Defense Health Agency

Protected Health Information Management Tool

(PHIMT)

Training Reference: Privacy Specialist 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 PRIVACY SPECIALIST 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 16
5.1.4 SWITCH ORGANIZATION 16
5.2 PATIENT TAB ACTIVITIES 17
5.2.1 PATIENT SEARCH 17
5.2.2 CREATE A PATIENT 19
5.2.3 CREATE AN ALTERNATIVE PHONE NUMBER 22
5.3 PRIVACY SPECIALIST ACTIVITIES 23
5.3.1 RECORD DISCLOSURE 24
5.3.2 APPROVE DISCLOSURES 28
5.3.3 AMEND A DISCLOSURE 30
5.3.4 RECORD A REQUEST FOR AN ACCOUNTING OF DISCLOSURES 32
5.3.5 APPROVE ACCOUNTING OF DISCLOSURES 36
5.3.6 GENERATE AN ACCOUNTING OF DISCLOSURES REPORT 38
5.3.7 CREATE A SUSPENSION 39
5.3.8 RECORD A SIMPLE DISCLOSURE 42
5.3.9 RECORD COMPLAINTS 48
5.3.10 RECORD A DISCLOSURE RESTRICTION 57
5.3.11 GENERATE AUTHORIZATIONS 60
5.3.12 SIGN AN AUTHORIZATION 64
5.3.13 REVOKE AN AUTHORIZATION 66
5.3.14 ADMINISTRATIVE SUMMARY REPORTS 68
6.0 GLOSSARY 70
7.0 USER ROLE PERMISSIONS 75

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.

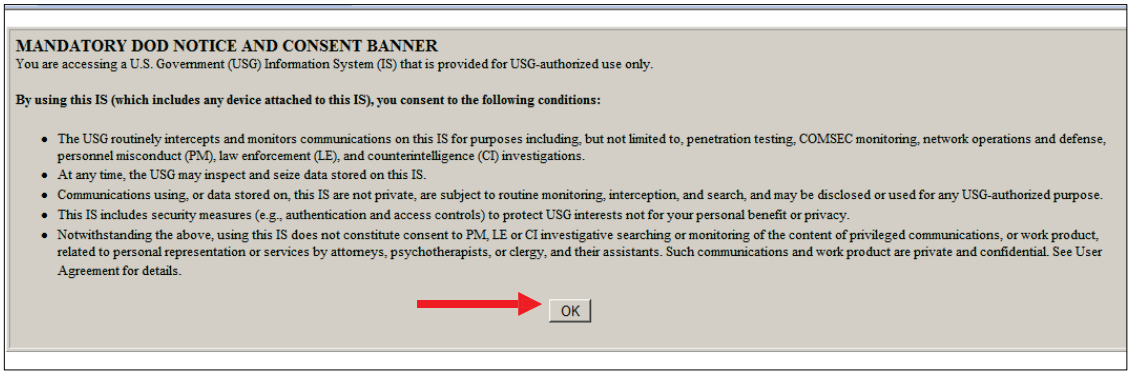
NOTE: To display the generated letters and reports in the browser, the Adobe Acrobat Plug-in is required. This is normally installed with Adobe Acrobat Reader. Download Adobe Acrobat for free at http://www.adobe.com.

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.

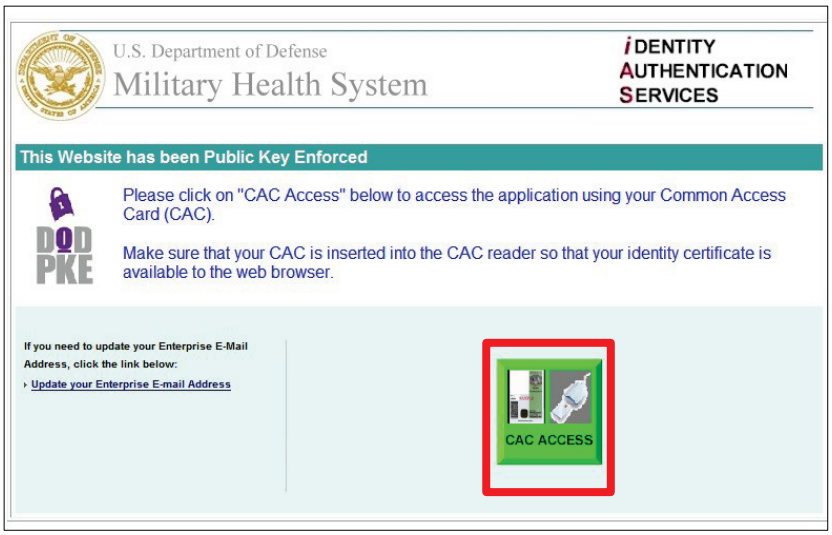
To login to the PHIMT application:

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.

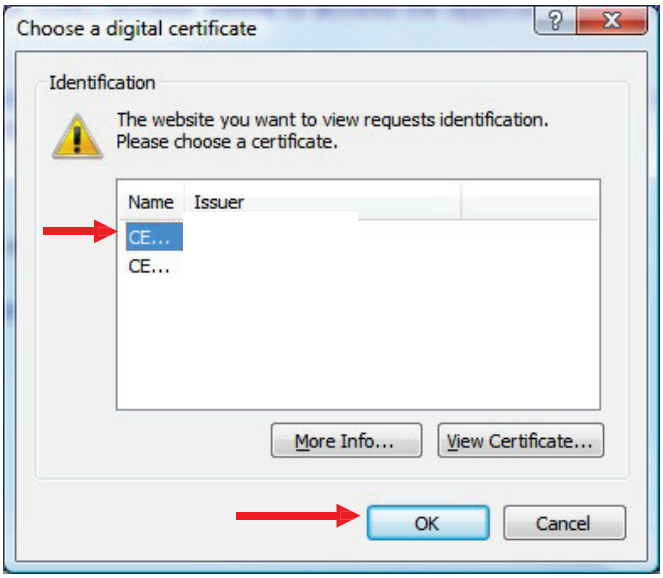
3. Click on the OK button.

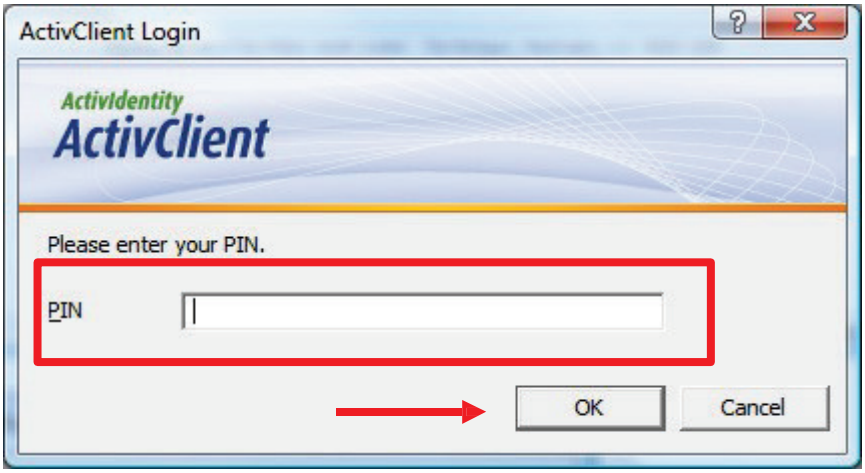


4. Click on the Green CAC Access button.

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

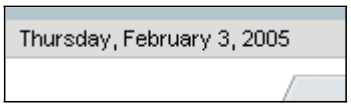
Each tab of the PHIMT screens contains some basic information that will be helpful to you when performing the various activities.

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.

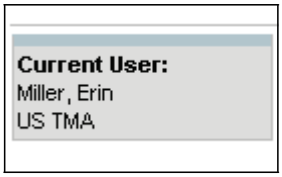


3.1.2 Navigational Options

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.

4.1 ACCESSING PATIENT ACCOUNTS

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.

Monday, April 19, 2010 — Patient Search — Logoff

Patient | User | Admin | Requests | Requester

Current Patient:
Test, Alice
05/05/1928

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

Patient Search

Patient Search Results

Error(s) have occurred:
- At least one record already exists that appears to be the same person

Link to an Existing Record - Click on the name to select a person

Name	ID	SSN	Sponsor SSN	Birth Date	Address
Test, Alice	208945	168226481	176325586	1928-05-05	13980 N Oracle Rd Tucson, AZ 85739

Create a new Record - - Click on the name to select a person

Name	ID	SSN	Sponsor SSN	Birth Date	Address
Test, Alice	new	168226481	176325586	1928-05-05	13980 N Oracle Rd Tucson, AZ 85739-4259

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

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.

Current Patient:
Test, Alexis
11/25/2003
EDIPN:1271043763

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

Patient Search

Patient Profile \ Person Details

* **Name** (Last): Test, (First): Alexis, (Middle), (Sr./Jr.)

* **Type**: Patient

EDIPN *(DoD EDI Person Identifier)*: 1271043763

* **SSN** *(in ###-##-#### format, enter '000-00-0000' if not known)*: 803 - 94 - 9516

* **Sponsor SSN** *(in ###-##-#### format, enter '000-00-0000' if not known)*: 318 - 74 - 3051

System ID *(the identifier created by this system for the person)*: 62140

* **Birth Date** *(birth date in MM/DD/YYYY format)*: 11 / 25 / 2003

Email *(example: johnf@yahoo.com)*:

Alternate Communication Instructions *(special instructions to send correspondence to the person)*:

Comments *(general comments about or for the person)*: Imported from TCL

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

5.0 PRIVACY SPECIALIST FUNCTIONALITY

As a Privacy Specialist, you have the highest level of functionality and responsibility within the system. The following information will provide you with step-by-step instructions for approving requests that have been routed to you from a Regular User.

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

- Approve a Request
- Create a Suspension
- Record a Complaint

5.1 USER TAB ACTIVITIES

The hyperlinks on the User tab allow you to perform "desk duties" such as updating your user profile information, viewing requests you have made, and viewing your tasks, and switching your organization. A discussion on using the User tab hyperlinks follows.

5.1.1 My Profile

The My Profile hyperlink brings you to the User Profile screen (shown below). This screen allows you to update or change your personal information such as: password, phone number, email address, signature block (used for personal or professional titles and credentials) and provide additional comments. Note the area for user roles, located on the bottom of the screen is not active. Only the PHIMT help desk has authorization to perform that activity. You also cannot change your User or System ID, user-to-user relationships, or user roles. The User Admin manages those. However, you can change backup person relationships (discussed later in the guide).

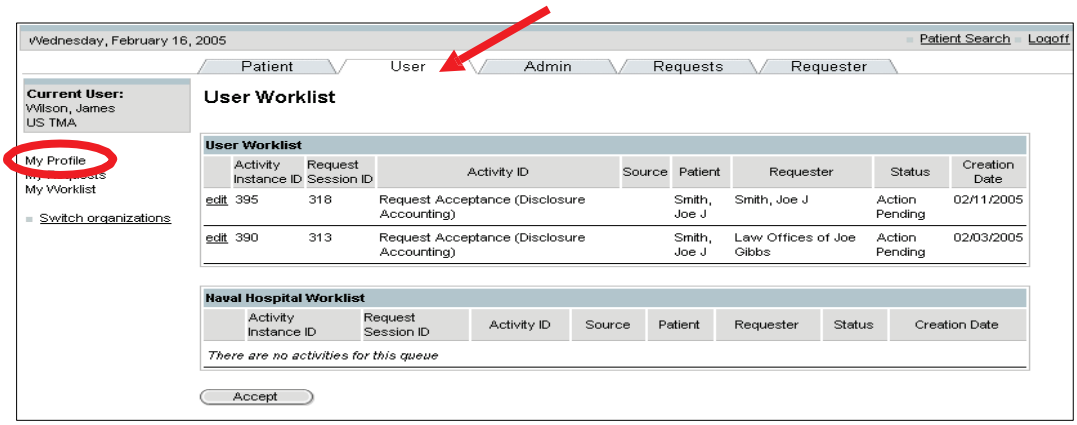
NOTE: When entering a phone number, remember that it will display on all correspondence when generated.

NOTE: PHIMT contains profiles for all users within the system. It is important to keep your personal information up to date. Therefore, you should update all personal information as it changes.

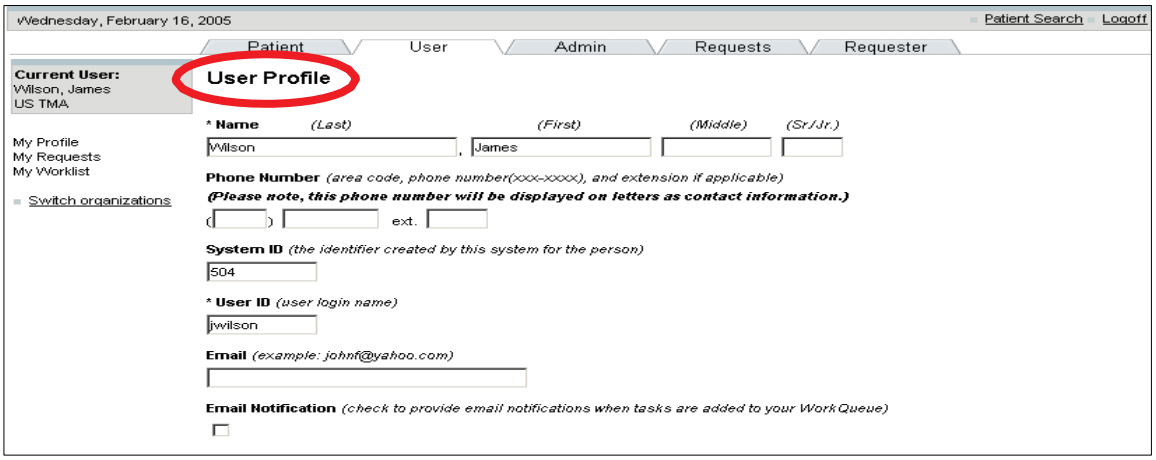
To update your user profile:

1. Select the User Tab.

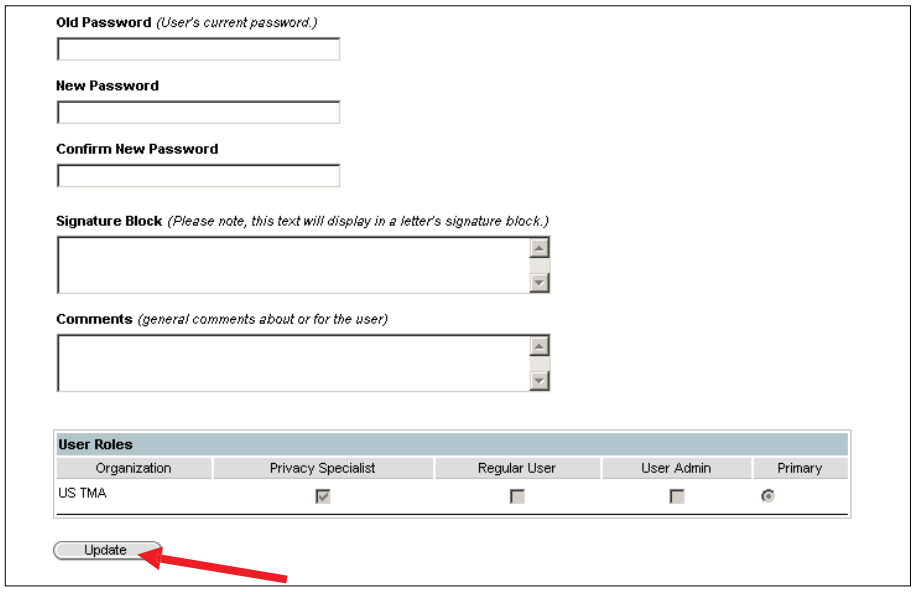
2. Select the My Profile hyperlink.



3. Enter your updated information in the information fields. (Changes can be made to any of the fields in the User Profile screen, except the System ID).



4. Click on the Update button.



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

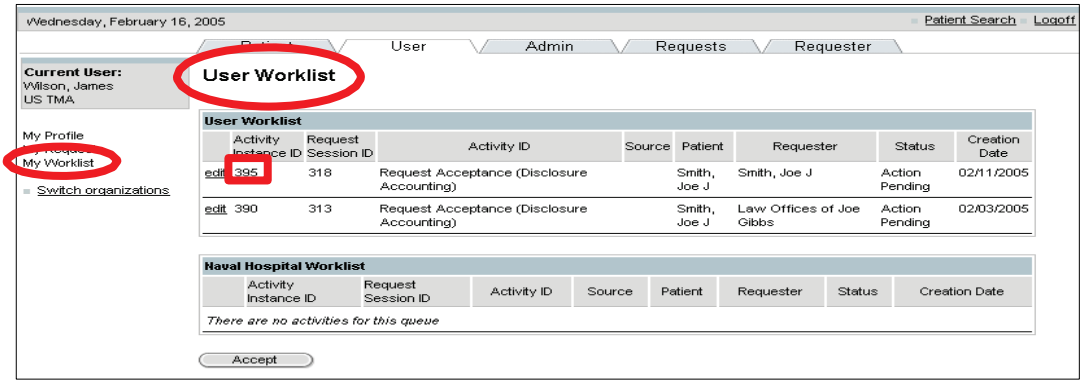
- Your new information will appear in the appropriate fields.

5.1.2 My Requests

The My Requests hyperlink brings you to the User Requests screen that allows you to view all PHIMT activity requests that you have made. To view a detailed summary of a specific request, select the Request Session ID.

5.1.3 My Worklist

The My Worklist hyperlink brings you to the User Worklist screen (shown below) and allows you to view and process all requests that have a task currently assigned to you. My Worklist serves as your electronic inbox. You should review your User Worklist to verify any tasks that have been assigned to you. To view more information on a particular activity, select the Activity Instance ID for that activity.



5.1.4 Switch Organization

The Switch Organizations link brings you to the Organization Search Results screen (shown below) and allows you to switch the status of your primary facility to a different facility, if you are assigned to more than one organization. For example, if you wanted to change your primary organization from US Primary Training Organization to DHA Clinical, just click the radio button next to the desired selection, and click Select. Your primary status change will be displayed in the status box.

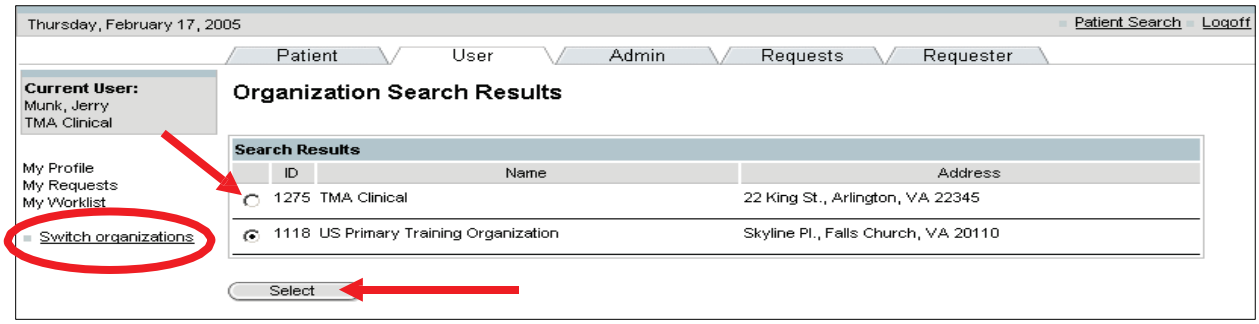
To switch your organization:

1. Select the Switch organizations hyperlink on the User Tab.

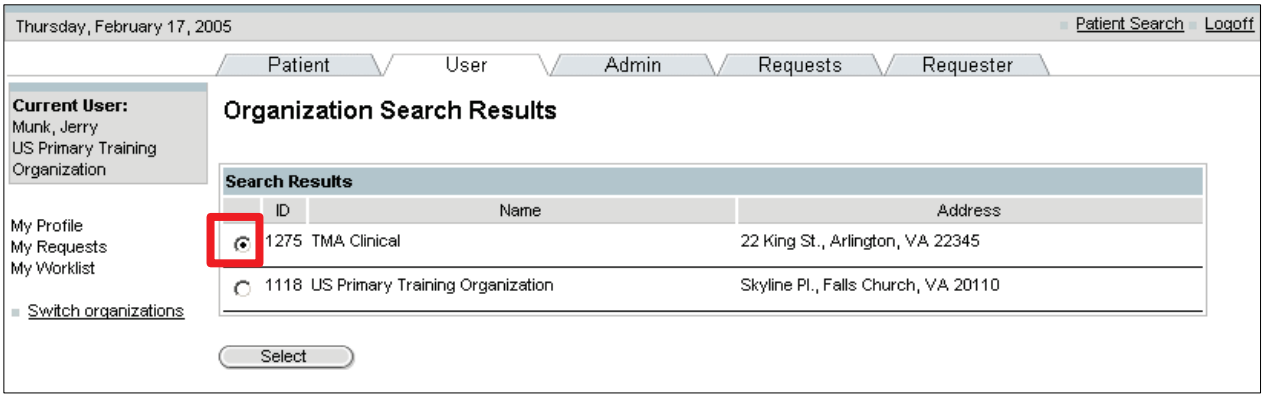
2. Select the organization you want using the radio button.

3. Click on the Select button.

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



- The Organization Search Results screen now shows the radio button located near the facility you selected. The new selection is also reflected in the status box.



5.2 PATIENT TAB ACTIVITIES

The Patient tab allows you to view summaries, make requests, record disclosures and create accounting suspensions, disclosure restrictions, authorizations, and patient profiles. It also allows you to search for patients. Two of the most common activities performed on the Patient tab are Patient Search and Create Patient. We will focus on these two activities here. The more complex Privacy Specialist activities using the Patient tab will be discussed in the Privacy Specialist Activities section.

5.2.1 Patient Search

PHIMT allows you to use its search feature to find a patient that has already been added to the system.

