Defense Health Agency

Protected Health Information Management Tool (PHIMT)

Training Reference: User Guide
Version 5.0

December 2016

TABLE OF CONTENTS

1.0 INTRODUCTION TO PHIMT

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule requires **covered entities** to safeguard the privacy of individuals **Protected Health Information (PHI)**.

- A covered entity is a health plan, such as the TRICARE Health Plan, a health care clearinghouse, which would include companies that perform electronic billing on behalf of Military Treatment Facilities (or MTFs), or a health care provider, such as a doctor or dentist working at an MTF, who transmits any health information in electronic form in connection with a covered transaction. Covered transactions are certain financial and administrative transactions covered by HIPAA. Examples of covered transactions include paying for health care, making billing requests, seeking eligibility determinations from a health plan, and providing referral authorization. For purposes of complying with HIPAA, the MHS is defined as a single covered entity. The MHS must comply with the requirements of HIPAA both as a provider of health care – through MTFs, which include both medical and dental facilities – and as the TRICARE health plan – through contracted network health care services.
- PHI is defined as individually identifiable health information (IIHI) that is transmitted or maintained by a covered entity or business associate in any form or medium. PHI excludes: (1) Employment records held by a covered entity in its role as an employer (such as sick leave information held by a hospital as an employee), and (2) Persons deceased more than 50 years. IIHI is defined as information that is a subset of health information, including demographic information collected from an individual, and:
    - is created or received by a covered entity or business associate; and
    - relates to the past, present or future physical or mental health condition of an individual; the provision of health care to an individual; or the past present or future payment for the provision of health care to an individual; and
        - That identifies the individual; or
        - With respect to which there is a reasonable basis to believe it can be used to identify the individual. A patient's name or account number are obvious identifiers of an individual, but other not so obvious types of information such as race and age together may also identify an individual.

The Department of Defense (DoD) regulation, DoD 6025.18-R, Health Information Privacy Regulation, implements the HIPAA Privacy Rule for the Military Health System (MHS). This regulation will ultimately be replaced with a DoD Instruction, Privacy of Individually Identifiable Health Information in DoD Health Care Programs, which will incorporate updates from the Omnibus Final Rule and developments within the MHS over the years.

The HIPAA Privacy Rule requires a covered entity to maintain a history of when and to whom disclosures of PHI are made. The MHS, as a covered entity, must be able to provide an accounting of those disclosures to an individual upon request.

In accordance with DoD 6025.18-R, 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, the Defense Health Agency (DHA) created an electronic disclosure-tracking tool. The Protected Health Information Management Tool (PHIMT) stores information about all disclosures that are made for a particular patient. PHIMT has a functionality built into it that can provide an accounting of disclosures.

PHIMT also contains the functionality to store Authorizations and Restrictions. This centralized retention allows Users to easily access the information across the MHS.

The PHIMT 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 the level of access an individual will have and may be limited to a facility level (e.g., a MTF). 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, 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.

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** is a general role with basic functionality. This role can create disclosures and authorization requests that can be routed on to a Privacy Specialist
- **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

- **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

- **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 access to users based on the user's job functions. 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 be designated as Regular Users or Privacy Specialists.

1.2.1 Privacy Specialist

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

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/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 understanding how to create a workflow for 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.*

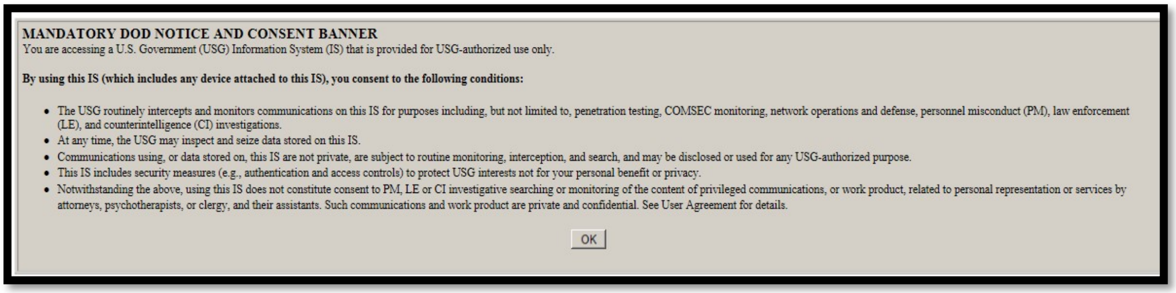
2.0 ACCESSING AND USING PHIMT

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 address bar in your Web browser:
   https://tma-phimt.csd.disa.mil/hipaax

