular User to initiate a request for a new disclosure activity.
Disclosure	A hyperlink on the Requests tab that allows the Regular User to forward a release of protected health information to the Privacy Specialist.
Disclosure Accounting	A hyperlink on the Requests tab that allows the Regular User to process a justification for a disclosure.
Disclosure Details	Refers to information about a specific release that the Regular User can
Disclosure Restriction	Placing constraints on either the information being released or its recipient.

TERM	DEFINITION
Display	An option that allows the Regular User to view various types of information about a particular patient or disclosure activity.
Generate Form	A hyperlink on the Patient tab that allows the Regular User to create forms and letters for various disclosure activities and situations.
Login	The opening screen that requires a User ID and Password.
Logoff	A hyperlink that allows the Regular User to exit PHIMT.
MDR Data	Data that has been imported from the MHS Data Repository.
MTF	Military treatment facility.
My Profile	A hyperlink on the User tab that allows the Regular User to enter/update personal information and preference data.
My Requests	A hyperlink on the User tab that allows Regular Users to view the status of all requests initiated by them.
My Worklist	A hyperlink on the User tab that serves as an electronic inbox. It allows Regular Users perform desktop duties such as viewing all tasks currently assigned to them.
New	An action button that allows the Regular User to develop a new item, patient, or organization.
New Patient Record	A hyperlink on the Patient Search Results screen that allows Regular Users to provide information about a new patient.
Next	A navigation button that allows the Regular User to proceed to the next step in an activity.
Organization	A Military Service or MTF.
Organization Management	A hyperlink on the Admin tab that allows the User Admin to create and/or modify facilities within the database. This term refers to the process of maintaining a user's organization profile and status.
Patient Profile	A hyperlink on the Patient tab that allows the Regular User to create or edit patient information.
Patient Search	A hyperlink on the Patient tab and main screen that allows the Regular User to look for a particular patient in the database.
Patient Tab	A tag or label that provides the User with patient-specific activities.
PHI	Protected Health Information.
PHIMT	Protected Health Information Management Tool.
Privacy Specialist	The Privacy Officer or designee at an MTF or Service level. This role allows the user to maintain disclosure reporting, approve/deny disclosure requests, amend requests, and to restrict and suspend disclosures.
Record Disclosure	Documention and confirmation of the release of PHI.
Regular User	A general role with basic functionality. This role can create disclosures and authorization requests that can be routed to a Privacy Specialist.

TERM	DEFINITION
Request	The first step in initiating a disclosure activity.
Request Action	A prompt for a specific performance (route to Privacy Specialist or route to your Worklist) to be taken on a disclosure.
Request Details	Allowing the Regular User to view relevant information about a particular disclosure.
Requester	The individual or agency asking for the disclosure.
Requester Profile	A hyperlink on the Requester tab that allows the user to view information about the individual or organization making the request.
Requester Requests	A hyperlink on the Requester tab that allows Regular Users to view a listing of all requests that were made by an individual or an organization.
Requester Summary	A hyperlink on the Requester tab that allows the Regular User to view a brief of all requests initiated by an individual or organization.
Requester Tab	A tag or label that allows the Regular User to access information about the individual or agency making a request for a disclosure.
Requests Tab	A tag or label that allows the regular User to access information about the activities that have been requested by an individual or organization.
Restriction	A constraint put upon a particular disclosure activity. The constraint could refer to denying access to a particular individual or a particular time frame.
Revoke Authorization	A user rescinding a previous approval for a particular disclosure
Role	A named collection of permissions. A role allows users with the same permissions to be grouped under a unique name such as: Regular User, User Admin, or Privacy Specialist.
Routing	Forwarding an approval request for disclosure to your worklist for later action, or to another individual. For example, a Regular User may forward the approval request to a Privacy Specialist.
Save	An action button that allows Regular Users to save data entries, information, and procedures.
Search	An action button that allows Regular Users to search for a particular individual or activity.
Search for a Request	A hyperlink on the Requests tab that allows the Regular User to look for a particular request made by that person.
Select	An action button that allows Regular Users to select a particular patient or activity.
Status Box	Avgray box in the upper left corner of all screens. This box displays the current information for a patient or activity; depending on actions being performed.

TERM	DEFINITION
Summary	A hyperlink on the Phone Number Details screen of the Patient tab that allows Regular Users to view a brief of all disclosure activities for a particular patient.
Summary Item Filter	A feature accessed on the Patient Summary screen. It allows the user to display a synopsis on disclosures, suspensions, restrictions, reports, letters, and complaints.
Suspension	The act of delaying a disclosure or putting it on hold temporarily.
Switch Organizations	A hyperlink on the User tab that allows Regular Users assigned to more than one organization to switch between their organizations. This allows them to change their primary status in an organization.
TCL	The table where the MDR data is stored.
DHA	Defense Health Agency
Update	An action button that allows Regular Users to update information or perform additional activities.
User Admin	A role that allows the user to set up all accounts for users within their facilities as directed by the MTF Privacy Officer. The User Admin creates and assigns user names and passwords, adds/modifies users from within their Service, assigns roles, creates user-to-user relationships, verifies the identity of individuals who access PHIMT, and provides login information to users. The User Admin also creates workflows by routing the requests of a Regular User to a Privacy Specialist and from a Privacy Specialist to another Privacy Specialist, if necessary.
User Profile	Used when referring to the Add User activity. This profile screen allows the User Admin to enter personal information and preference data about a new user
User Role	A named collection of permissions. A role allows Users with the same permissions to be grouped under a unique name such as Regular User, User Admin, or Privacy Specialist. Each role has varying degrees of permissions. Roles allow users with the same permissions to be grouped under a unique name (ex. Regular User, User Admin, and Privacy Specialist). The MTF Privacy Officer usually determines the appropriate role.
User Search	A hyperlink on the Admin tab that allows the User Admin to search for a particular user.
User Tab	A tag or label that allows the Regular User to access all PHIMT User-related information. This tab is designed to track all tasks assigned to a user

TERM	DEFINITION
User-to-User Relationship	The different user types and how they work with one another. The User Admin creates this relationship as directed by the MTF Privacy Officer. The Privacy Officer understands how the MTF manages disclosures. The User Admin understands how to create a workflow by routing requests of a Regular User to a Privacy Specialist and from a Privacy Specialist to another Privacy Specialist, thereby creating the working relationships between the different users. Multiple user relationships can be established throughout the facility.

7.0 USER ROLE PERMISSIONS

PHIMT REGULAR USER PERMISSIONS	
PHIMT Regular User Tab	Enabled Permissions
Logon/Logoff	Both
Patient Tab	Create patient Generate form Generate letter Patient authorization Patient profile Patient search Patient summary Patient workflow View disclosure
User Tab	Change password Switch to other organizations Update address User profile User workflow User worklist Workflow activity Workflow request Workflows tab
Admin Tab	None (can attach file as part of another activity)