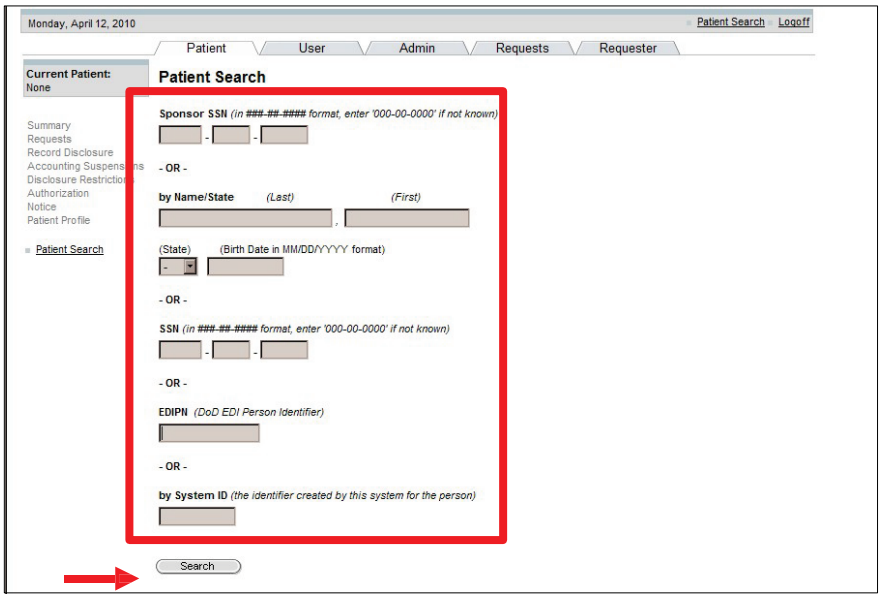
To search for a patient:

1. Select the Patient Tab.

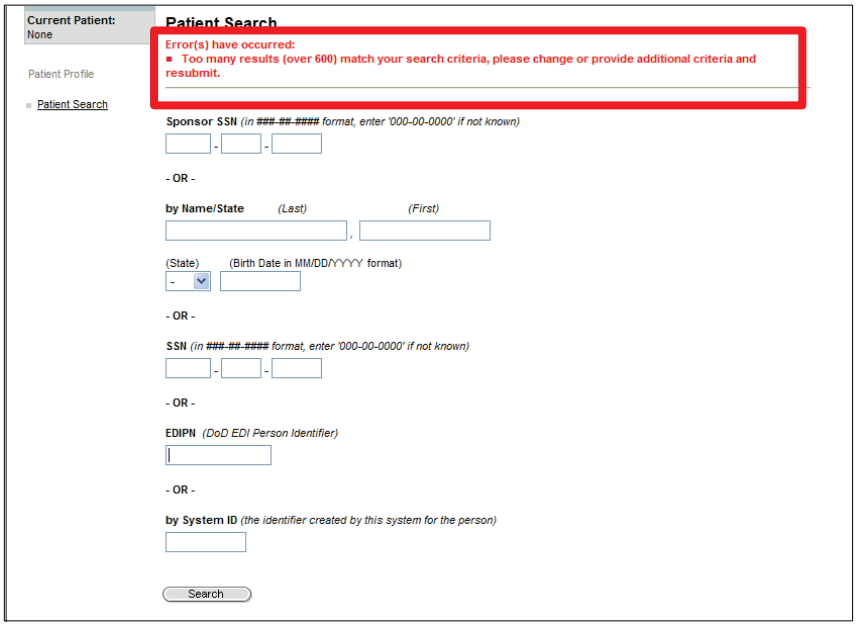
2. Enter the search criteria. (You can search for a patient by the Sponsor's SSN, by the patient's name/state, SSN, EDIPN or System ID).

NOTE: If you do not know how to spell the last name, just enter the first few letters and an asterisk. PHIMT will find the correct spelling.

3. Click on the Search button.

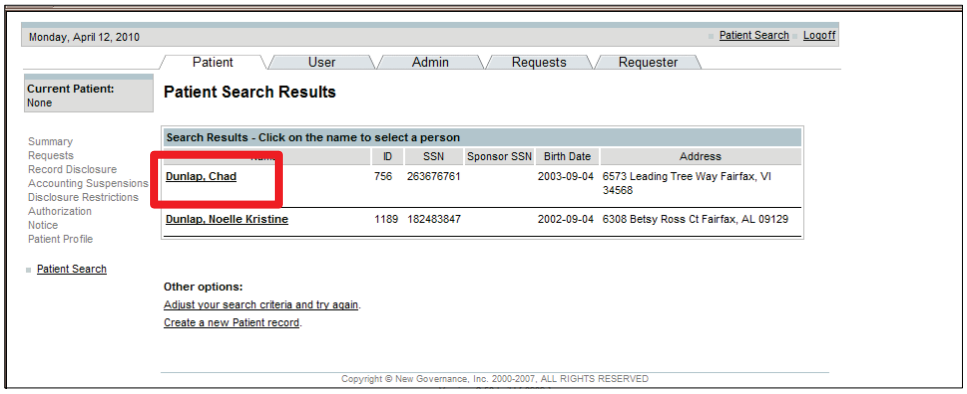


NOTE: The search limitation within the PHIMT is 600 records. This means that if your search results in over 600 records, you will have to narrow down your search.

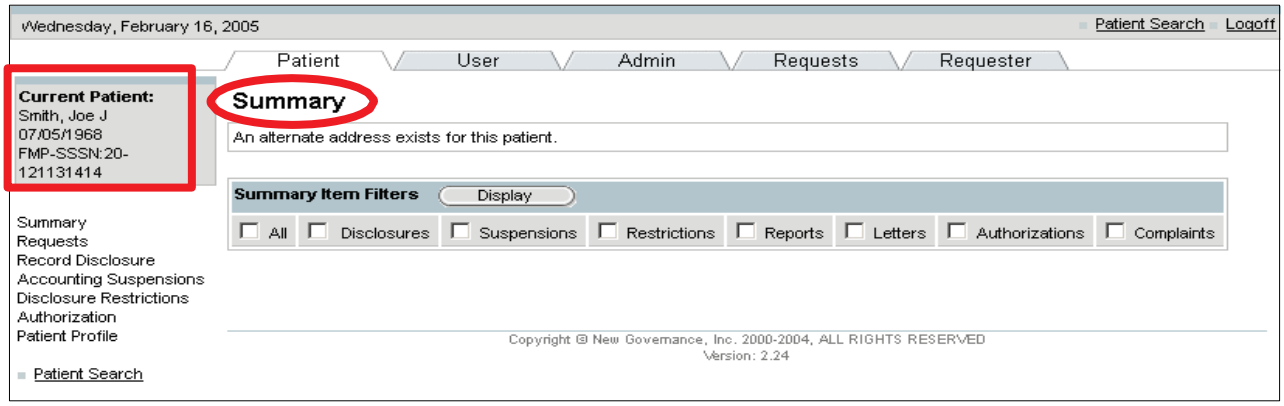


4. Enter additional search criteria (if applicable).

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



- The Patient Summary Screen appears and the current patient is displayed in the status box.



5.2.2 Create a Patient

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. When adding a new patient record, conduct a search within the system initially to ensure that the patient does not already exist. Patient records must be added to the system before disclosures, authorizations or restrictions can be documented.

To create a patient:

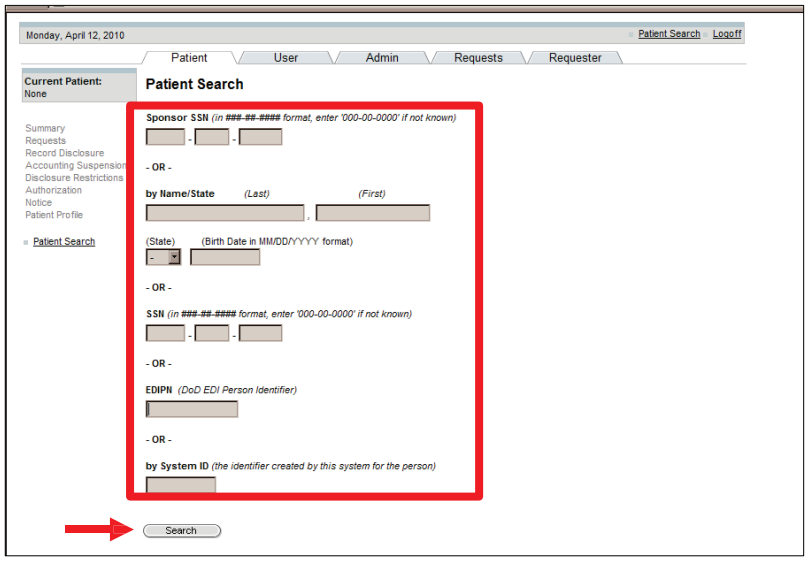
1. Select the Patient Tab.

2. Select the Patient Search hyperlink.

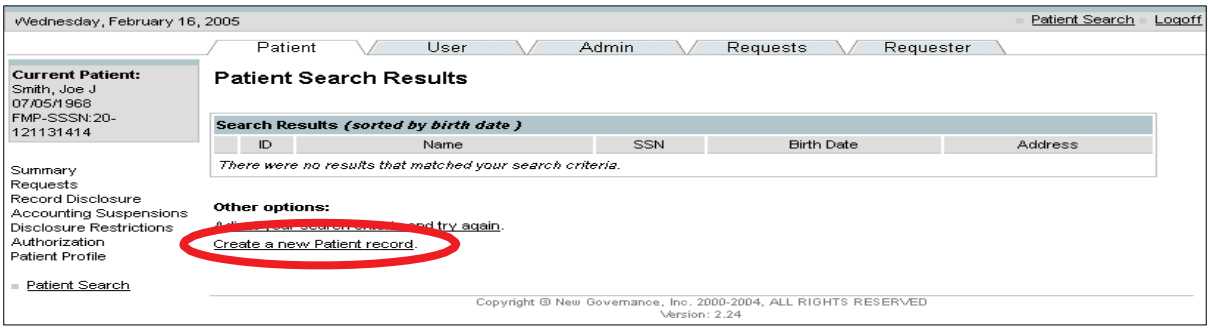
3. Enter the patient search criteria. (You can search for a patient by the Sponsor's SSN, by the patient's name/state, SSN, EDIPN or System ID).

   NOTE: If you do not know how to spell the last name, just enter the first few letters and an asterisk. PHIMT will find the correct spelling.

4. Click on the Search button.

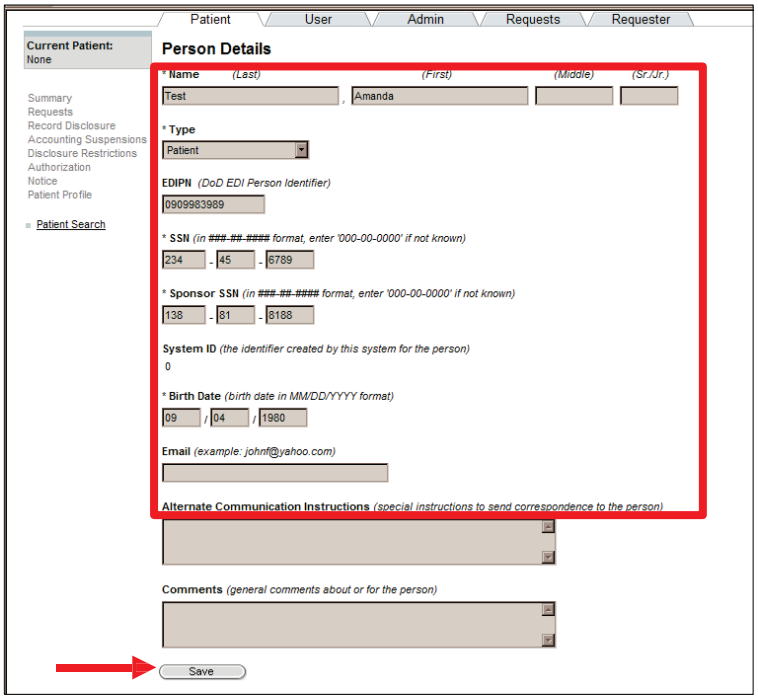


5. If no results matched your search, select the "Create a New Patient Record" hyperlink.



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

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

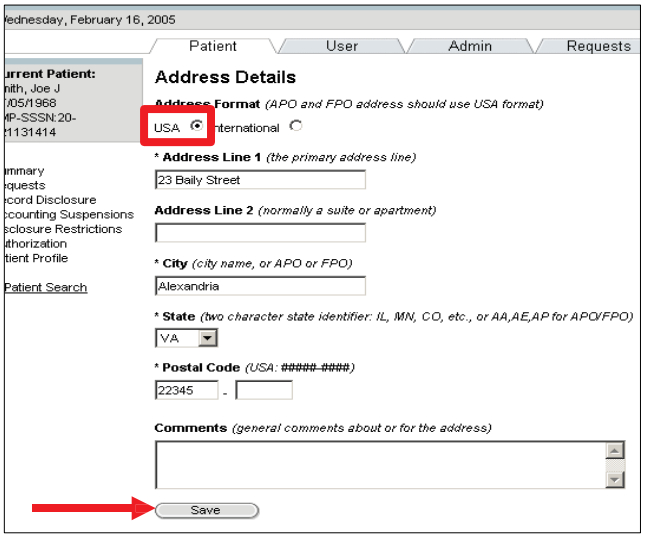


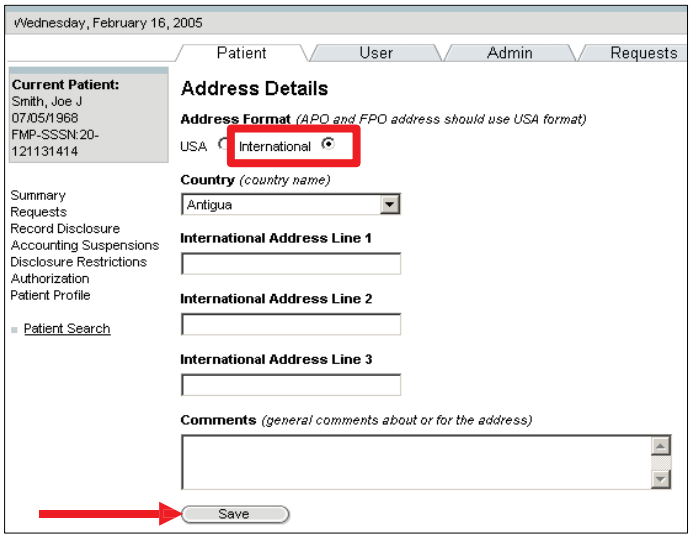
NOTE: All required fields are marked with an asterisk.

7. Click on the Save button.

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

9. 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 patient summary screen for the new patient will appear. (The patient is brand new so no specific patient information will be displayed at this time.) The information is also displayed in the status box.

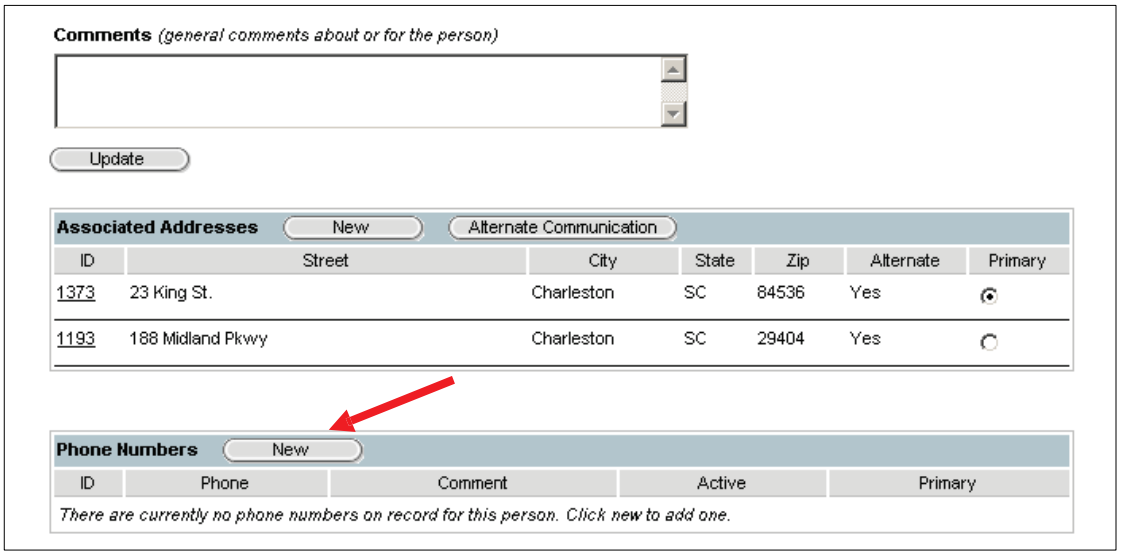
5.2.3 Create an Alternative Phone Number

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.

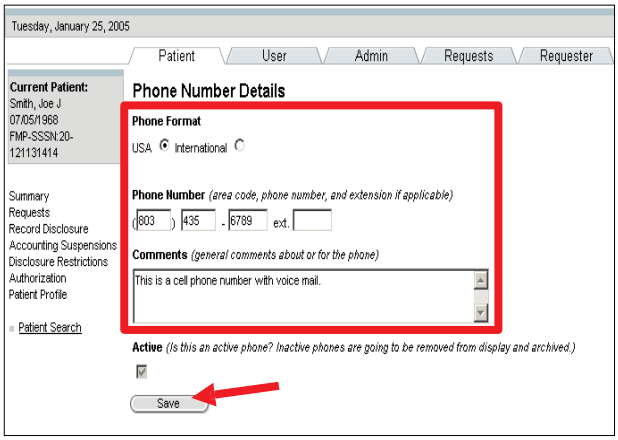


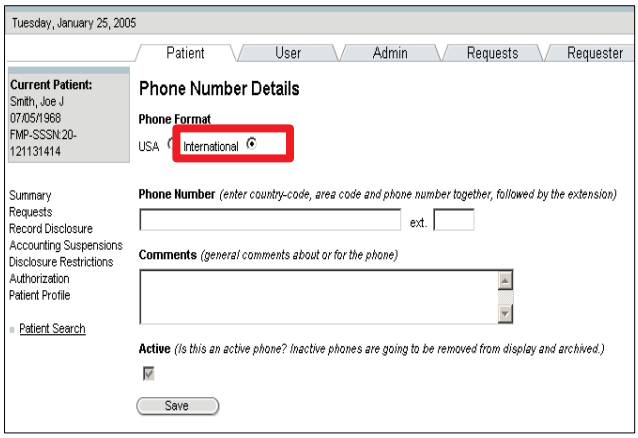
- The Phone Number Details screen will display (choose the USA or International format).

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

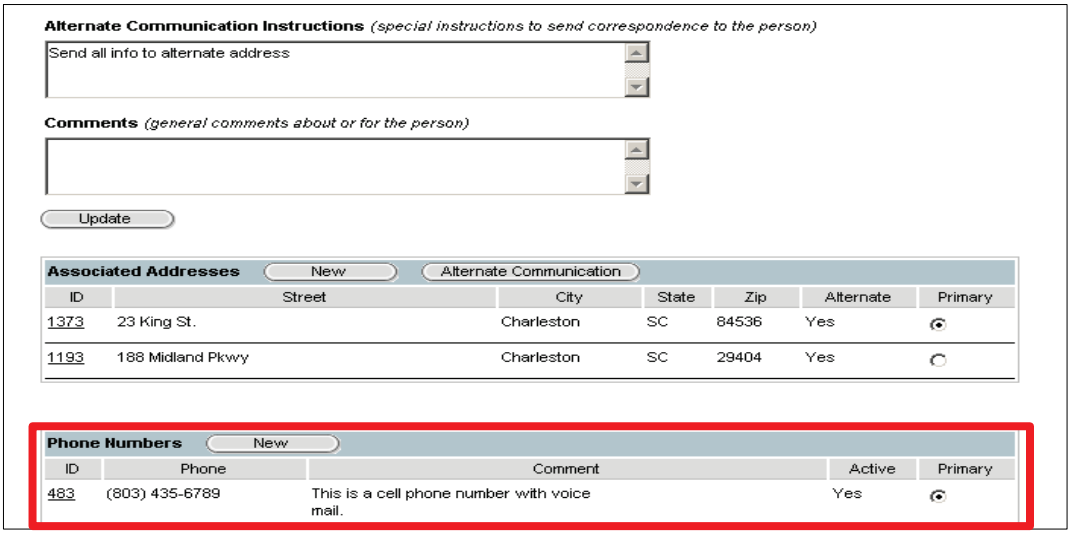
3. Enter the phone number and enter any comments.

4. Click on the Save button.





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



5.3 PRIVACY SPECIALIST ACTIVITIES

This section will focus on the more complex Privacy Specialist activities including: approving disclosures, approving accounting of disclosures, recording complaints, recording disclosure restrictions, generating authorizations, revoking authorizations, and performing accounting suspensions. Instructions for performing these activities are provided in this section.

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

5.3.1 Record Disclosure

The Privacy Specialist can use either the Disclosure Request or the Disclosure hyperlink to record disclosures. The Disclosure Request allows for forwarding the disclosure for approval or denial. The Disclosure hyperlink allows for immediate approval or denial.

If you're using the Disclosure Request you can enter Action Requested from the Action drop down menu, route it to your own worklist for later approval/denial, or route it to another Privacy Specialist.

If you're using the disclosure hyperlink you can complete the Disclosure in the Disclosure Status Field. Select Save when you have completed all fields pertaining to the disclosure.

NOTE: The Disclosure Type and Disclosure Purpose cannot be set to Undefined.

To record a disclosure:

1. Select the Patient Tab.

2. 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).

3. Click on the Search button.

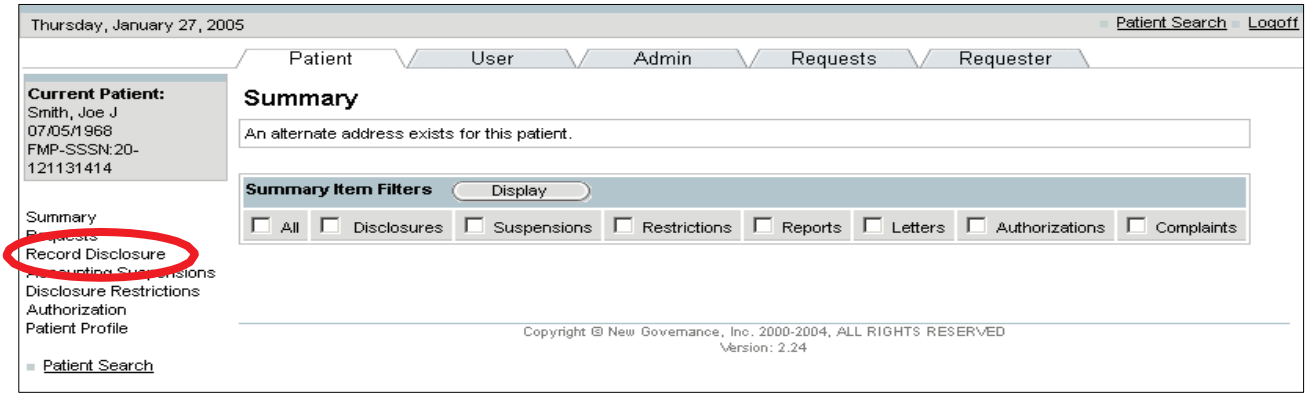
4. Select the patient from the Patient Search Results screen.

5. Click on the Select button.

   - The Patient Summary screen appears.

NOTE: The steps 1-5 for recording a disclosure are the same as steps 1-5 in section 5.2.1 Patient Search. Refer to section 5.2.1 Patient Search for screen displays of steps 1-5.

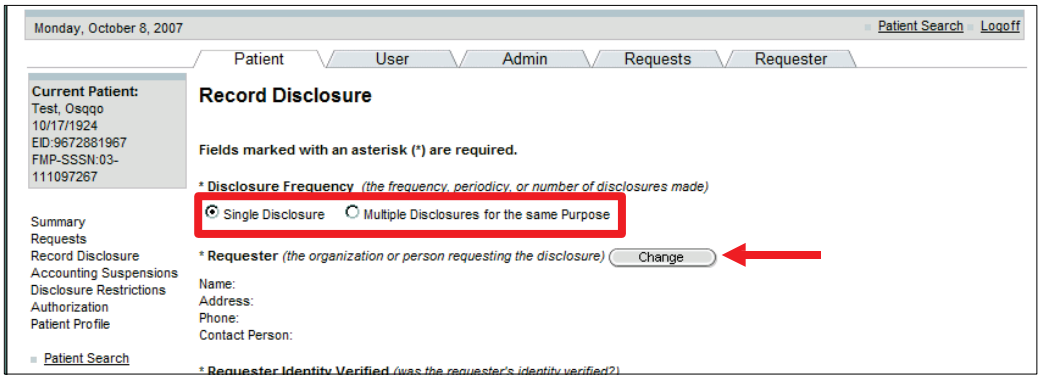
6. Select the Record Disclosure hyperlink on the Patient Summary screen.