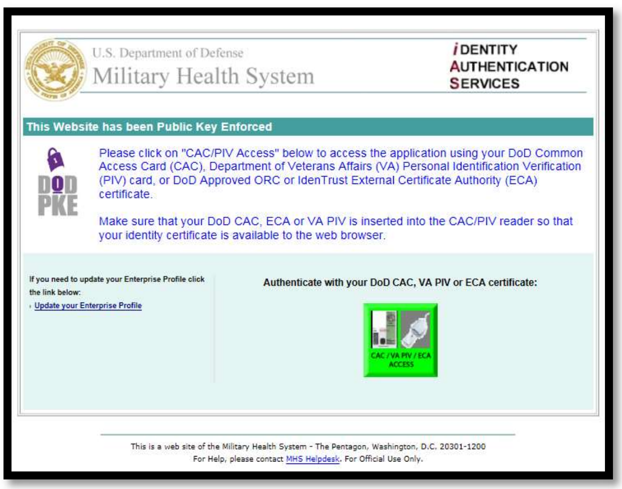
The Internet window should open to the MANDATORY DOD NOTICE AND CONSENT BANNER window shown below.



2. Read the DoD Notice and Consent Banner

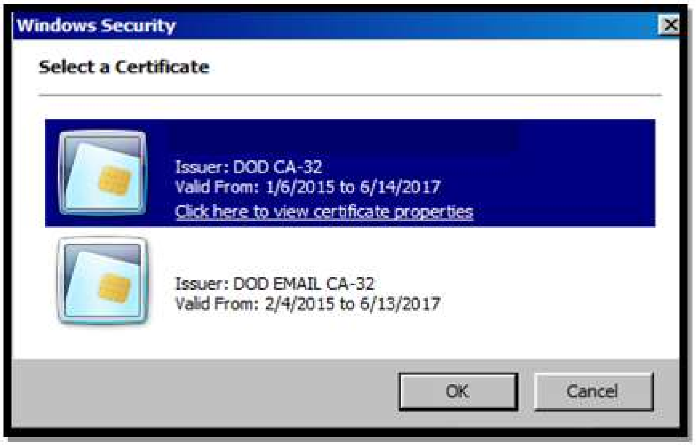
3. Click on the “OK” button at the bottom of the notice

   After clicking on the “OK” button, you should be taken to the DoD MHS PKE and CAC screen shown below:



4. Click on the Green CAC Access button at the bottom of the screen.

   This will display the “Select Certificate” window.