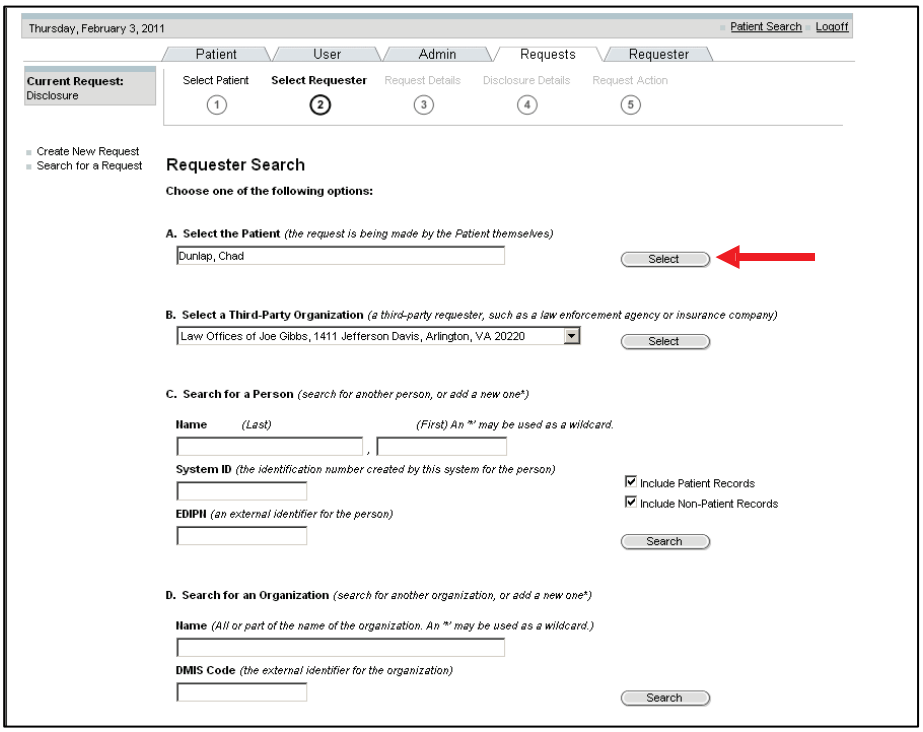
Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

7. Select the Disclosure Frequency radio button.

8. Click on the Change button to change or update the requester.



9. Select the requester.

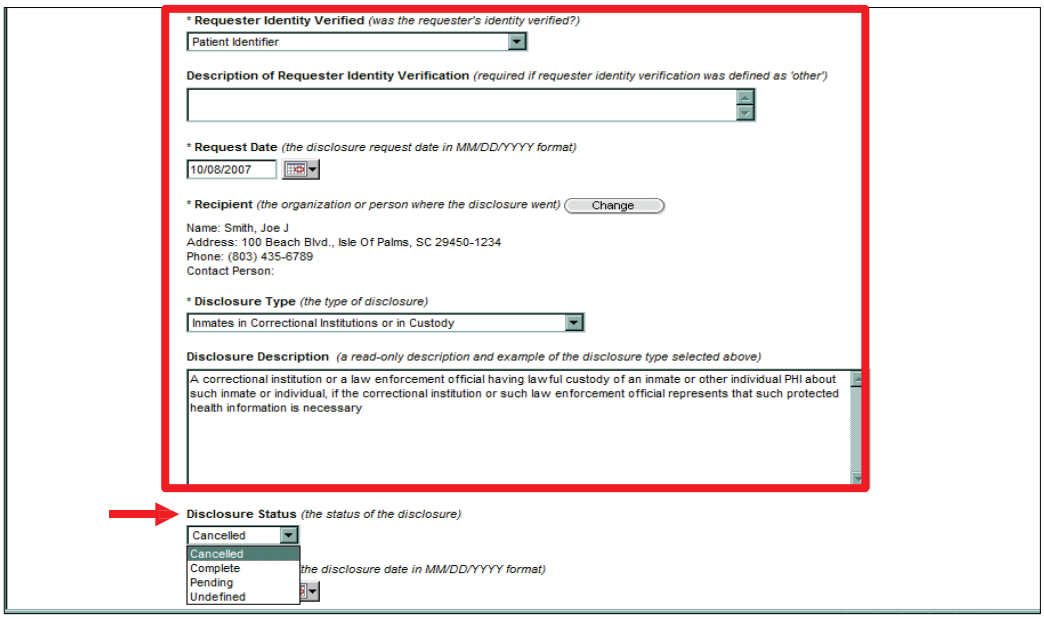


10. Record the Disclosure details: requester authority, form, date, recipient, and disclosure type.

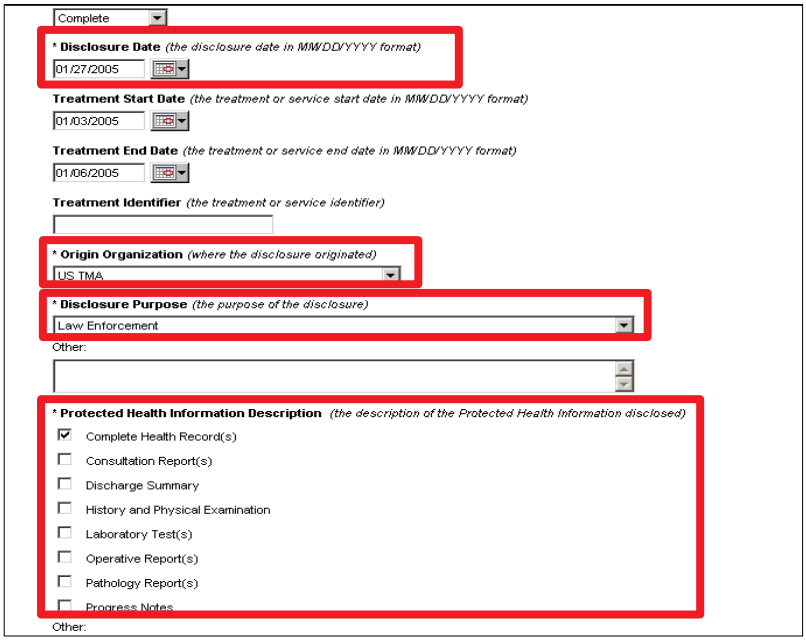
NOTE: The disclosure description will automatically be populated when the disclosure type is selected.

NOTE: All required fields are marked with an asterisk.

11. Select the Disclosure Status from the drop-down box



12. Scroll down the screen and enter: disclosure date, origin organization, disclosure purpose, and PHI description.



13. Scroll down to the bottom of the screen and click on the Save button.

Laboratory Test(s)
Operative Report(s)
Pathology Report(s)
Progress Notes
Other:

Disclosure Comments *(the INTERNAL comments for this disclosure - these do NOT show up in the Protected Health Information disclosure report)*

Improper Disclosure *(checked if this disclosure occured improperly)*

Improper Disclosure Description *(the details about the improper disclosure)*

Improper Disclosure Mitigation *(the details about how the improper disclosure was mitigated)*

Save

- The disclosure is now complete and only the disclosure comments and improper fields can be updated.

Thursday, January 27, 2005 Patient Search Logoff

Patient | User | Admin | Requests | Requester

Current Patient:
Smith, Joe J
07/05/1968
FMP-SSSN:20-121131414

Summary
Requests
Record Disclosure
Accounting Suspensions
Disclosure Restrictions
Authorization
Patient Profile

Patient Search

Record Disclosure

This disclosure (ID #286) was created on 01/27/2005 at 11:09:57 AM EST, and last updated on 01/27/2005 at 11:09:57 AM EST.

Requester *(the organization or person requesting the disclosure)*
Name: Smith, Joe J
Address: 23 King St., Charleston, SC 84536
Phone: (803) 435-6789
Contact Person:

Requester Authority *(the authority of the requester)*
Patient is Requester

Request Form *(the form of the disclosure request)*
Received Request in Writing

Request Date *(the disclosure request date in MM/DD/YYYY format)*
01/27/2005

* **Recipient** *(the organization or person where the disclosure went)*
Name: Law Offices of Joe Gibbs
Address: 1411 Jefferson Davis, Arlington, VA 20220
Phone:
Contact Person:

NOTE: To view the disclosure:

- Select the user tab
- Select My Requests hyperlink
- The disclosure is displayed in the User Request box
- To view specific details of the disclosure, select the Request Session ID for that particular request

NOTE: To Amend Disclosures:
Once a disclosure has a disclosure status of completed, the only way to amend it is by assigning it as an Improper Disclosure. For information on Improper Disclosures, see section 9.3 Amend Disclosures.

NOTE: Disclosures with Special Circumstances:
When making multiple disclosures for the same patient, and for the same purpose, record all information in one disclosure record. Record the disclosure as stated in the previous steps using the following guidance.

Guidance for Completing Disclosure with Special Circumstances	
Data Field	Data to be Provided
Information Start Date	Provide the date for which the disclosure request begins
Information End Date	Leave blank if unknown or insert the date for one year later
Disclosure Date	Insert the date of the first disclosure
Treatment Start Date	Insert the date on which the treatment began
Treatment End Date	Leave blank
Disclosure Purpose/Other	Select Disclosure Purpose from the drop down menu and if applicable, insert text to indicate the frequency of disclosure and the number of disclosures to be made in addition to any other pertinent information such as the name of the report it will support

If there is no end date, be sure to report that there is no end date at this time and therefore the disclosure record will expire in one year. At that time, if the regular disclosures are still ongoing, then a new disclosure record will be created.

NOTE: Remember that the text entered in this field does appear on reports and correspondence generated by the PHIMT.

5.3.2 Approve Disclosures

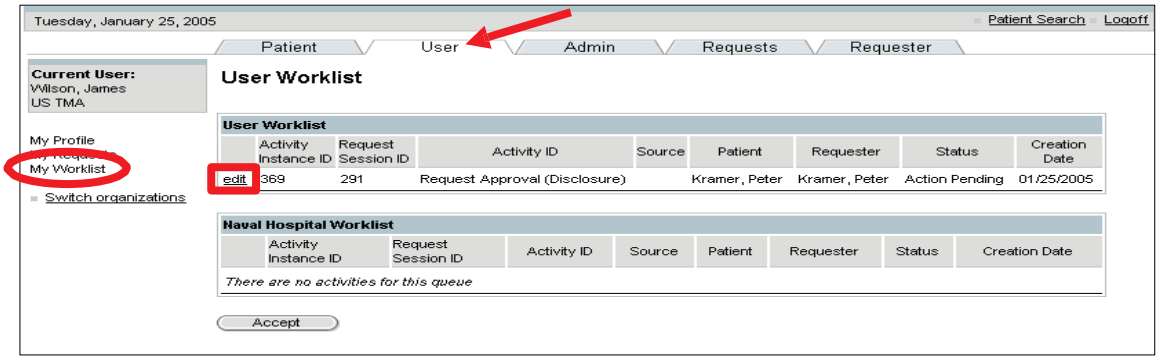
NOTE: Those disclosures recorded by you using the Record Disclosure hyperlink have already been approved. This approval activity is for those disclosures that were developed using the Record Disclosure wizard and routed to your worklist for later action.

To approve a disclosure:

1. Select the User Tab.

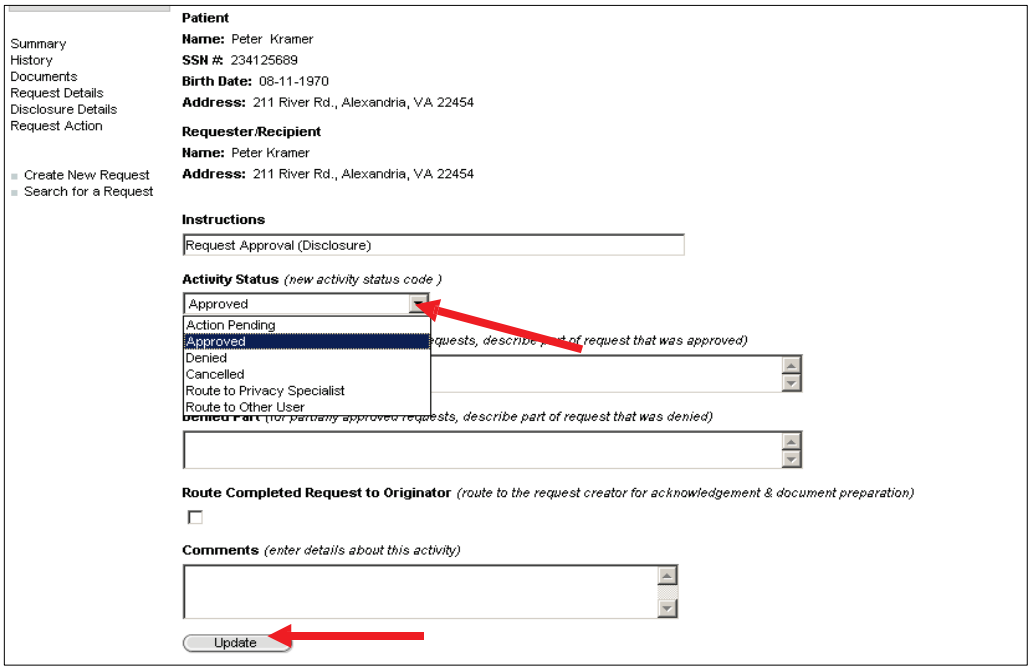
2. Select the My Worklist hyperlink.

3. Select the Edit hyperlink for the disclosure you want to approve.



4. Select Approved from the Activity Status drop-down box.

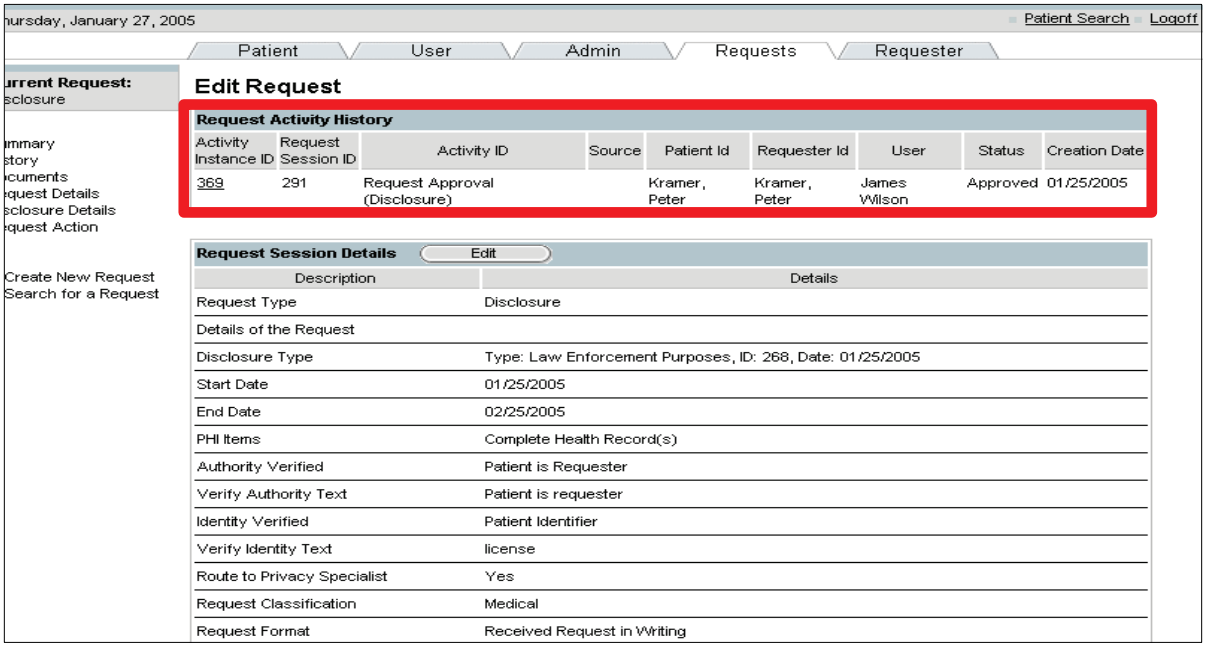
5. Click on the Update button.



- The Edit Request screen appears. The approved request will display in the Request Activity History box. The status has been changed to Approved.

<u>NOTE</u>: The disclosure is no longer shown in your User Worklist.

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



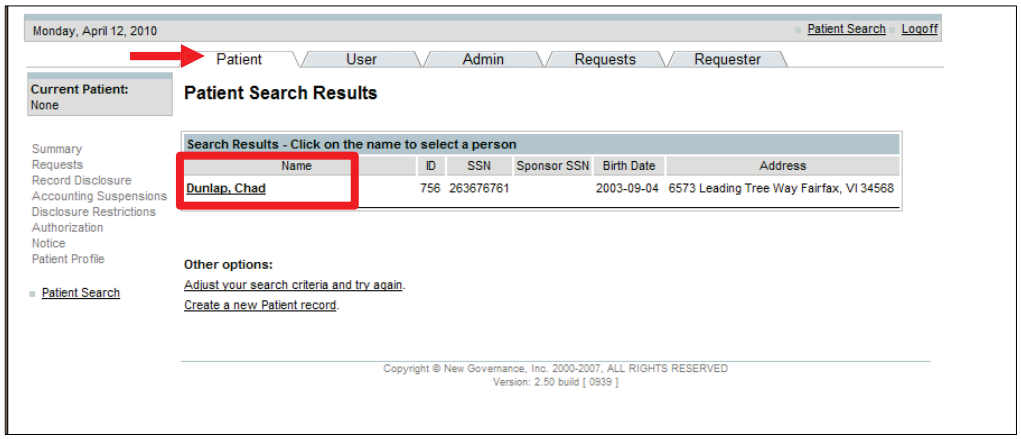
5.3.3 Amend a Disclosure

As a Privacy Specialist you are authorized to label a disclosure as Improper. Once a Disclosure status is marked as completed, it can only be amended by marking it as an Improper Disclosure, which means the disclosure was made incorrectly.

To amend a disclosure:

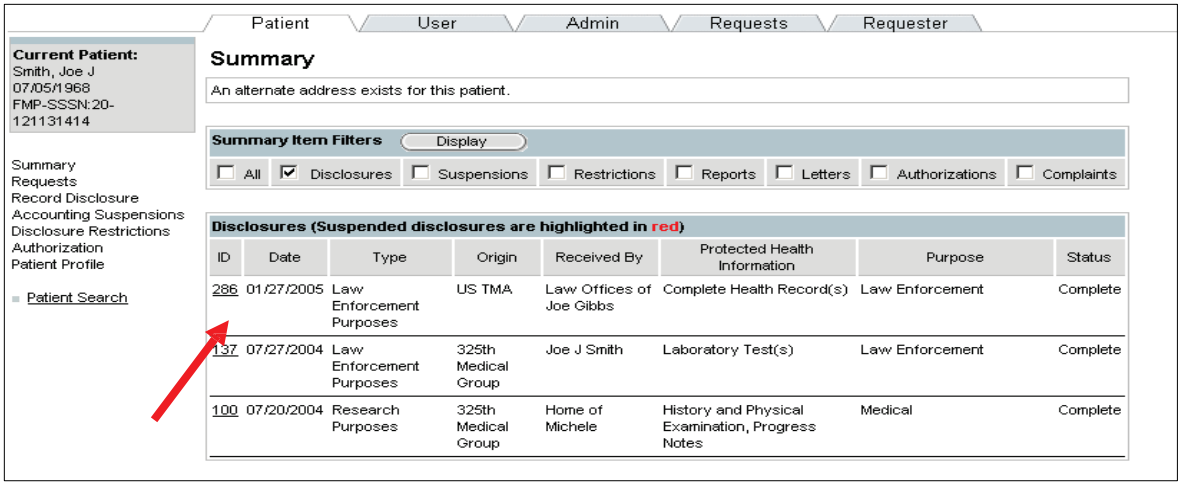
1. Select the Patient Tab.

2. Search for and select the patient.

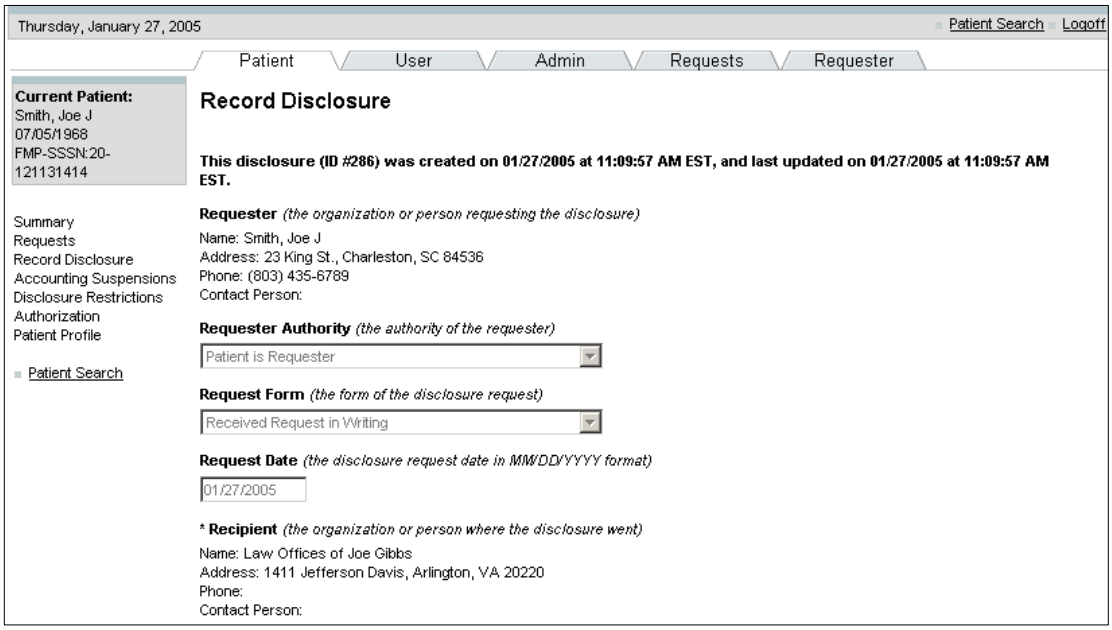


3. Place a check in the Disclosures box and click on the Display button.

4. Select the ID hyperlink for the disclosure that you want to amend.



- The Record Disclosure screen will display.

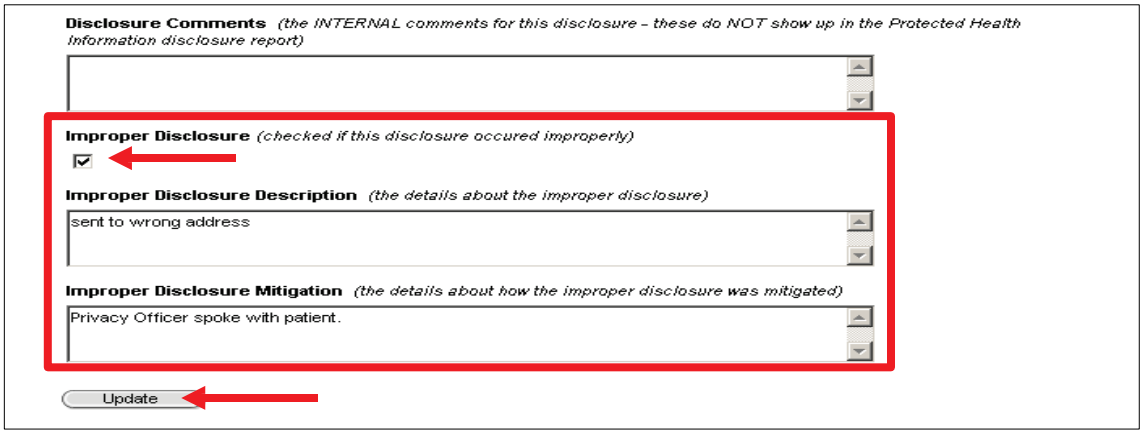


Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

5. Scroll to the bottom of the screen and place a check in the Improper Disclosure checkbox.

6. Enter a description of the Improper Disclosure and mitigation.

7. Click on the Update button.



5.3.4 Record a Request for an Accounting of Disclosures

An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the 6 years prior to the date that the accounting is requested– DoD 6025.18-R Chapter 13.

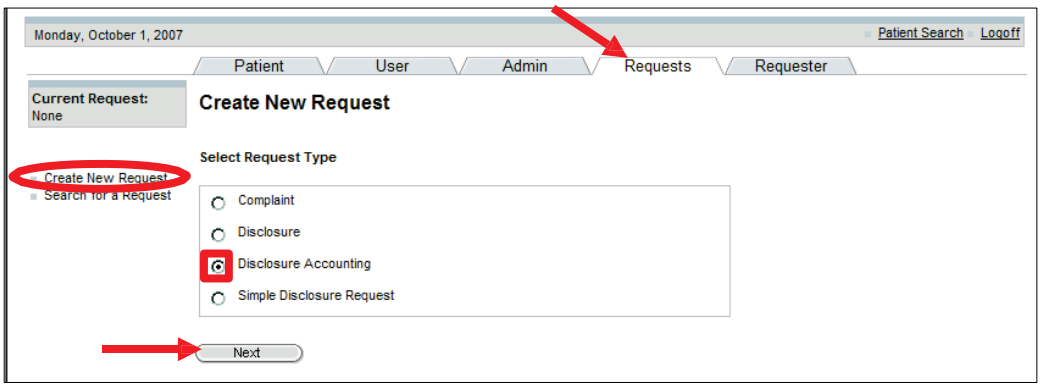
Both Regular Users and Privacy Specialists can record a request for an accounting of disclosures, but only Privacy Specialists can approve or deny the request.

To record a request for an accounting of disclosures:

1. Select the Requests Tab.

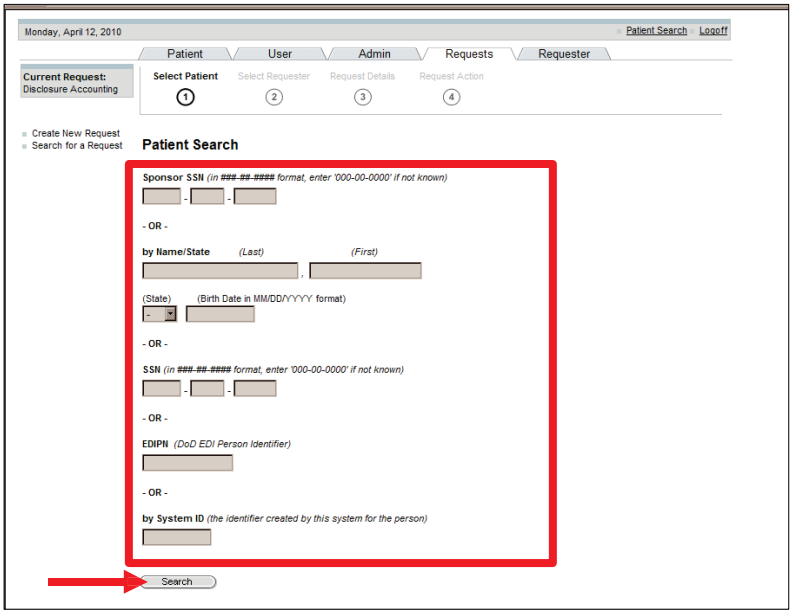
2. Select the Create New Request hyperlink and/or click on the radio button for Disclosure Accounting.

3. Click on the Next button.

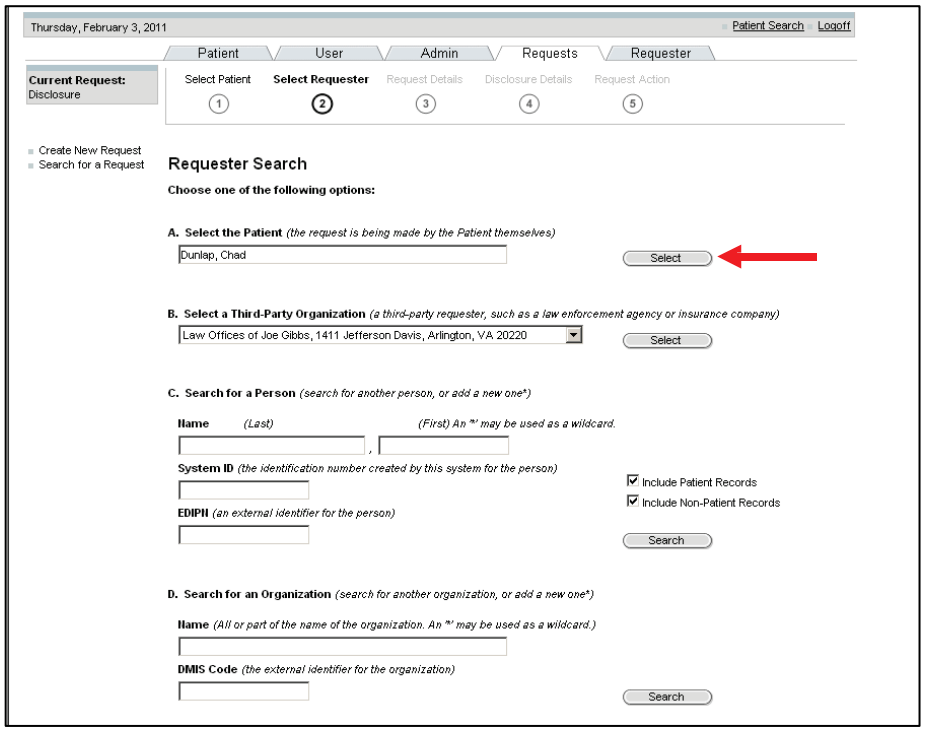


Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

4. Search for the patient.

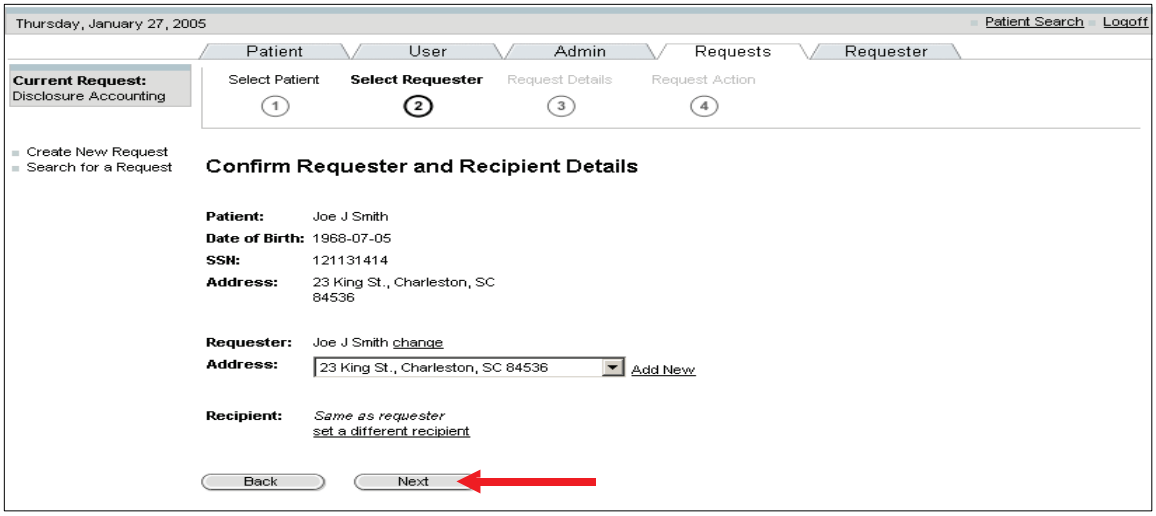


5. Select the Requester.



6. Confirm the requester and recipient details.

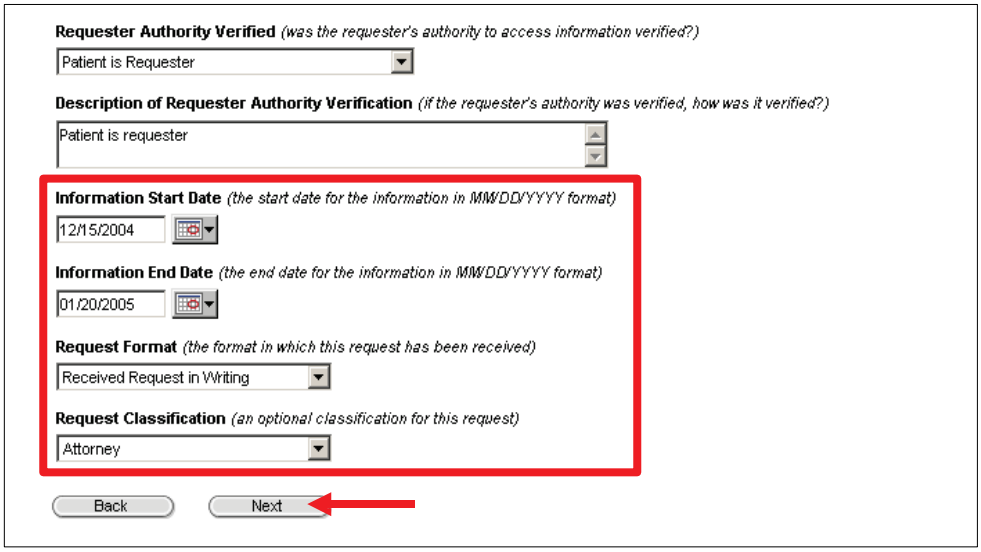
7. Click on the Next button.



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

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

10. Click on the Next button.



11. Enter in the Request Action Details.

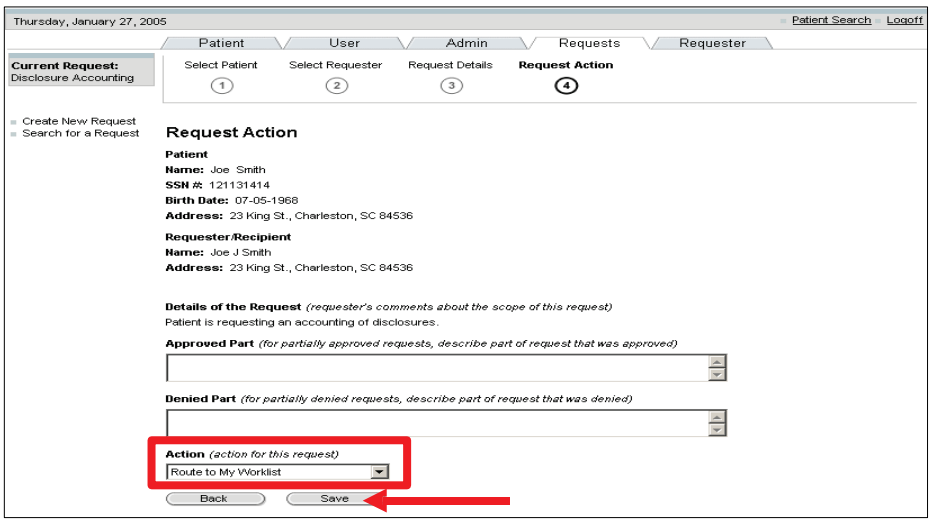
12. From the Action Drop-down box, select the appropriate person to route the request to.

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

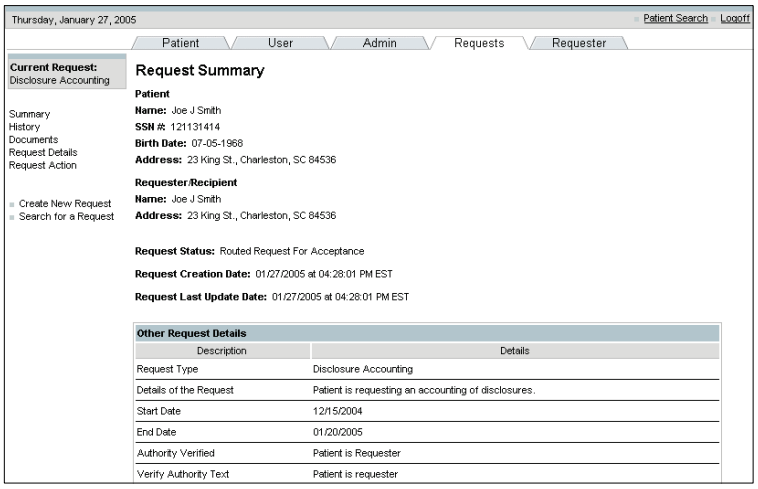
The Request Action window provides you with various accounting disclosure actions, which are shown in this table:

Accounting for Disclosures - Request Actions	
Action	Description
Route to My Worklist	Allows you to place it in your worklist to follow up when appropriate
Process Request Now	Allows you to place it in your worklist for approval
Deny Request Now	Allows you to deny the disclosure
Route to Privacy Specialist	Allows you to pass the disclosure on to another Privacy Specialist to be processed, as established in a User-to-User Relationship
Route to Other User	Allows you to pass the disclosure back to another user to process the letter generation after approving or denying the request, as established in a User-to-User Relationship

13. Click on the Save button.



- The Request Summary screen will display.



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

5.3.5 Approve Accounting of Disclosures

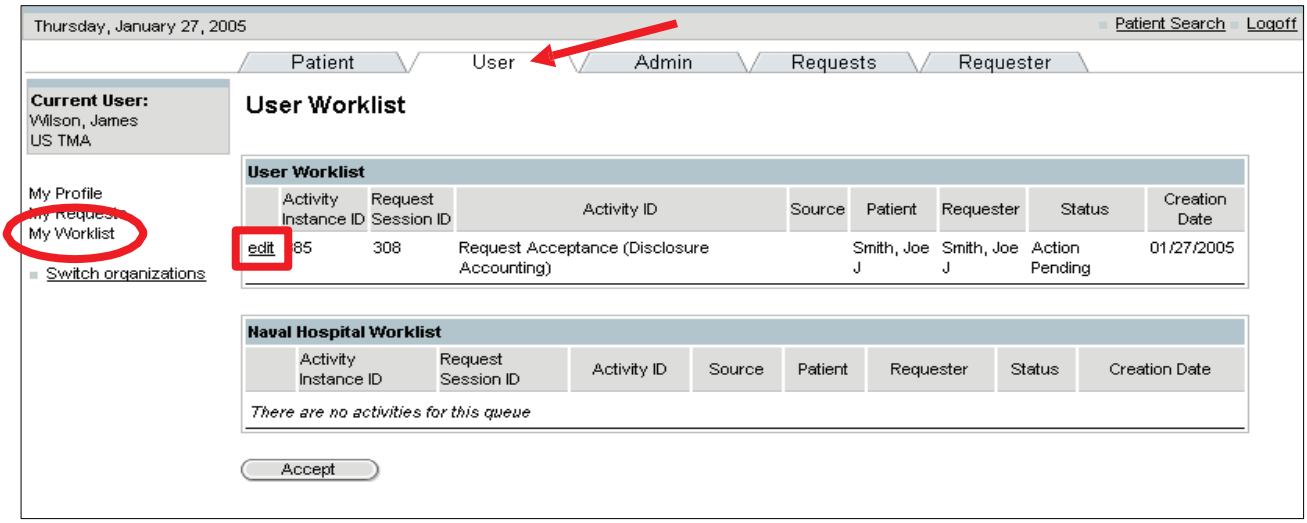
A patient may ask for an Accounting of Disclosures at any time. PHIMT allows for a quick reporting of this accounting.

To approve an accounting of a disclosure:

1. Select the User Tab.

2. Select the My Worklist hyperlink.

3. Select the Edit hyperlink for the disclosure accounting that you want to approve.



- The Edit Activity Details screen will display.

4. Select Accepted from the Activity Status drop-down box.

5. Click on the Update button.

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

Thursday, January 27, 2005 Patient Search Logoff

Patient User Admin Requests Requester

Current Request: Disclosure Accounting

Summary
History
Documents
Request Details
Request Action

Create New Request
Search for a Request

Edit Activity Details

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

Instructions
Request Acceptance (Disclosure Accounting)

Activity Status *(new activity status code)*
Accepted
Action Pending
Accepted
Denied
Cancelled
Route to Privacy Specialist
Route to Other User

describe part of request that was approved)

(for partially approved requests, describe part of request that was denied)

Comments *(enter details about this activity)*

Update

- The Disclosure Accounting Request screen will display with the approved accounting of disclosures.

  NOTE: The accounting disclosure (Activity Instance ID 85) is no longer shown in your User Worklist.

Thursday, January 27, 2005 Patient Search Logoff

Patient User Admin Requests Requester

Current Request: Disclosure Accounting

Summary
History
Documents
Request Details
Request Action

Create New Request
Search for a Request

Disclosure Accounting Request

Reportable Disclosures ***(checked disclosures will be included in the disclosure accounting report, suspended disclosures are highlighted in red)***

Include	Disclosure ID	Date	Type	Origin	Receiving Entity	PHI	Purpose	Status
☑	286	01/27/2005	Law Enforcement Purposes	US TMA	Law Offices of Joe Gibbs	Complete Health Record(s)	Law Enforcement	Complete
☑	137	07/27/2004	Law Enforcement Purposes	325th Medical Group	Joe J Smith	Laboratory Test(s)	Law Enforcement	Complete
☑	100	07/20/2004	Research Purposes	325th Medical Group	Home of Michele	History and Physical Examination, Progress Notes	Medical	Complete

Disclosures Accounting Suspensions

Suspension ID	Suspended Disclosure	Identifier	Start Date	End Date	Comments
26	The specific disclosure of type **Law Enforcement Purposes** that occured on **07/27/2004** with a disclosure ID of **137**		07/27/2004	07/27/2004	

Create

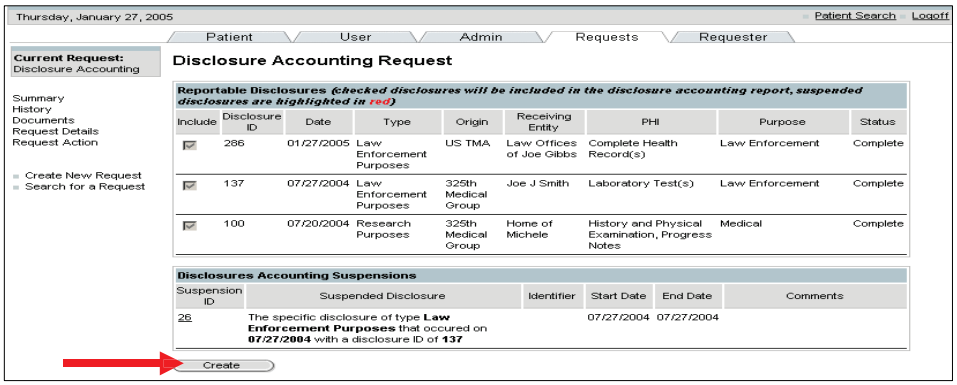
5.3.6 Generate an Accounting of Disclosures Report

An accounting of disclosures report is a summary of all of the disclosures made for a particular patient. Once a request has been approved, an accounting of disclosures report can be generated. Pending disclosures will not display in the report.

The Privacy Specialist has the option to route the report back to the originator.

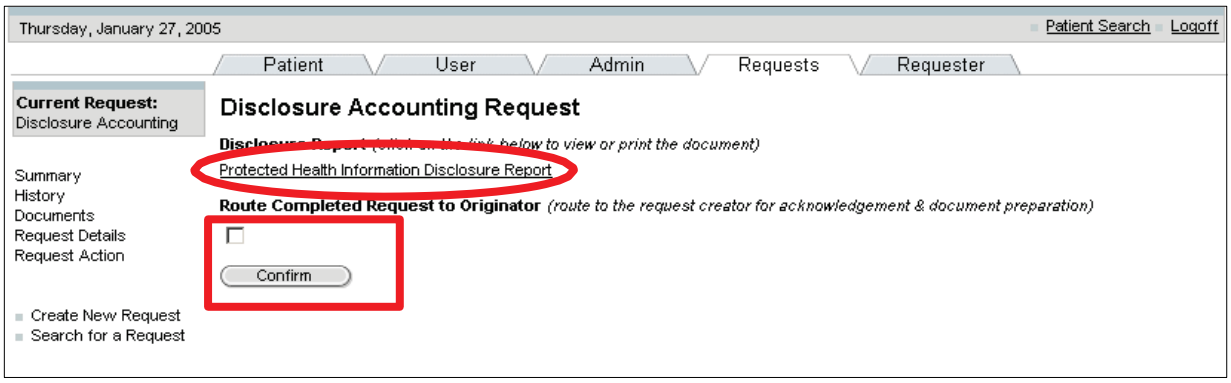
To generate an Accounting of Disclosures Report:

1. From the Disclosure Accounting Request screen, click on the Create button to generate the report.



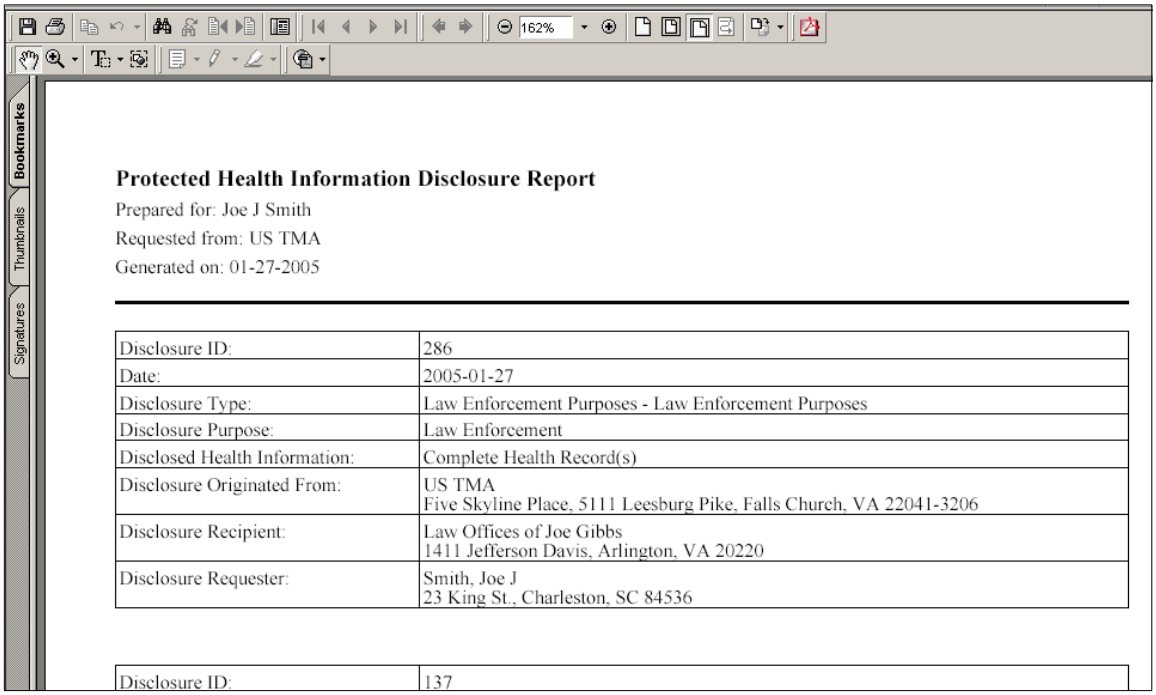
2. Select the "Protected Health Information Disclosure Report" hyperlink to create the report.