5. Select valid CAC Identification then click on the “OK” button

6. The DHA MHS PHIMT SERVER Notice and Terms of Use window should appear

7. Read the Notice and Terms of Use

8. Click on the “Accept” button at the bottom of the window

9. Upon successful login into PHIMT, you will land on the User Tab, which is the default setting, shown below:

3.0 UNDERSTANDING PHIMT SCREENS

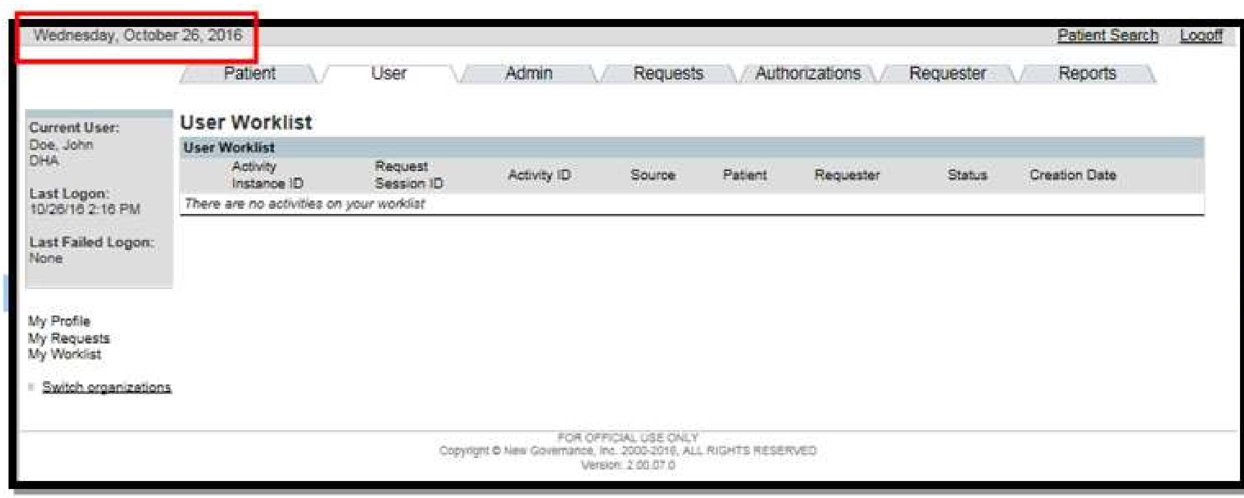
Each tab of the PHIMT screens contains basic information that will be helpful to you when performing various activities.

3.1 SCREEN FEATURES

There are many features to the PHIMT screen that you can use as you navigate your way through the many disclosure activities you will perform. These screen features include Date, Navigational Options, Status Box, and Activity Hyperlinks.

3.1.1 Date

The date feature 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 the Patient Search, provide directional hyperlinks that will help you 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 for all PHIMT screens. The status box displays the following information; Current User Name, User Organization, and Assigned Role, and Patient Information. This information is updated when making inputs for various activities.

3.1.4 Activity Hyperlinks

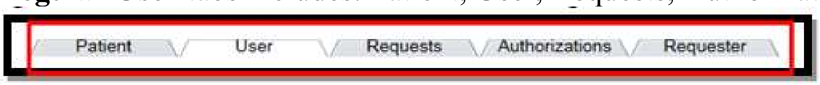
The Activity Hyperlinks feature is located under the status box, on the left hand side of the PHIMT screen. This listing consists of hyperlinks for activities that can be performed while in a specific "tab." The hyperlinks may include: My Profile, My Requests, or My Worklist; depending on which tab you 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, Authorizations, 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 PHIMT Screen 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 that 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, where applicable.

Feature	Definition
Radio Buttons	Radio buttons appear as black dots to indicate your selection. You can toggle the buttons between selected and not selected
Check Marks	Check Marks are used to indicate a completed or not completed 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 item causes it to be selected and appears 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. Choose a date by selecting the arrow in the date window. A calendar icon appears for easy inputs. Click on 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

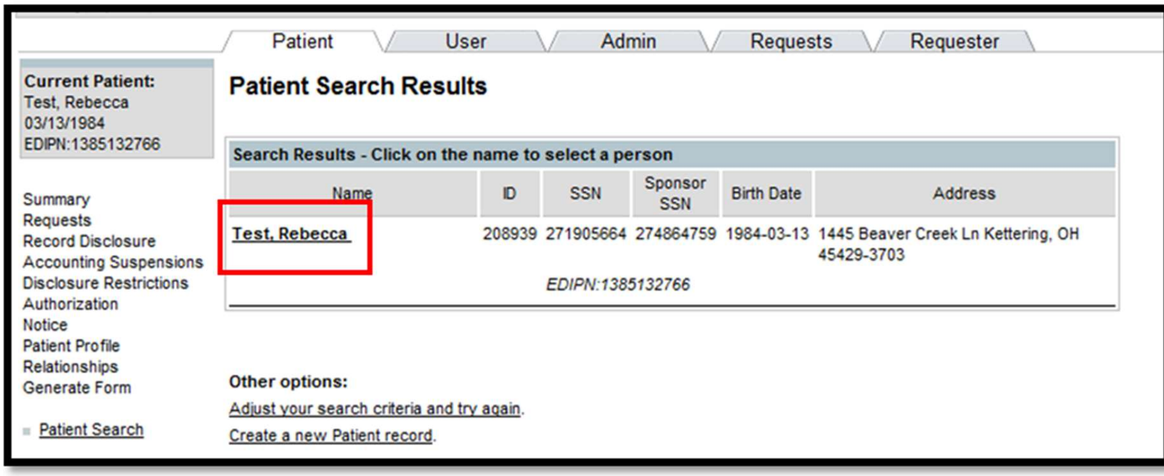
PHIMT automatically uploads patient demographic information from the Military Health System (MHS) Data Repository (MDR) on a monthly basis. This avoids the need for Users to manually enter patient demographics information prior to recording a disclosure, thus significantly decreasing the time needed 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