NOTE: If you want to route the completed request back to the originator, place a check in the box and click on confirm.



- The Accounting of Disclosures Report will display.

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



Protected Health Information Disclosure Report

Prepared for: Joe J Smith
Requested from: US TMA
Generated on: 01-27-2005

Disclosure ID:	286
Date:	2005-01-27
Disclosure Type:	Law Enforcement Purposes - Law Enforcement Purposes
Disclosure Purpose:	Law Enforcement
Disclosed Health Information:	Complete Health Record(s)
Disclosure Originated From:	US TMA Five Skyline Place, 5111 Leesburg Pike, Falls Church, VA 22041-3206
Disclosure Recipient:	Law Offices of Joe Gibbs 1411 Jefferson Davis, Arlington, VA 20220
Disclosure Requester:	Smith, Joe J 23 King St., Charleston, SC 84536

Disclosure ID:	137

5.3.7 Create a Suspension

The covered entity shall temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official…DoD 6025.18-R C13.1.2.1 Two types of disclosures can be suspended: Law enforcement purposes and Health oversight activities. Privacy Specialists have the ability to enter an accounting suspension in two ways: Specific disclosure and Type of disclosure. As a best practice, it is recommended that users enter in an accounting suspension using the Specific disclosure hyperlink. Once a suspension has been entered, all users can view it.

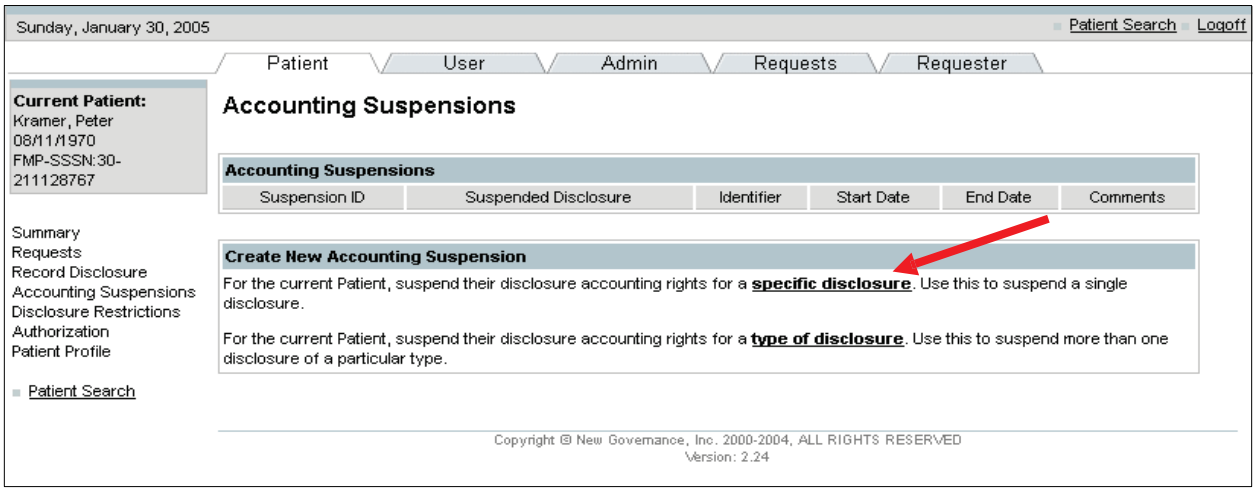
To create a suspension:

1. Search for and select a patient record.

2. Select the Accounting Suspensions hyperlink.

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

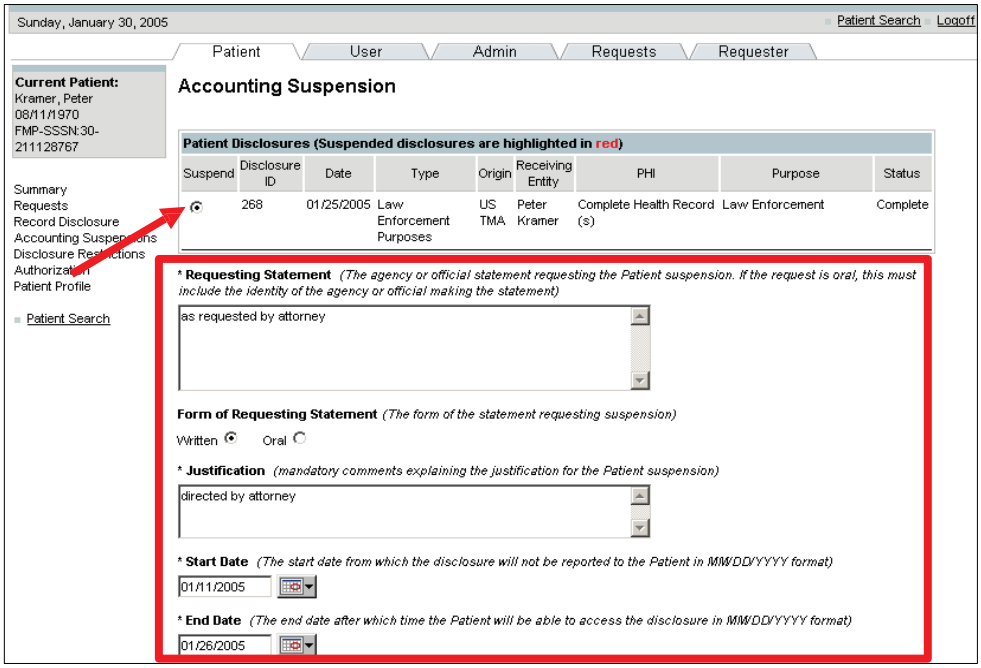
3. Select the Specific Disclosure hyperlink.



4. Click on the radio button for the disclosure you want to suspend.

5. Enter the suspension details: requesting statement and form, justification, and start and end date.

NOTE: All required fields are marked with an asterisk.



6. Scroll to the bottom of the screen and 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.

Form of Requesting Statement *(The form of the statement requesting suspension)*

Written ◉ Oral ○

* **Justification** *(mandatory comments explaining the justification for the Patient suspension)*

directed by attorney

* **Start Date** *(The start date from which the disclosure will not be reported to the Patient in MM/DD/YYYY format)*

01/30/2005

* **End Date** *(The end date after which time the Patient will be able to access the disclosure in MM/DD/YYYY format)*

02/05/2005

Identifier *(The OPTIONAL identifier for the suspension, could be a case number, warrant number, subpoena ID, etc.)*

Comments *(OPTIONAL general comments about or for the Patient)*

Save

7. Select the Summary hyperlink.

Sunday, January 30, 2005 — Patient Search | Logoff

Patient | User | Admin | Requests | Requester

Current Patient:
Kramer, Peter
08/11/1970
FMP-SSSN:30-211128767

Summary
Requests
Record Disclosure
Accounting Suspensions
Disclosure Restrictions
Authorization
Patient Profile

Patient Search

Accounting Suspension

Patient Disclosures (Suspended disclosures are highlighted in red)

Suspend	Disclosure ID	Date	Type	Origin	Receiving Entity	PHI	Purpose	Status
◉	268	01/25/2005	Law Enforcement Purposes	US TMA	Peter Kramer	Complete Health Record (s)	Law Enforcement	Complete

* **Requesting Statement** *(The agency or official statement requesting the Patient suspension. If the request is oral, this must include the identity of the agency or official making the statement)*

as requested by attorney

Form of Requesting Statement *(The form of the statement requesting suspension)*

Written ◉ Oral ○

* **Justification** *(mandatory comments explaining the justification for the Patient suspension)*

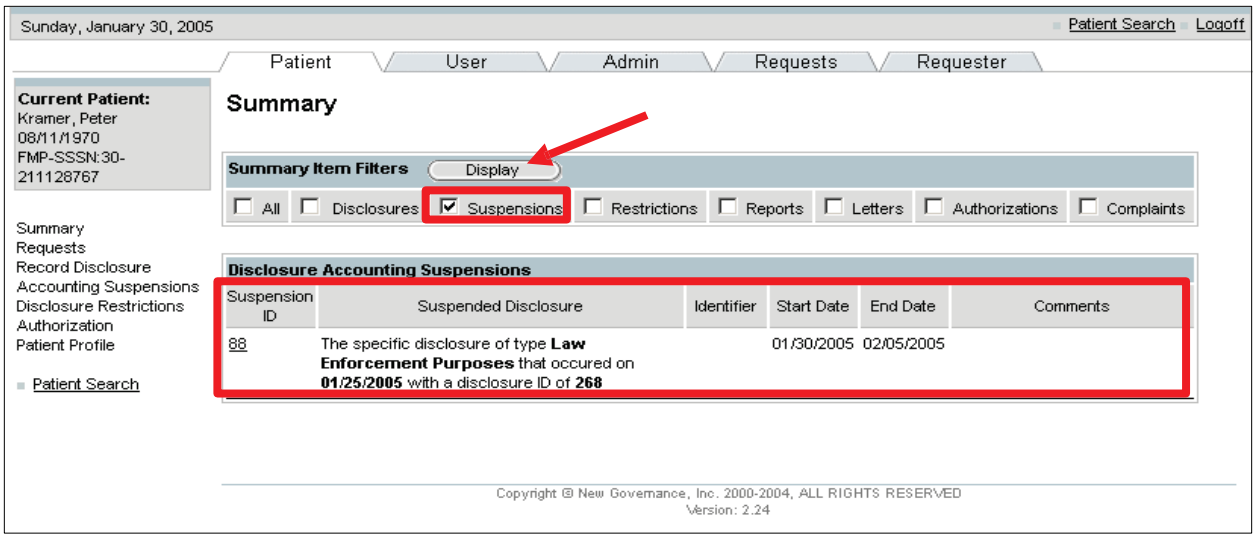
directed by attorney

8. Check the Suspensions checkbox.

9. Click on the Display button.

- The Disclosure that you suspended will display in the Disclosure Accounting Suspensions section.

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



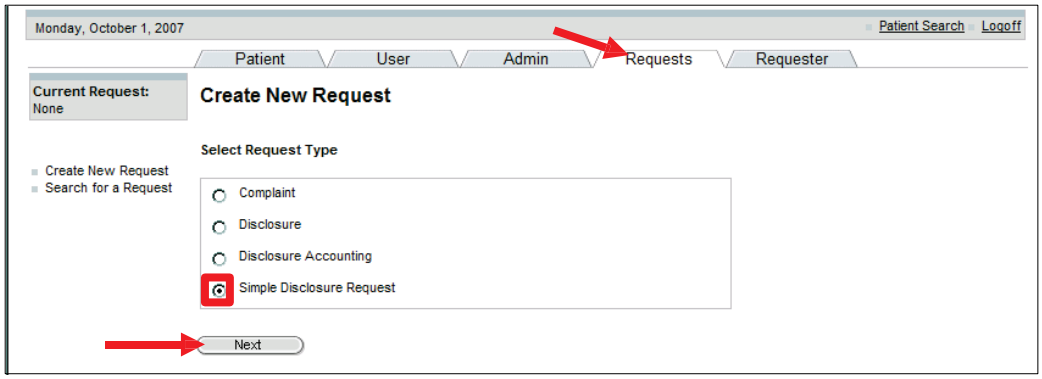
5.3.8 Record a Simple Disclosure

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.

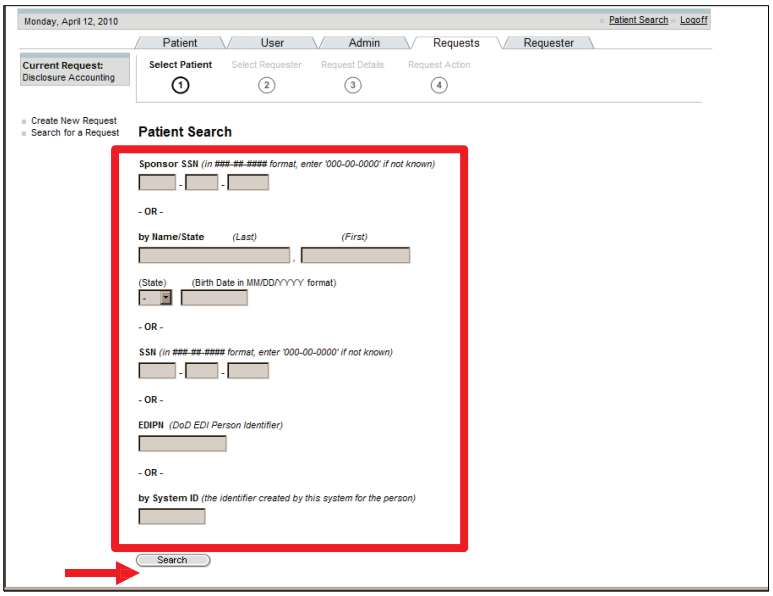
2. Click on the Simple Disclosure radio button.

3. Click on the Next button.

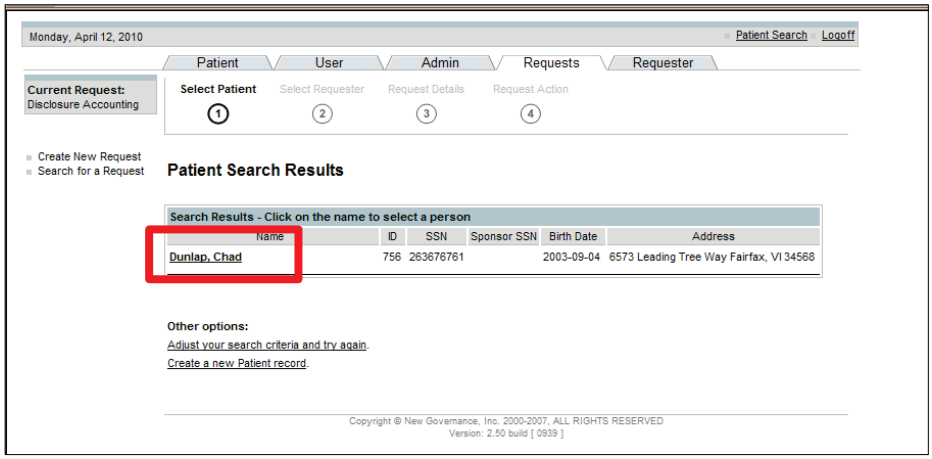


4. Search for the Patient.

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

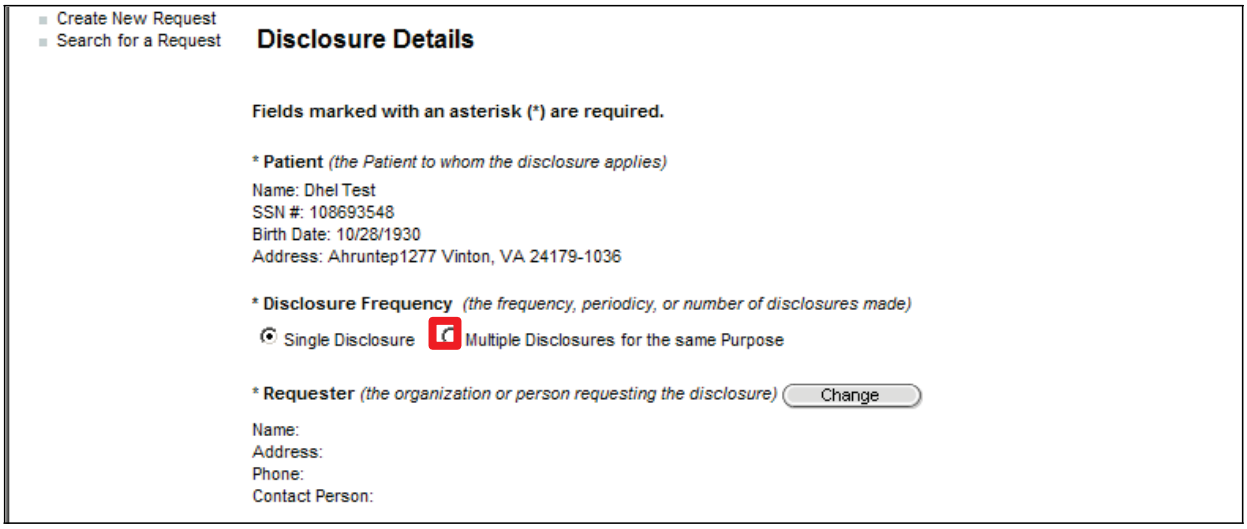


5. Select patient from the Search Results screen.



6. 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.

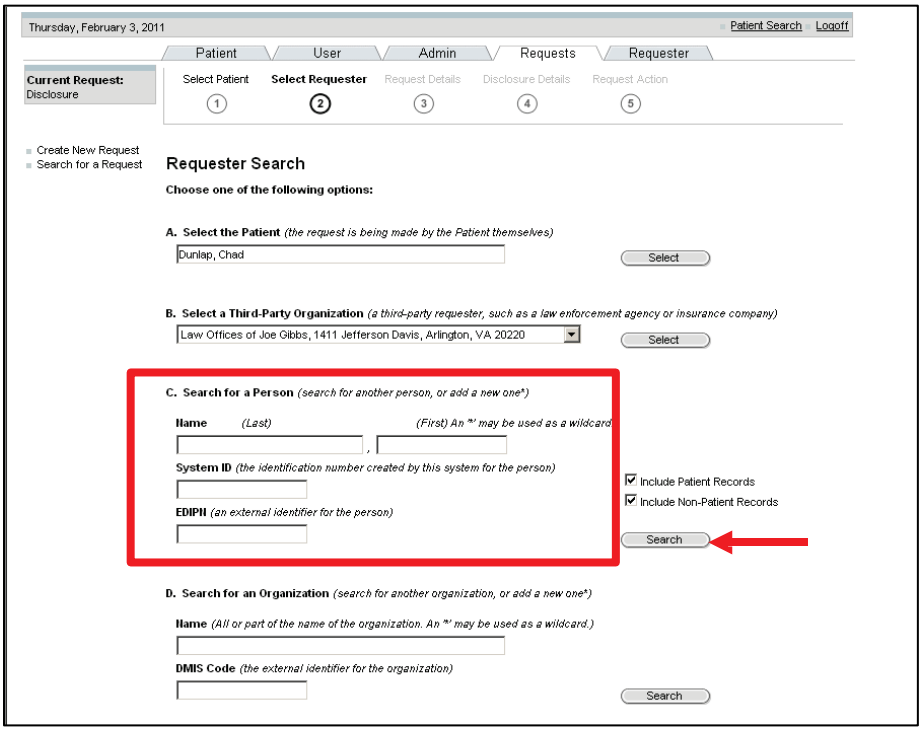


7. The Disclosure Frequency fields will appear.

8. Select the occurrence, start date, and end date. (Users can select from the drop-down, 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 Requester Change button.

10. Search for the Requester.



11. Select the Requester from the Search Results screen.

Monday, April 12, 2010 Patient Search Logoff

Patient User Admin Requests Requester

Current Requester: None

Requester Search Results

Requester Summary
Requester Requests
Requester Profile

Requester Search

Search Results - Click on the name to select a requester

Name	ID	Address
Smith, John	253	1456 Terry Ln., Warston, MT 12554
Smith, John	749	13450, Bob Wilson, San Diego, CA 92134
Smith, John 2	748	34800, Suite 4, San Diego, CA 92134-9999

Other options:
Adjust your search criteria and try again.
Create a new requester as a person.
Create a new requester as an organization.

Copyright © New Governance, Inc. 2000-2007, ALL RIGHTS RESERVED
Version: 2.50 build [0939]

12. Select the Requester Identity Verified drop-down.

13. Select the Disclosure Type from the drop-down.

NOTE: The disclosure description will automatically be populated when the disclosure type is selected.

* **Requester** *(the organization or person requesting the disclosure)* Change

Name: Smith, John
Address: 1456 Terry Ln., Warston, MT 12554
Phone:
Contact Person:

* **Requester Identity Verified** *(was the requester's identity verified?)*

Social Security Number

Description of Requester Identity Verification *(required if requester identity verification was defined as 'other')*

* **Request Date** *(the disclosure request date in MM/DD/YYYY format)*

05/14/2007

* **Recipient** *(the organization or person where the disclosure went)* Change

Name: Smith, John
Address: 1456 Terry Ln., Warston, MT 12554
Phone:
Contact Person:

* **Disclosure Type** *(the type of disclosure)*

Specialized Government Functions (Active Duty Disclosure)

Disclosure Description *(a read-only description and example of the disclosure type selected above)*

Use and disclose the PHI of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission. The purposes for which any and all of the PHI of an individual who is a member of the Armed Forces may be used or disclosed are: 1) To determine the member's fitness for duty 2) To determine the member's fitness to perform any particular mission, assignment, order, or duty, including compliance with any actions required as a precondition to performance of such mission, assignment, order, or duty. 3) To carry out activities under the authority of DoD Directive 6490.2. 4) To report on casualties in any military operation or activity in accordance with applicable military regulations or procedures. 5) To carry out any other activity necessary to the proper execution of the mission of the Armed Forces

14. Select the Disclosure Purpose from the drop-down.

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

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

Disclosure Date *(the disclosure date in MM/DD/YYYY format)*

06/14/2007

* **Origin Organization** *(where the disclosure originated)*

US TMA

* **Disclosure Purpose** *(the purpose of the disclosure)*

Medical

Other/Details (*Required for all Multiple Disclosures):

To determine the member's fitness to perform any particular mission, assignment, order, or duty, including compliance with any actions rquired as a precondition to performance of such mission,

* **Protected Health Information Description** *(the description of the Protected Health Information disclosed)*

- [x] Complete Health Record(s)
- [ ] Consultation Report(s)
- [ ] Discharge Summary
- [ ] History and Physical Examination
- [ ] Laboratory Test(s)
- [ ] Operative Report(s)
- [ ] Pathology Report(s)
- [ ] Progress Notes

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

17. Type the document title. (If applicable)

18. Click on the browse button to attach the document. (It applicable)

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

20. 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.

You may attach up to three documents, with file size not exceeding 2M

FILE 1: Document Title *(enter this document's title)*

Test

Please select a file you wish to attach

C:\Documents and Settings\514708\Desktop\PHIMT TEST.doc Browse...

FILE 2: Document Title *(enter this document's title)*

Please select a file you wish to attach

Browse...

FILE 3: Document Title *(enter this document's title)*

Please select a file you wish to attach

Browse...