With MDR data uploaded to 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.

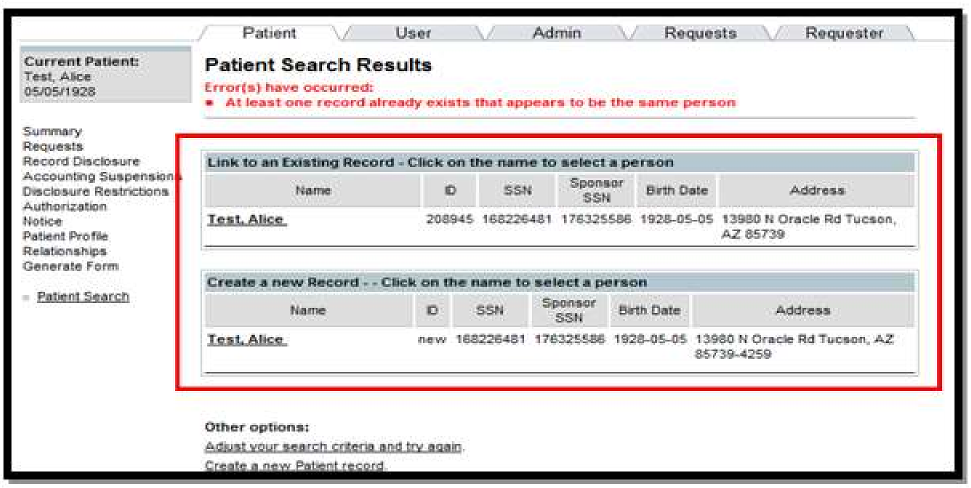
> **NOTE:** *When available, the address in the MDR will supersede the address in the PHIMT, unless the address in the MDR is blank. If the address in the MDR does not match the address in the PHIMT, the address in the MDR will be the default address. If there is not an address listed in the PHIMT, the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



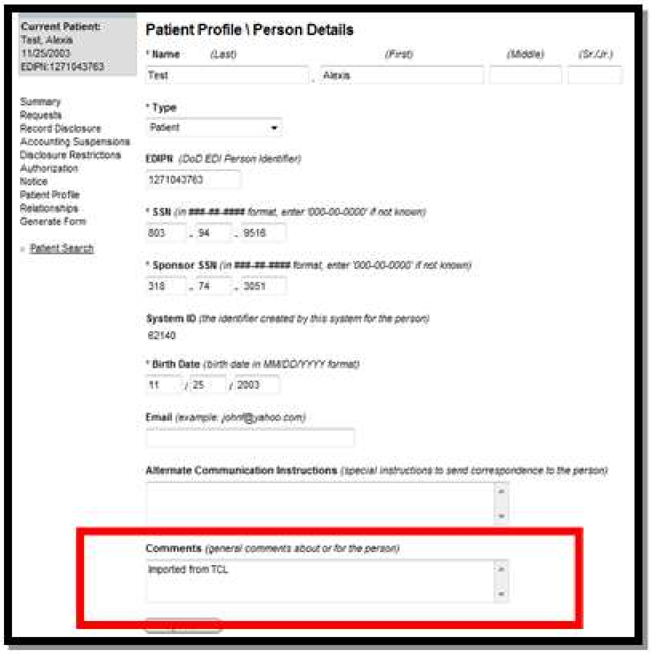
4.2 DUPLICATE ACCOUNTS

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



4.3 PATIENT PROFILE

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



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.

5.1.2 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:

- Phone number
- Email address
- Signature block (used for personal or professional titles and credentials)

- 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.*

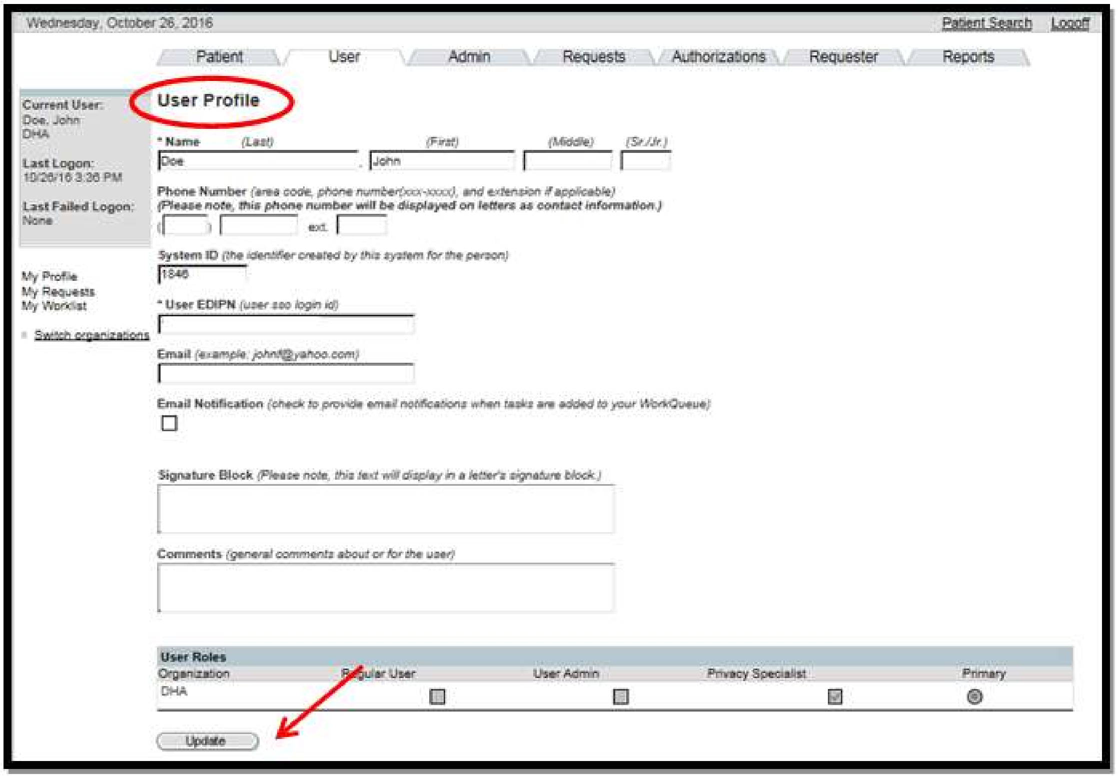
NOTE: *PHIMT contains profiles for all users within the system. It is important to keep your personal information up to date. Therefore, you should update all personal information as it changes.*

Steps 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). Then click the Update button.