Action *(action for this request)*

Route to Privacy Specialist

Back Save

- 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

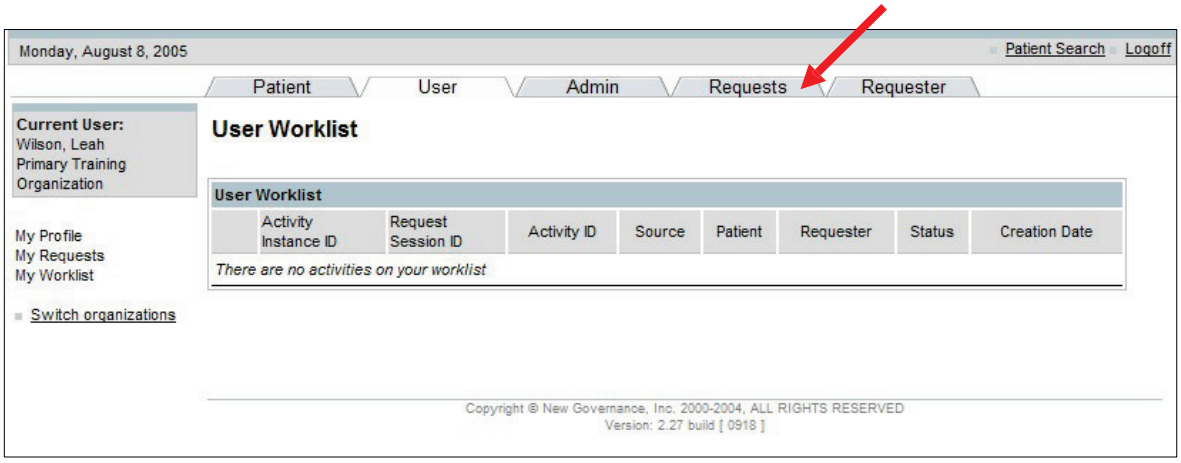
Description	Details
Request Type	Simple Disclosure Request
Disclosure Type	Type: Specialized Government Functions (Active Duty Disclosure), ID: 676, Date: 06/14/2007
Route to Privacy Specialist	Yes
Identity Verified Text	Social Security Number

5.3.9 Record Complaints

NOTE: To document a complaint in the PHIMT, you must complete three steps: Record the Complaint, Receive the Complaint, and Update the Complaint after the investigation.

To Record a Complaint:

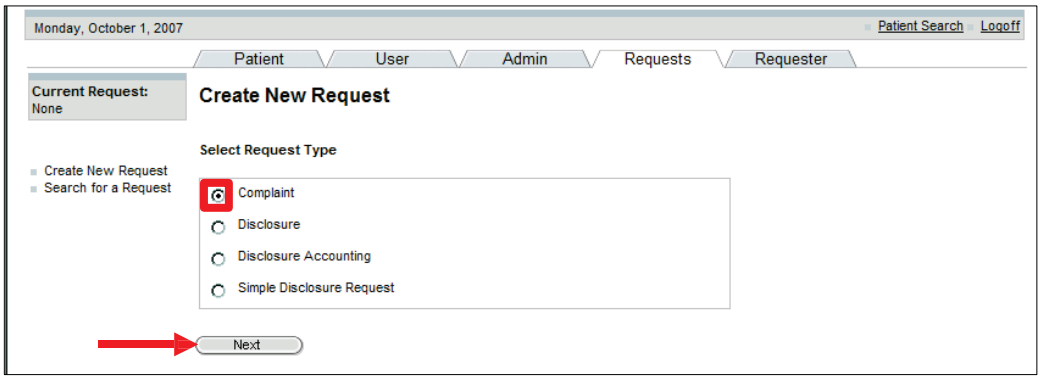
1. Select the Requests Tab.



- The Create New Request Screen will appear.

2. Click the Complaint radio button.

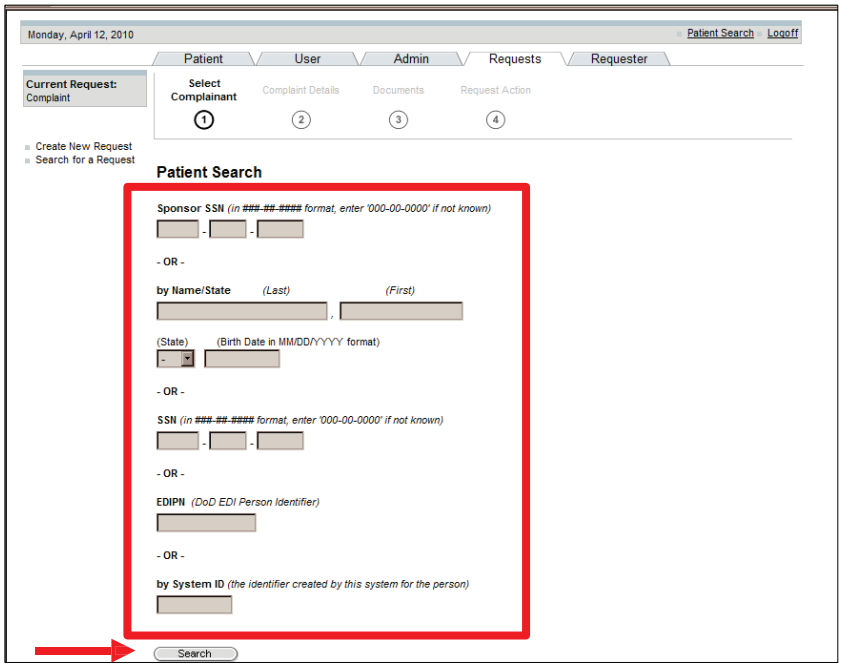
3. Click on the Next button.



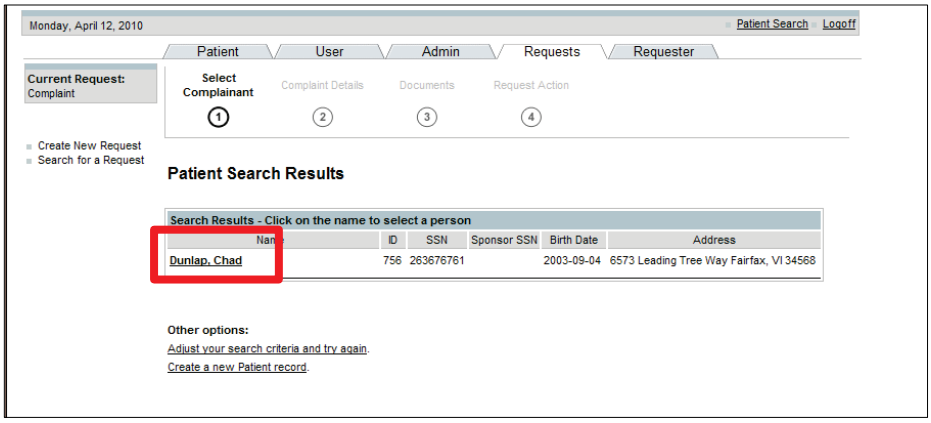
4. Search for the patient.

5. 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.



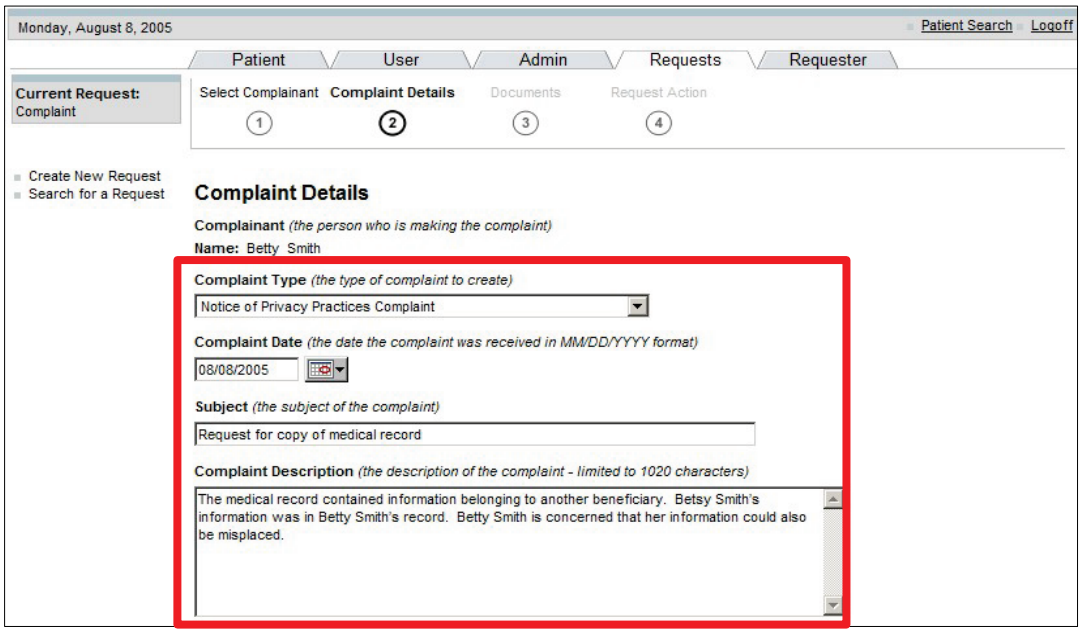
6. Select the Patient.



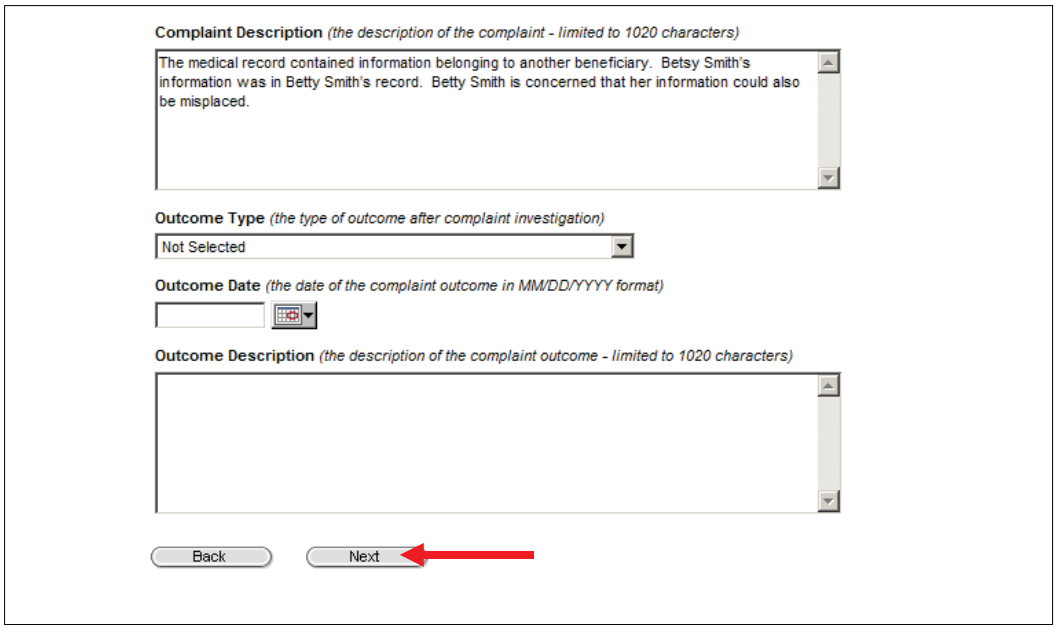
- The Complainant Details Screen will appear.

7. Complete the Complaint Details: complaint type, complaint date, subject and description of the complaint.

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



8. Scroll to the bottom of the screen and click on the Next button.



9. To attach any documents, type in the document title.

10. Click on the Browse button to attach the file.

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.

Monday, August 8, 2005 Patient Search Logoff

Patient User Admin Requests Requester

Current Request: Complaint

Select Complainant (1) Complaint Details (2) Documents (3) Request Action (4)

Create New Request
Search for a Request

Documents

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

FILE 1: Document Title *(enter this document's title)*
Complaint Form

Please select a file you wish to attach
C:\Documents and Settings\514708\Desktop\Complaint form.doc Browse...

FILE 2: Document Title *(enter this document's title)*

Please select a file you wish to attach
Browse...

FILE 3: Document Title *(enter this document's title)*

Please select a file you wish to attach
Browse...

Back Next

- The Request Action Screen will appear.

12. Select the appropriate action from the drop-down box.

13. Click on the Save button.

Monday, August 8, 2005 Patient Search Logoff

Patient User Admin Requests Requester

Current Request: Complaint

Select Complainant (1) Complaint Details (2) Documents (3) Request Action (4)

Create New Request
Search for a Request

Request Action

Patient
Name: Betty Smith
SSN #: 222222222
Birth Date: 07-03-1975
Address: 1125 West Pleasant View Dr., Ogden, UT 98277

Details of the Request *(requester's comments about the scope of this request)*
The medical record contained information belonging to another beneficiary. Betsy Smith's information was in Betty Smith's record. Betty Smith is concerned that her information could also be misplaced.

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 My Worklist

Back Save

- The Request Summary Screen will display.

To Receive a Complaint:

1. Select the User Tab.

Monday, August 8, 2005 Patient Search Logoff

Patient User Admin Requests Requester

Current Request: Complaint

Summary
History
Documents
Complaint Details

Create New Request
Search for a Request

Request Summary

Patient
Name: Betty Smith
SSN #: 222222222
Birth Date: 07-03-1975
Address: 1125 West Pleasant View Dr., Ogden, UT 98277

Request Status: Routed Complaint to be Received

Request Creation Date: 08/08/2005 at 01:29:18 PM EDT

Request Last Update Date: 08/08/2005 at 01:29:19 PM EDT

Other Request Details

Description	Details
Request Type	Complaint
Details of the Request	The medical record contained information belonging to another beneficiary. Betsy Smith's information was in Betty Smith's record. Betty Smith is concerned that her information could also be misplaced.
ComplaintID	200
File1	Complaint form.doc
FileTitle1	Complaint Form

- The complaint will appear in the User Worklist.

2. Select the Edit hyperlink.

Monday, August 8, 2005 Patient Search Logoff

Patient User Admin Requests Requester

Current User:
Wilson, Leah
Primary Training Organization

My Profile
My Requests
My Worklist

Switch organizations

User Worklist

User Worklist

	Activity Instance ID	Request Session ID	Activity ID	Source	Patient	Requester	Status	Creation Date
edit	755	537	Complaint to be Received		Smith, Betty		Action Pending	08/08/2005

- The Edit Activity Details Screen will appear.

3. Select Received from the Activity Status drop-down box.

4. Click on the Update button.

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

Monday, August 8, 2005 Patient Search Logoff

Patient | User | Admin | Requests | Requester

Current Request: Complaint

Summary
History
Documents
Complaint Details

Create New Request
Search for a Request

Edit Activity Details

Patient
Name: Betty Smith
SSN #: 222222222
Birth Date: 07-03-1975
Address: 1125 West Pleasant View Dr., Ogden, UT 98277

Instructions
Complaint to be Received

Activity Status *(new activity status code)*
Received

Comments *(enter details about this activity)*

Update

Request Session Details

Description	Details
Request Type	Complaint

- The Edit Request Screen will appear.

5. Select the Complaint-Received Letter hyperlink in the Letters and Attached Documents field.

Monday, August 8, 2005 Patient Search Logoff

Patient | User | Admin | Requests | Requester

Current Request: Complaint

Summary
History
Documents
Complaint Details

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
756	537	Complaint Investigation		Smith, Betty		Leah Wilson	Action Pending	08/08/2005
755	537	Complaint to be Received		Smith, Betty		Leah Wilson	Received	08/08/2005

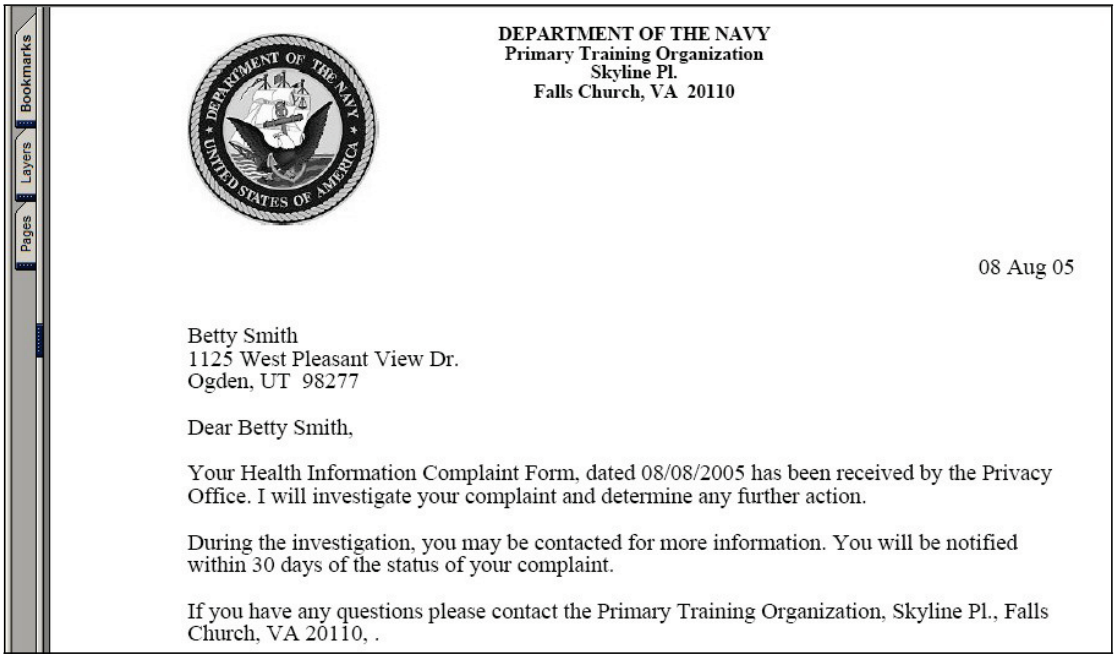
Request Session Details Edit

Description	Details
Request Type	Complaint
Details of the Request	The medical record contained information belonging to another beneficiary. Betsy Smith's information was in Betty Smith's record. Betty Smith is concerned that her information could also be misplaced.
ComplaintID	200
File1	Complaint form.doc
FileTitle1	Complaint Form

Letters and Attached Documents Attach

ID	Date	Title
753	08/08/2005	Complaint - Received Letter
752	08/08/2005	Complaint Form

- The Complaint Received Letter is generated.



DEPARTMENT OF THE NAVY
Primary Training Organization
Skyline Pl.
Falls Church, VA 20110

08 Aug 05

Betty Smith
1125 West Pleasant View Dr.
Ogden, UT 98277

Dear Betty Smith,

Your Health Information Complaint Form, dated 08/08/2005 has been received by the Privacy Office. I will investigate your complaint and determine any further action.

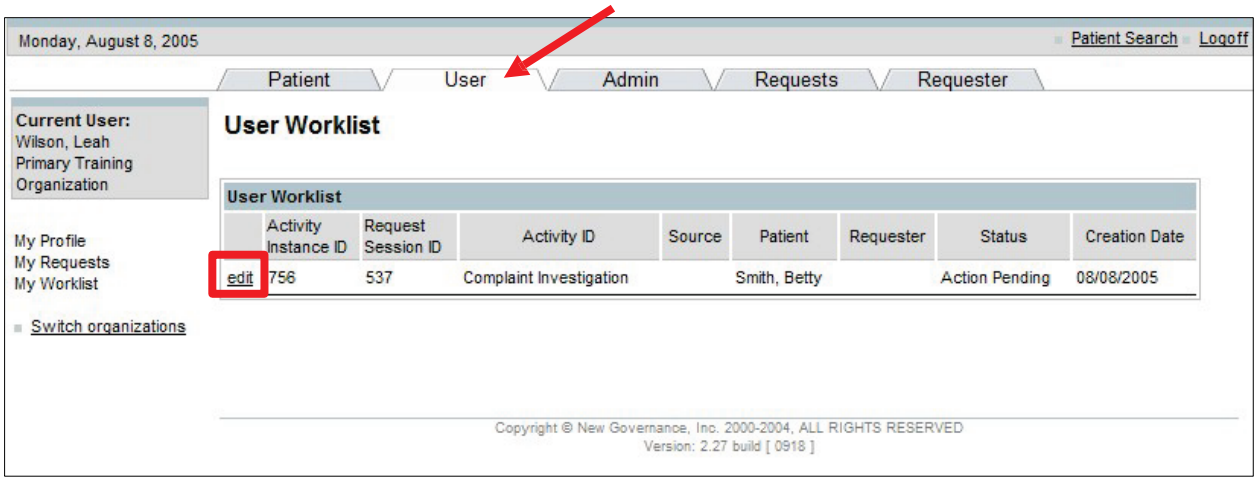
During the investigation, you may be contacted for more information. You will be notified within 30 days of the status of your complaint.

If you have any questions please contact the Primary Training Organization, Skyline Pl., Falls Church, VA 20110, .

To Update the Complaint:

1. Select the User Tab.

2. Select the Edit hyperlink.



3. Select Completed from the Activity Status drop-down box.

4. Click on the Update button.

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

Monday, August 8, 2005 Patient Search Logoff

Patient | User | Admin | Requests | Requester

Current Request: Complaint

Summary
History
Documents
Complaint Details

Create New Request
Search for a Request

Edit Activity Details

Patient
Name: Betty Smith
SSN #: 222222222
Birth Date: 07-03-1975
Address: 1125 West Pleasant View Dr., Ogden, UT 98277

Instructions
Complaint Investigation

Activity Status *(new activity status code*
Completed

Comments *(enter details about this activity)*

Update

Request Session Details

Description	Details
Request Type	Complaint
Details of the Request	The medical record contained information belonging to another beneficiary. Betsy Smith's information was in Betty Smith's record. Betty Smith is concerned that her information could also be misplaced.

- The Complaint Details Screen will appear.

5. Complete the Complaint Details: type, date and description.

6. Click on the Update button.

Complaint Description *(the description of the complaint - limited to 1020 characters)*
The medical record contained information belonging to another beneficiary. Betsy Smith's information was in Betty Smith's record. Betty Smith is concerned that her information could also be misplaced.

Outcome Type *(the type of outcome after complaint investigation)*
Substantiated

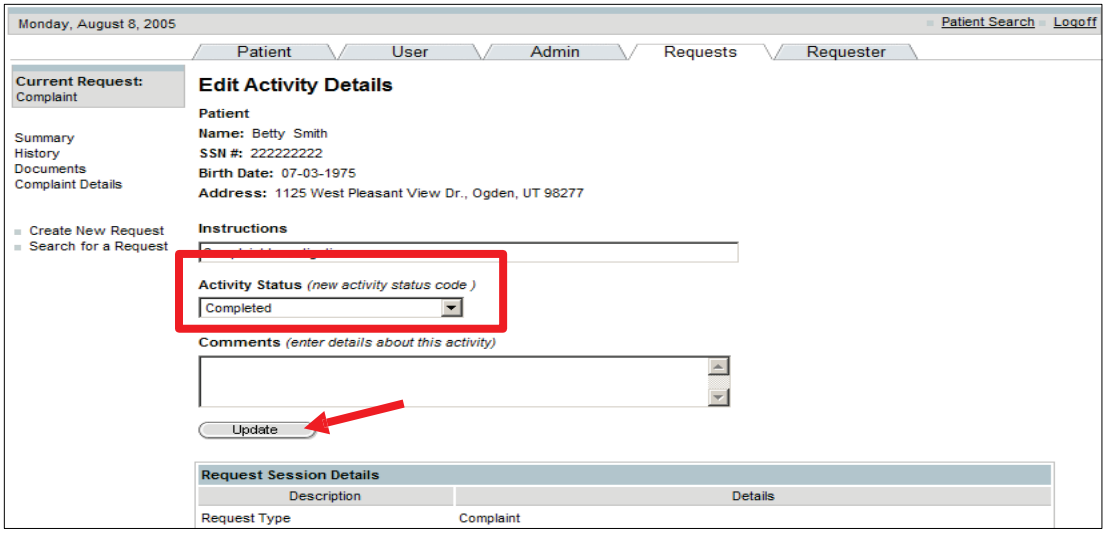
Outcome Date *(the date of the complaint outcome in MM/DD/YYYY format)*
08/08/2005

Outcome Description *(the description of the complaint outcome - limited to 1020 characters)*
The complaint was found to be validated. Information was misfiled by the personnel and medical records department. They have been retrained on HIPAA and counseled. Policies were reviewed and strengthened.