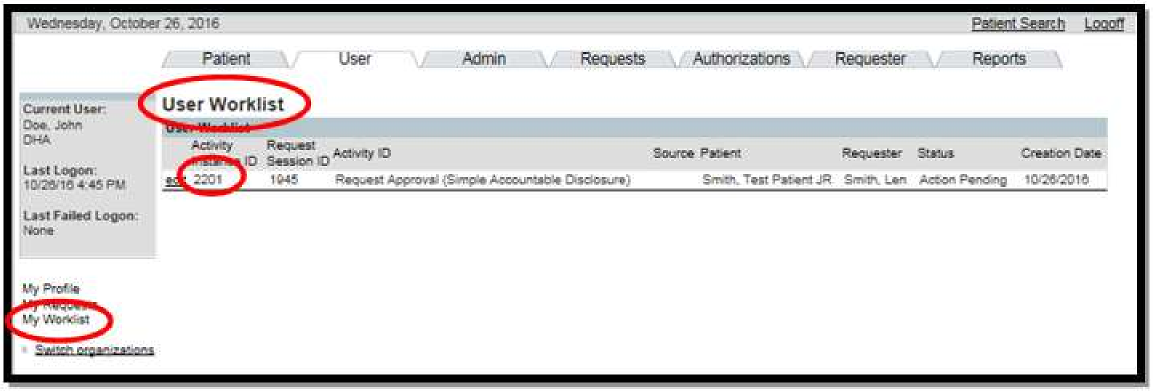
Your new information will appear in the appropriate fields.

5.1.3 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.

5.1.4 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.



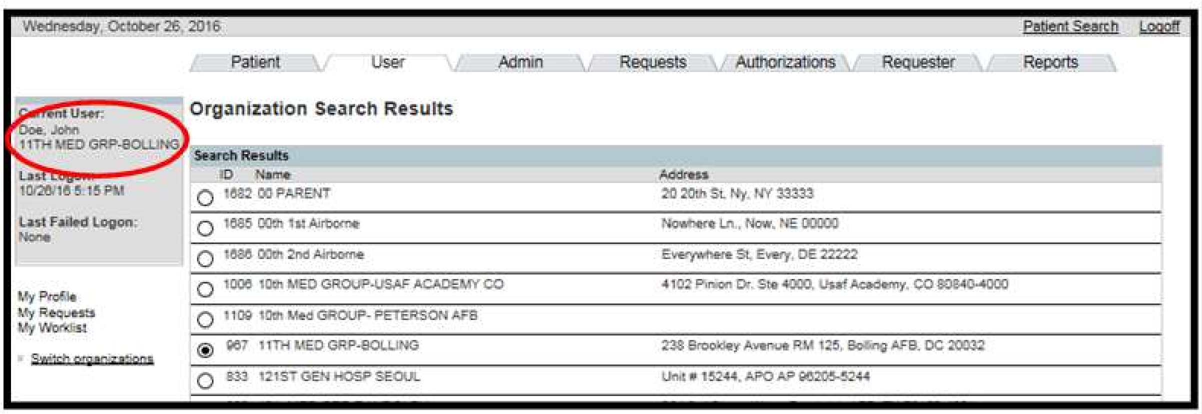
5.1.5 Switch Organization

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.

Steps 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.

- 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.

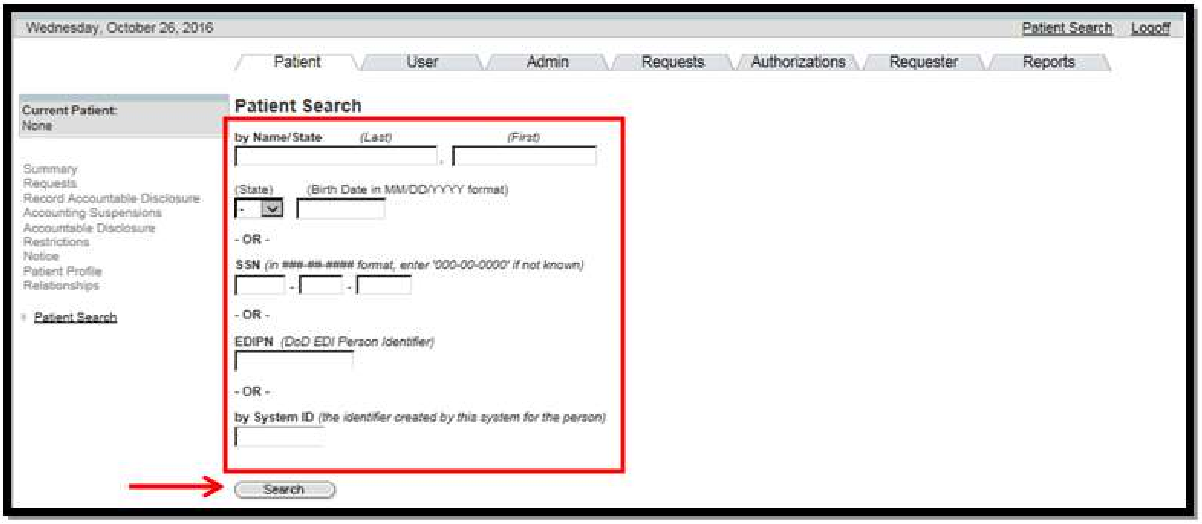
Steps to search for a patient:

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.*

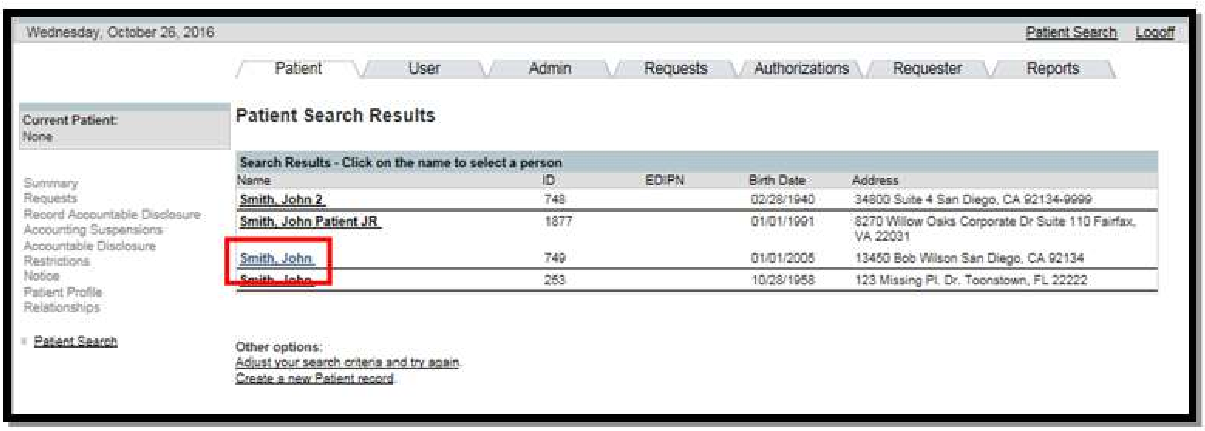
3. Click on the Search button.



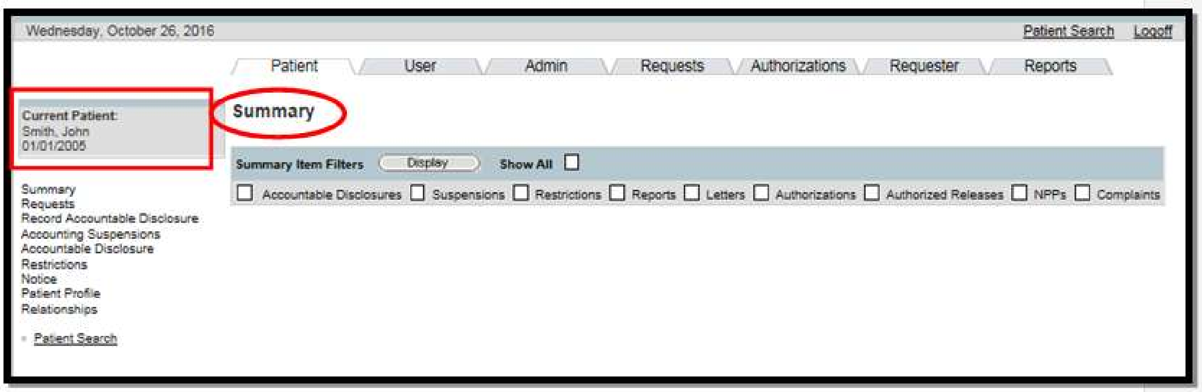
NOTE: *The search limitation within the PHIMT is 600 records. This means that if your search results in over 600 records, you will have to narrow down your search*

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.