Update

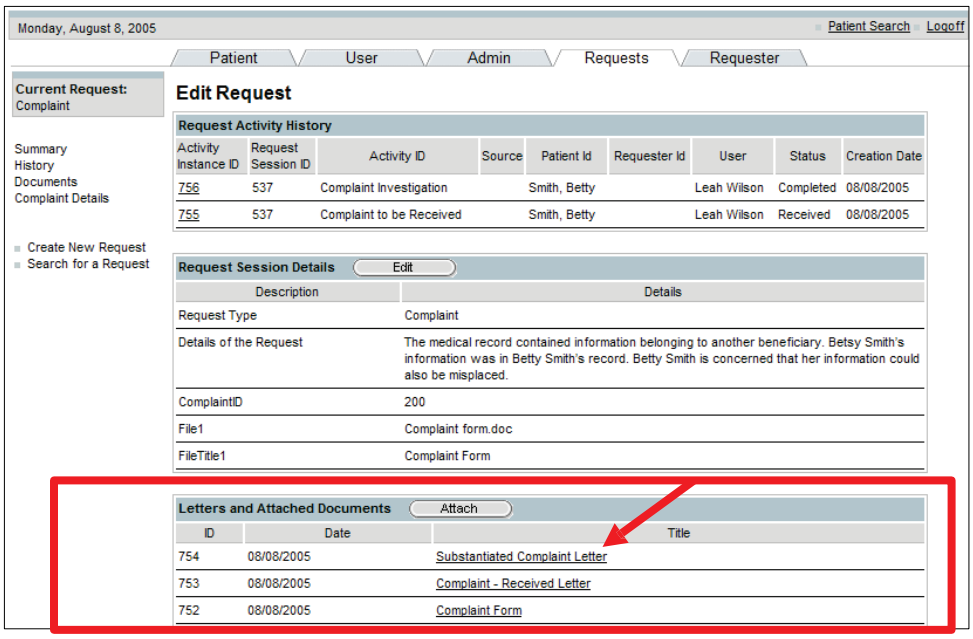
7. Select Completed from the Activity Status drop-down box.

8. Click on the Update button.



- The Edit Request Screen will appear.

9. Select the Substantiated Complaint Letter hyperlink.



- The Substantiated Complaint Letter is generated.

Falls Church, VA 20110

08 Aug 05

Betty Smith
1125 West Pleasant View Dr.
Ogden, UT 98277

Dear Betty Smith,

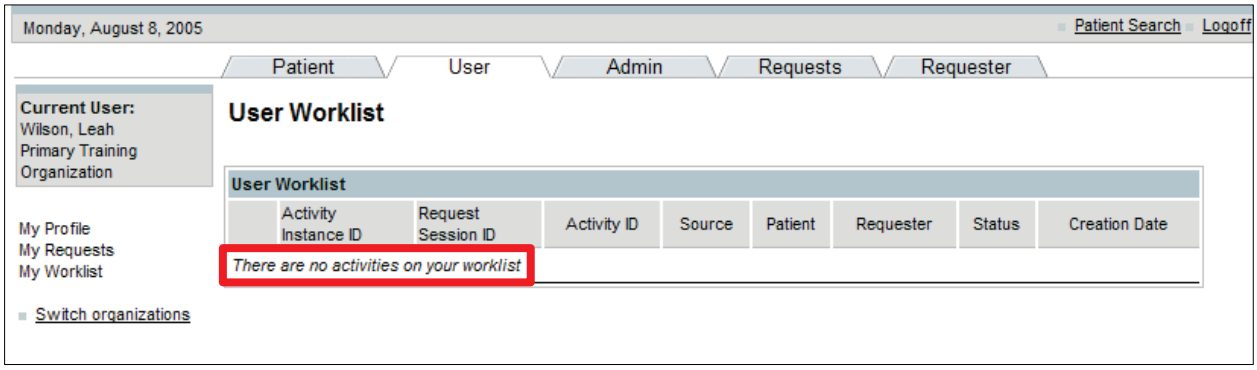
The investigation of your Health Information Privacy Complaint, regarding Request for copy of medical record, is now complete.

The allegations within your complaint are substantiated. As a result of your complaint, the following actions will take place:

The complaint was found to be validated. Information was misfiled by the personnel and medical records department. They have been retrained on HIPAA and counseled. Policies were reviewed and strengthened.

If you have any questions, please contact Primary Training Organization, Skyline Pl., Falls Church, VA 20110, .

- The Complaint Activity will no longer appear in the User Worklist.



5.3.10 Record a Disclosure Restriction

As a Privacy Specialist you are able to enter a Restriction of Disclosure or terminate a Restriction of Disclosure. Restriction of Disclosures allows members to restrict uses and disclosure of their PHI.

When selecting the Disclosure Type if you determine that you need a new type of disclosure, contact the PHIMT help desk.

NOTE: Ensure that you enter specific details of what information is being restricted. It is important to be specific in this entry because it will provide other staff members with the details about the individual and organization, and about the restrictions on the disclosure.

To record a disclosure restriction:

1. Search for and select a patient record.

2. Select the Disclosure Restrictions hyperlink.

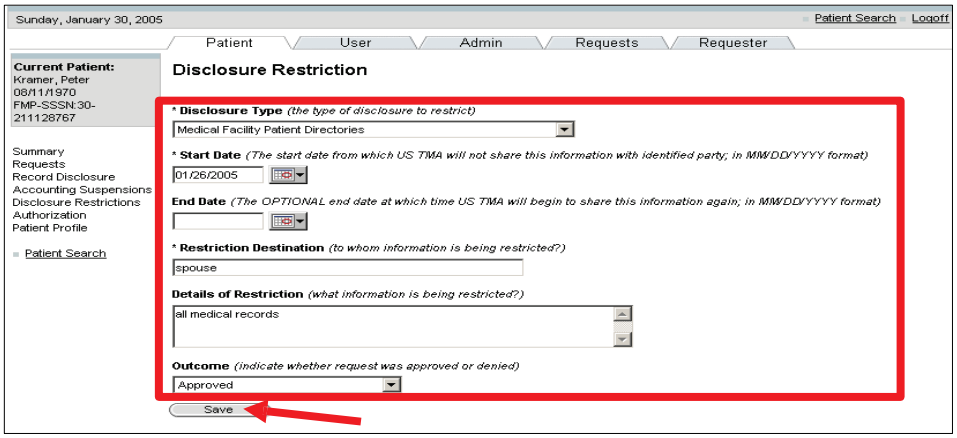
3. Click on the New button in the Disclosures Restrictions box.

4. Enter the Disclosure Restriction details: disclosure type, start and end date, restriction destination (to whom information is being restricted) and details.

5. Select Approved or Denied from the Outcome drop-down box.

6. 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.

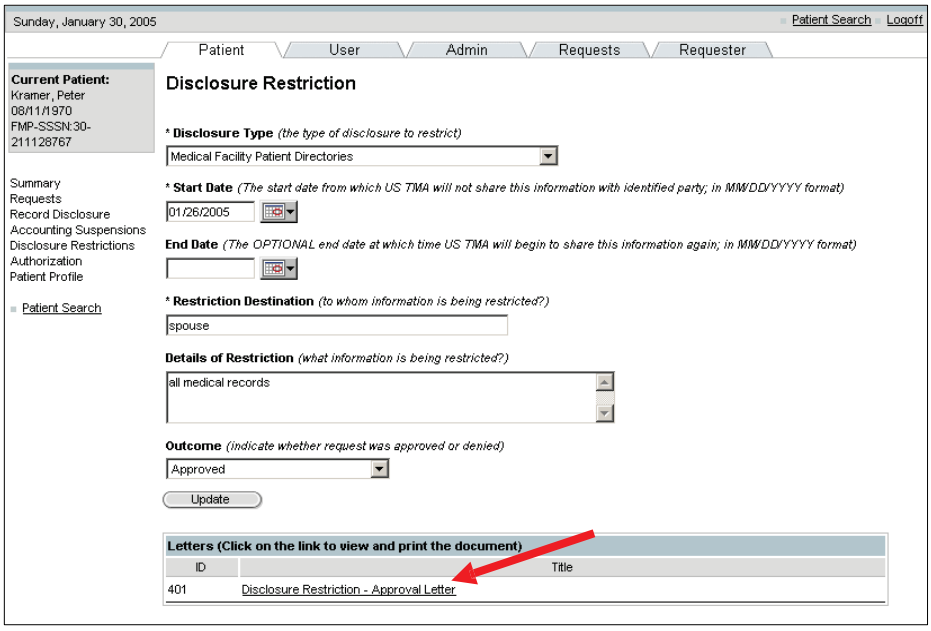


- The Patient Disclosure Restriction screen re-appears with your information. The Save button has changed to an Update button.

Once you have approved or denied the disclosure restriction you have the ability to generate an approval or denial letter. The letter will be pre-populated with the information that you entered for that particular restriction.

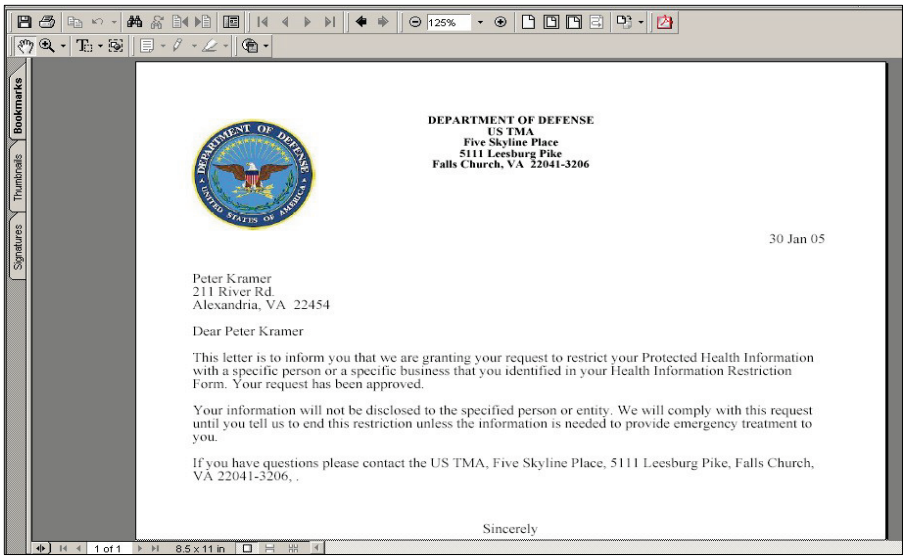
To print the Approval or Denial Letter:

1. Select the title of the letter in the Letters box on the Patient Disclosure Restriction screen.



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

- The Approval/Denial letter is generated.



DEPARTMENT OF DEFENSE
US TMA
Five Skyline Place
5111 Leesburg Pike
Falls Church, VA 22041-3206

30 Jan 05

Peter Kramer
211 River Rd.
Alexandria, VA 22454

Dear Peter Kramer

This letter is to inform you that we are granting your request to restrict your Protected Health Information with a specific person or a specific business that you identified in your Health Information Restriction Form. Your request has been approved.

Your information will not be disclosed to the specified person or entity. We will comply with this request until you tell us to end this restriction unless the information is needed to provide emergency treatment to you.

If you have questions please contact the US TMA, Five Skyline Place, 5111 Leesburg Pike, Falls Church, VA 22041-3206, .

Sincerely

5.3.11 Generate Authorizations

Privacy Specialist can record an Authorization by the patient when there is an exchange of PHI that occurs outside of the treatment, payment, or healthcare options.

- Select Type of authorization. NOTE: Based on the Type selected, the following fields are populated; however, that data can be changed.

- Enter PHI to be released as it was entered on the authorization form. NOTE: The greater the detail that is provided by the patient, the easier it will be to respond to the request at the time of disclosure.

NOTE: Enter either the Authorization Expiration or an Action Completed date; not both. If there is no expiration date, then enter text in the Action Completed field (ex. Authorization to remain in effect until revoked.)

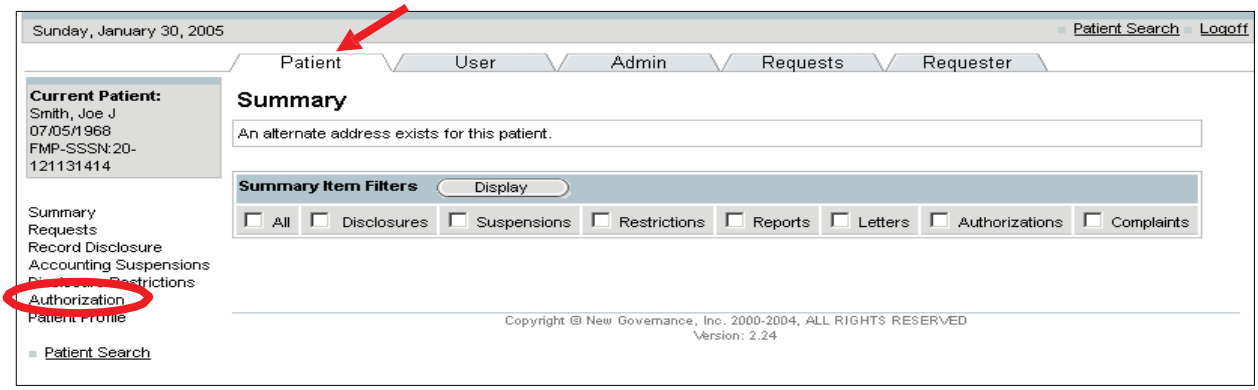
NOTE: Once the authorization has been manually signed you can go back into the particular authorization and select the Signed checkbox and enter the date of the signature using MM/DD/YYYY format or the calendar icon to select a date.

To generate an authorization:

1. Select the Patient Tab.

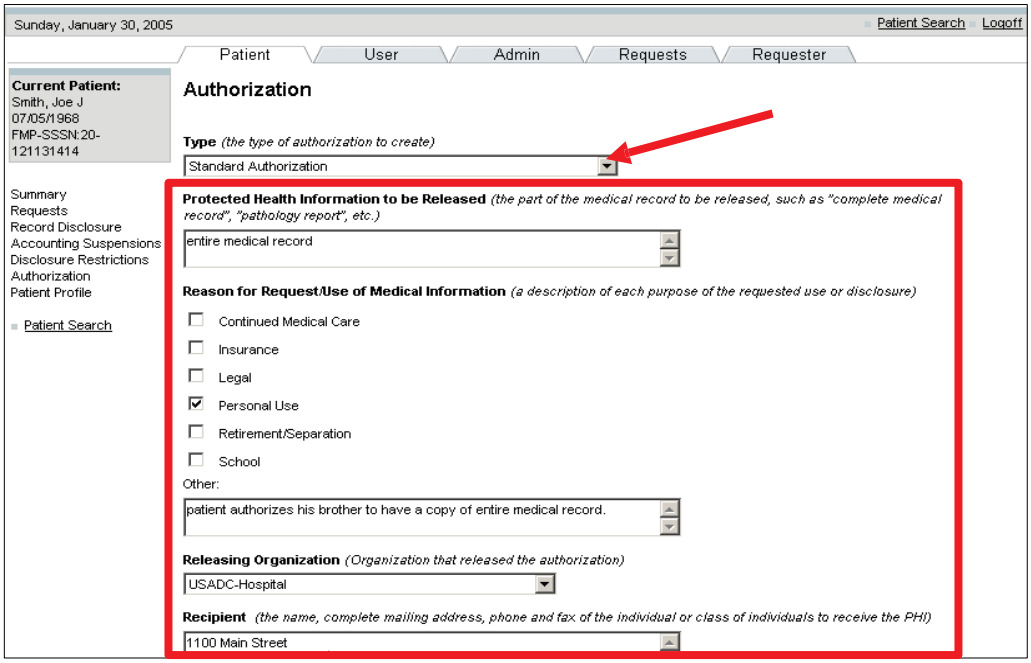
2. Search for and select the patient record.

3. Select the Authorization hyperlink.



4. Select the Authorization Type from the drop-down box.

5. Enter the Authorization Details: reason for request, releasing organization, and recipient.



6. Scroll down the screen and enter: authorization start and expiration date, treatment type, and treatment start and end date.

7. Place a check in the Generate Authorization checkbox.

8. 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.

Authorization Start Date *(the effective date of the authorization in MM/DD/YYYY format)*
06/08/2004

Authorization Expiration *(the expiration date of the authorization in MM/DD/YYYY format, an **Action Completed** may be used instead of a date)*
06/08/2005

Action Completed *(the expiration event for the authorization, such as "Upon completion of the investigation", an **Authorization Expiration** may be used instead of an action if known)*

Treatment Type *(the type of Treatment)*
Outpatient and Inpatient

Treatment Start Date *(the treatment or service start date in MM/DD/YYYY format)*
03/01/2004

Treatment End Date *(the treatment or service end date in MM/DD/YYYY format)*

Generate Authorization *(generate Authorization for Disclosure form for printing purposes)*

Save

- The Signed Status and Revoked Status boxes on this screen indicate if the DD Form 2870 is signed or revoked.

Update

Signed Status
Signed *(checked if the authorization is signed)*

Signed Date *(the date that the authorization is signed in MM/DD/YYYY format)*
01/30/2005

Signed By Person *(the individual who signed the authorization)*
Joe J Smith

Revoked Status
Revoked *(checked if the authorization is revoked)*

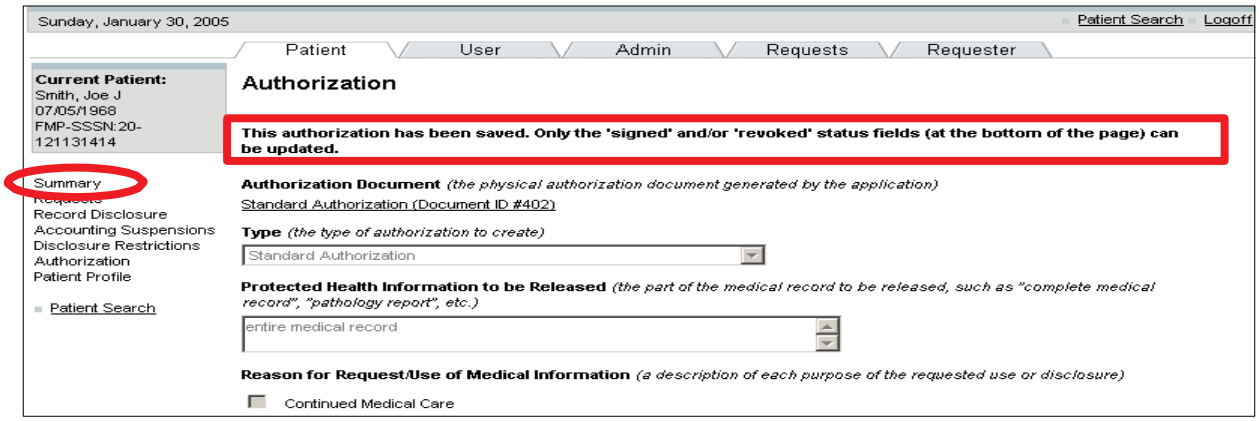
Revoked Date *(the date that the authorization was revoked in MM/DD/YYYY format)*
01/30/2005

Revoked By Person *(the individual who revoked the authorization)*
Joe J Smith

Update

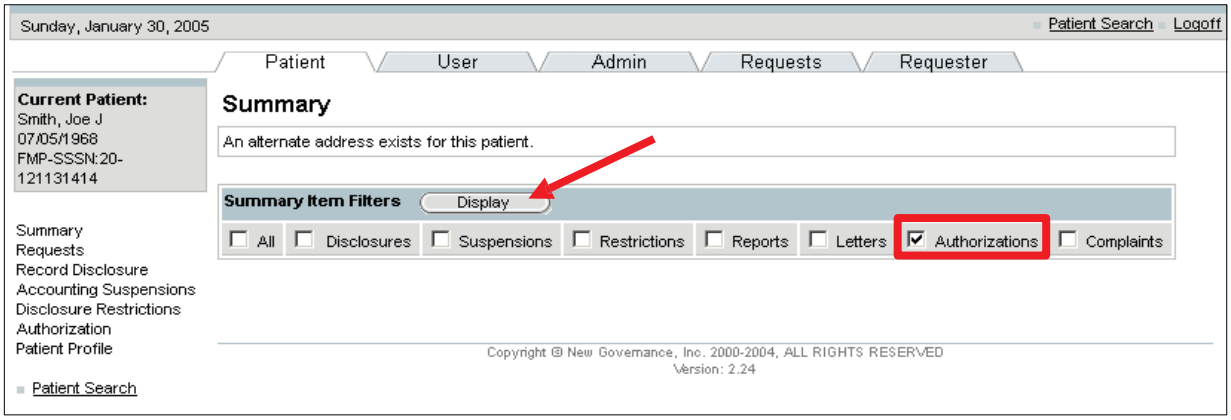
- A note appears at the top of the screen indicating the authorization is saved and that only the "Signed" or "Revoked" status fields may be changed at this point.

9. Select the Summary hyperlink.



10. Place a check in the Authorizations checkbox.

11. Click on the Display button.



- The new authorization will appear on the Summary screen.

To generate the DD Form 2870 (Adobe Acrobat format):

1. Select the Authorization title hyperlink.

Sunday, January 30, 2005 Patient Search Logoff

Patient | User | Admin | Requests | Requester

Current Patient:
Smith, Joe J
07/05/1968
FMP-SSSN:20-121131414

Summary
Requests
Record Disclosure
Accounting Suspensions
Disclosure Restrictions
Authorization
Patient Profile

Patient Search

Summary

An alternate address exists for this patient.

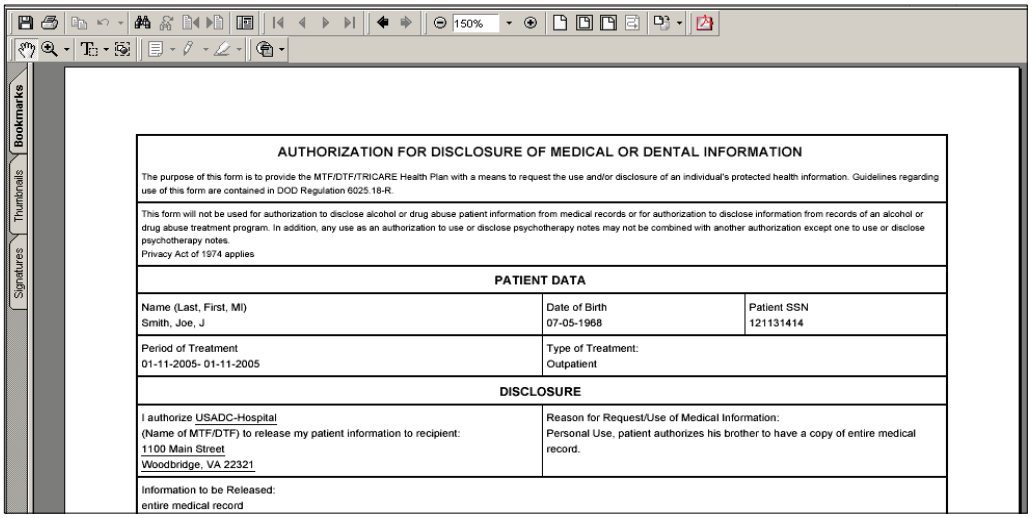
Summary Item Filters Display

☐ All ☐ Disclosures ☐ Suspensions ☐ Restrictions ☐ Reports ☐ Letters ☑ Authorizations ☐ Complaints

Authorizations (Revoked authorizations are highlighted in red)

ID	Title	Description	Signed	Expiration	Revoked
40	Standard Authorization	For disclosures of 'entire medical record' to '1100 Main Street Woodbridge, VA 22321'		02/03/2006	
124	Standard Authorization	For disclosures of 'medical record' to 'Jenny Smith 152 Brook Land Charleston SC 29404'	07/20/2004	07/27/2005	07/20/2004

2. You may print the form and request the patient's signature.



AUTHORIZATION FOR DISCLOSURE OF MEDICAL OR DENTAL INFORMATION

The purpose of this form is to provide the MTF/DTF/TRICARE Health Plan with a means to request the use and/or disclosure of an individual's protected health information. Guidelines regarding use of this form are contained in DOD Regulation 6025.18-R.

This form will not be used for authorization to disclose alcohol or drug abuse patient information from medical records or for authorization to disclose information from records of an alcohol or drug abuse treatment program. In addition, any use as an authorization to use or disclose psychotherapy notes may not be combined with another authorization except one to use or disclose psychotherapy notes.
Privacy Act of 1974 applies

PATIENT DATA

Name (Last, First, MI)	Date of Birth	Patient SSN
Smith, Joe, J	07-05-1968	121131414

Period of Treatment	Type of Treatment:
01-11-2005- 01-11-2005	Outpatient

DISCLOSURE

I authorize USADC-Hospital (Name of MTF/DTF) to release my patient information to recipient: 1100 Main Street Woodbridge, VA 22321	Reason for Request/Use of Medical Information: Personal Use, patient authorizes his brother to have a copy of entire medical record.

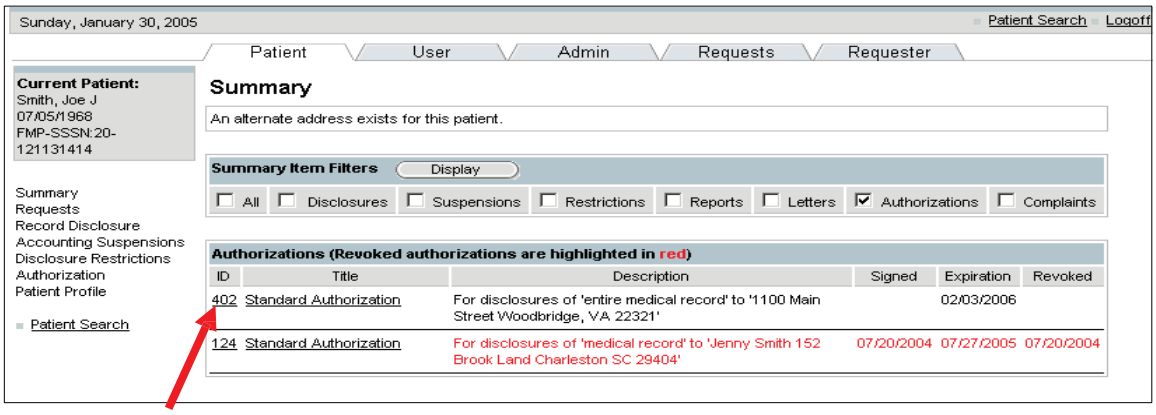
Information to be Released:
entire medical record

5.3.12 Sign an Authorization

Once an authorization has been entered, it needs to be signed by the patient for validation. After the authorization is signed by the patient, a user has the ability to document the signature within the PHIMT.

To sign an authorization:

1. Select the authorization ID hyperlink to return to the detailed authorization record.

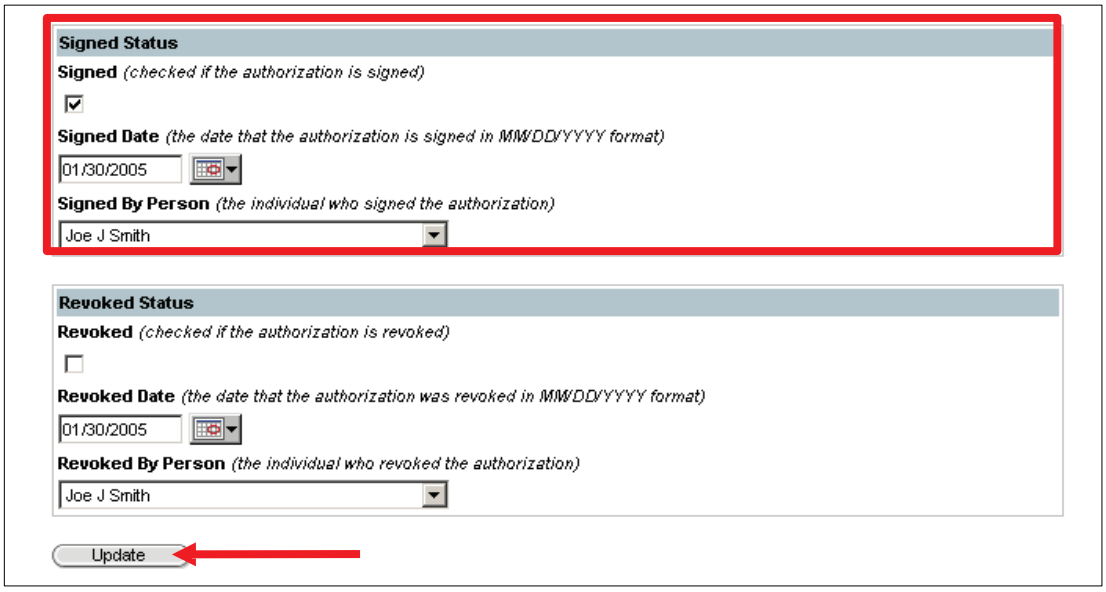


2. Scroll to the bottom of the page to the Signed Status box.

3. Place a check in the Signed Status checkbox.

4. Select the date and the authorizing person's identity from the drop-down box.

5. Click on the Update button.



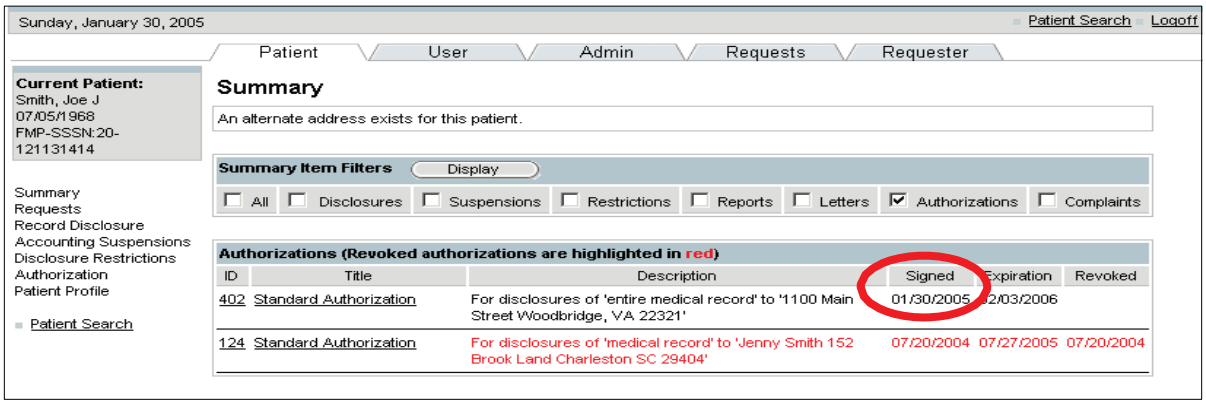
6. Select the Summary hyperlink.

7. Place a check in the Authorizations checkbox.

8. Click on the Display button.

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

- You will now see that the authorization indicates that it has been signed.



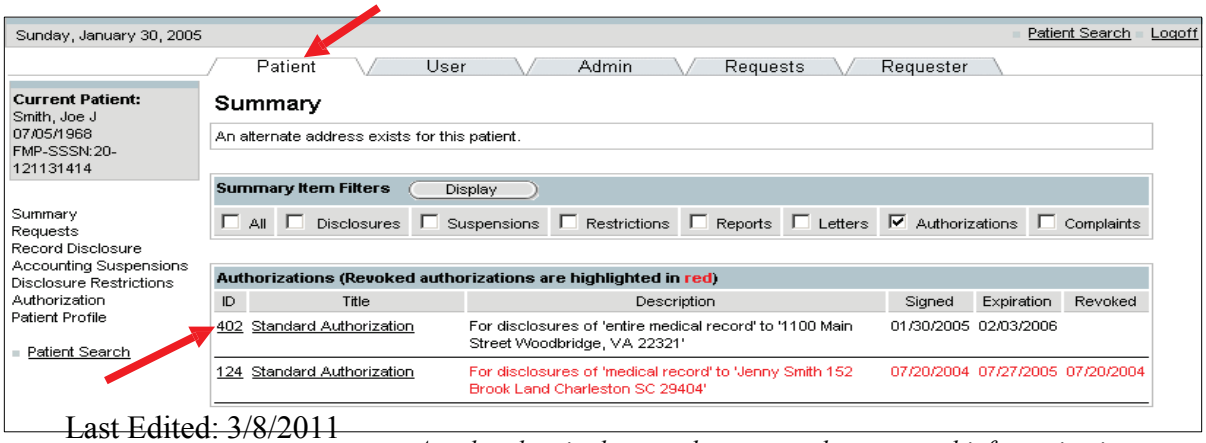
5.3.13 Revoke an Authorization

Previously generated authorizations may need to be revoked as a result of legal issues, new information, or for other reasons.

To revoke an authorization:

1. Select the Patient Tab.

2. Select the Authorization ID hyperlink.



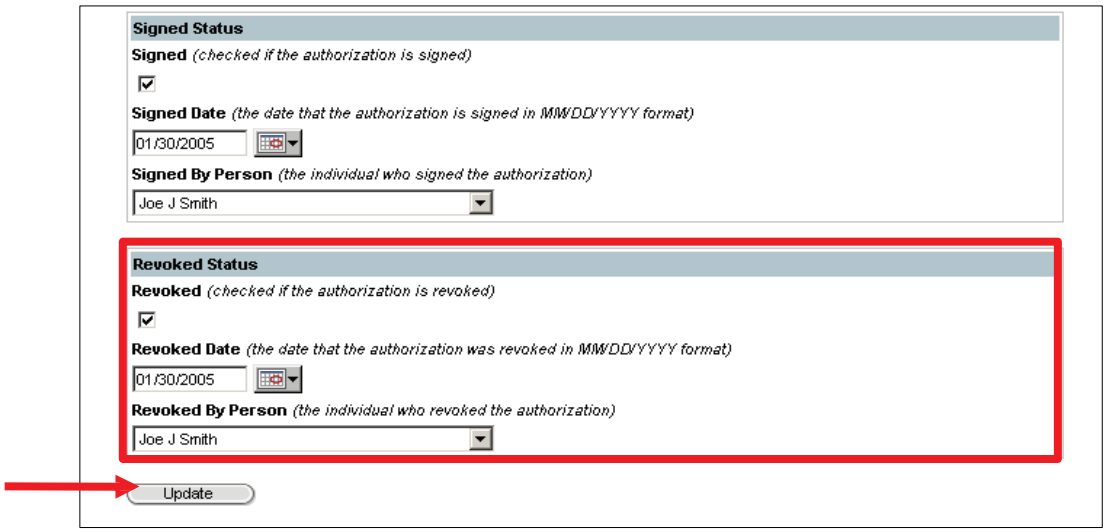
Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

3. Scroll to the bottom of the screen to the Revoked Status box.

4. Place a check in the Revoked check box.

5. Select the date and the revoking person's identity in the drop-down box.

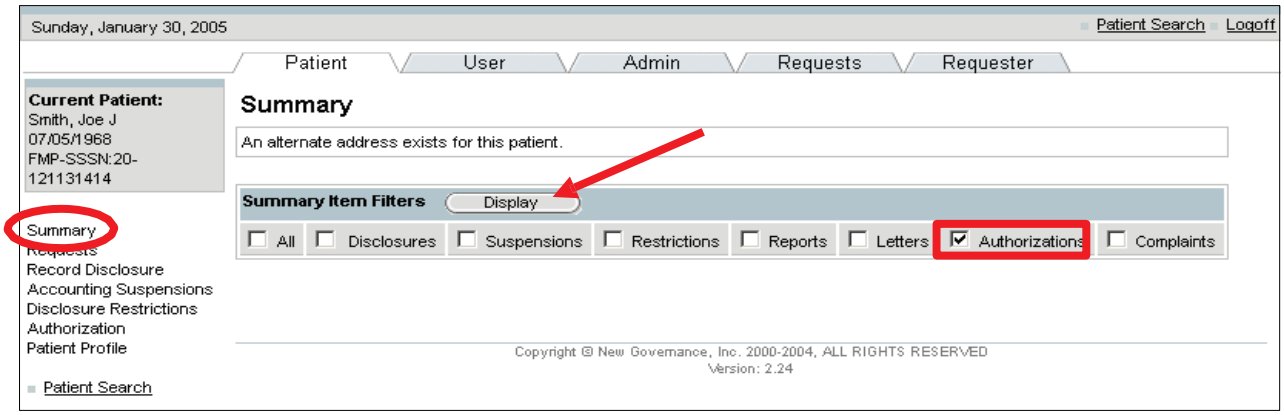
6. Click on the Update button.



7. Select the Summary hyperlink to view the authorization.

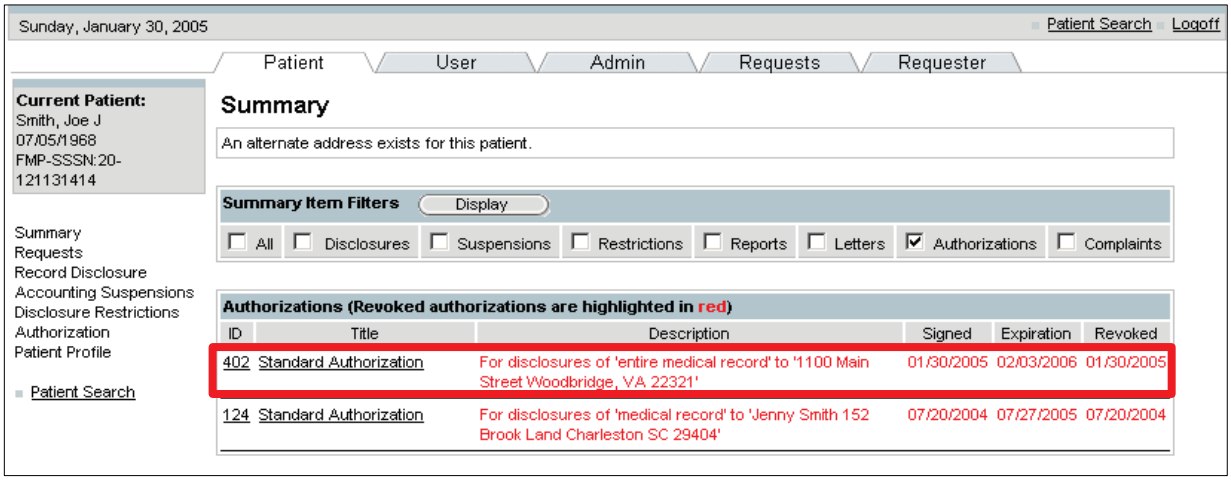
8. Place a check in the Authorizations checkbox.

9. Click on the Display button.



- The revoked authorization is highlighted in red.

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



5.3.14 Administrative Summary Reports

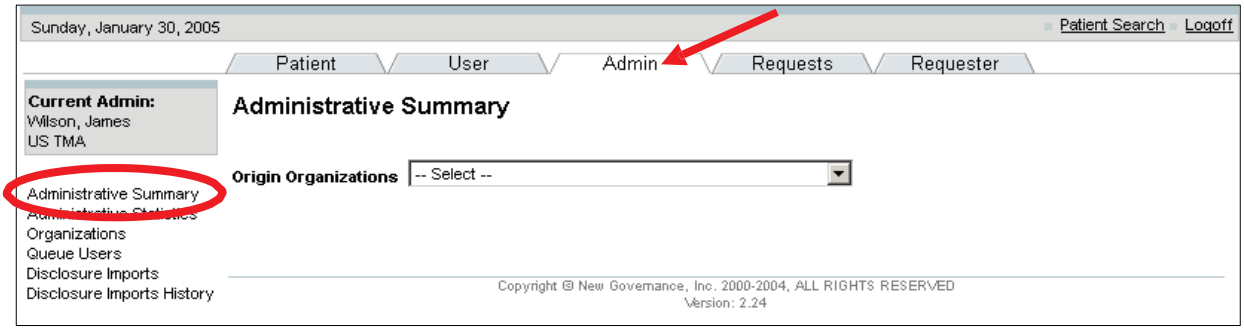
The PHIMT is capable of running several reports, which are called Administrative Summaries. Administrative Summaries provide a visual representation or snapshot view of your facilities disclosure activities.

The Administrative Summary Reports are performed by Privacy Specialists.

To create an Administrative Summary Report:

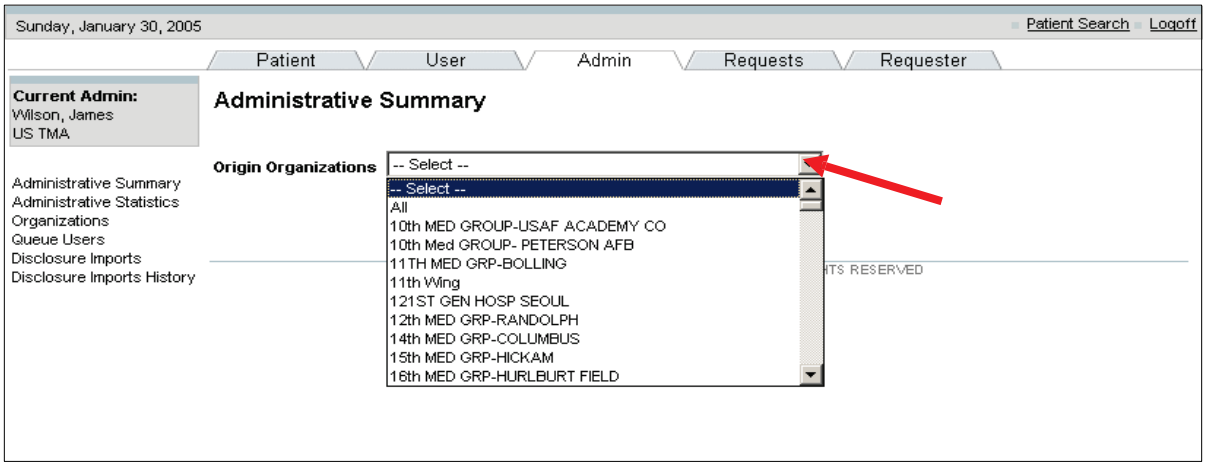
1. Select the Admin Tab.

2. Select the Administrative Summary hyperlink.

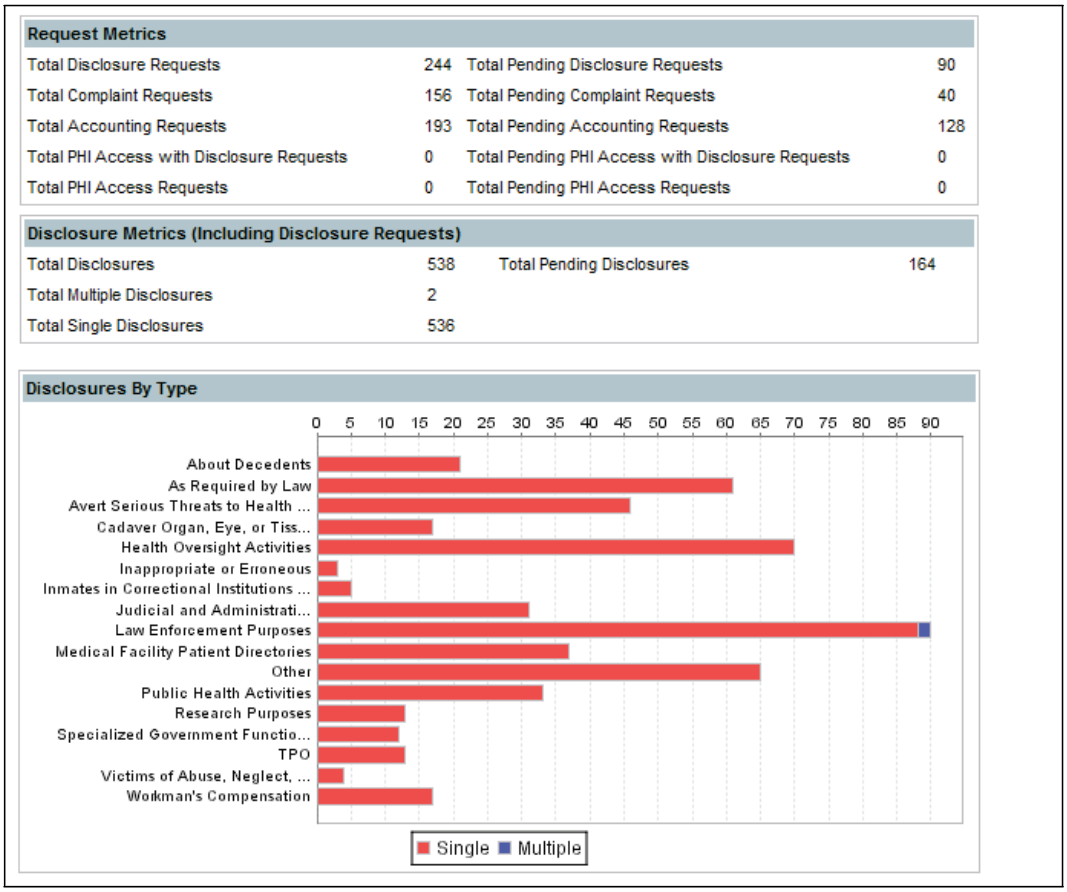


3. Select your Organization from the drop-down box.

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



- The Administrative Summary reports will display.



Request Metrics

Total Disclosure Requests	244	Total Pending Disclosure Requests	90
Total Complaint Requests	156	Total Pending Complaint Requests	40
Total Accounting Requests	193	Total Pending Accounting Requests	128
Total PHI Access with Disclosure Requests	0	Total Pending PHI Access with Disclosure Requests	0
Total PHI Access Requests	0	Total Pending PHI Access Requests	0

Disclosure Metrics (Including Disclosure Requests)

Total Disclosures	538	Total Pending Disclosures	164
Total Multiple Disclosures	2		
Total Single Disclosures	536		

Disclosures By Type

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 PRIVACY SPECIALIST PERMISSIONS	
PHIMT Privacy Specialist Tab	Enabled Permissions
Logon/Logoff	Both
User Tab	Change password Switch to other organizations Update address User profile User workflow Workflow activity Workflow request Workflows tab
Admin Tab	Administrative workflow Attach file Backup person relationship Organization management
Patient Tab	Create patient New request: deny request now Patient accounting request Patient accounting suspensions Patient alternate communication Patient authorization Patient disclosure restrictions Patient profile Patient search Patient summary Patient workflow Record disclosure View disclosure
Requests Tab	Complaint workflow Disclosure accounting Disclosure request

	Simple disclosure request Disclosure imports Edit request: accept request Edit request: approve request Edit request: complete PHI retrieval Edit request: process complaint Edit request: route to another Privacy Specialist Edit request: route to other user New request: process request now New request: route to another Privacy Specialist New request: route to other user New request: route to My Worklist
Requester Tab	Requester summary Requester workflow