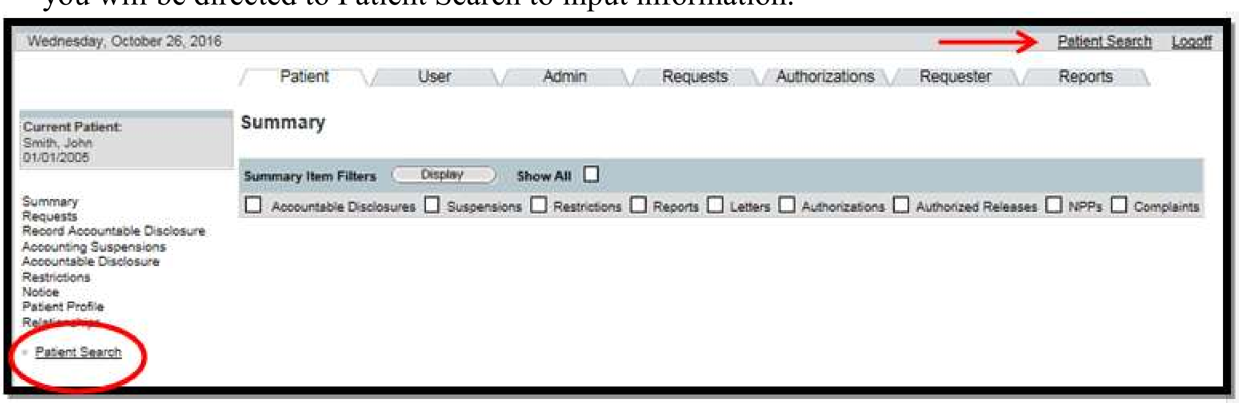


5.2.2 Create a Patient

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.

Steps to create a patient:

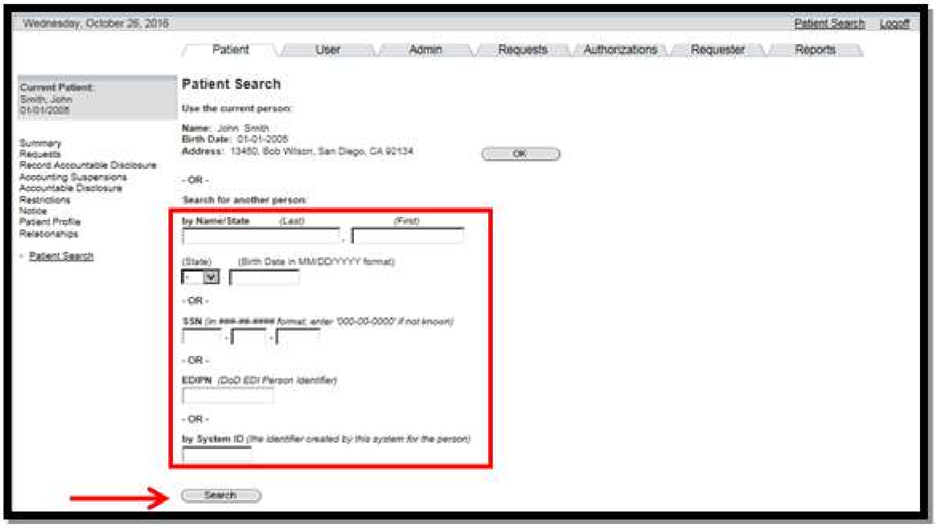
1. Select the Patient Tab. If a patient is currently selected, the screen below will appear as it pertains to items you may call up about that patient. If no patient was previously selected, you will be directed to Patient Search to input information.



2. Select the Patient Search hyperlink. You can also go directly to Patient Search by clicking as denoted by the arrow.

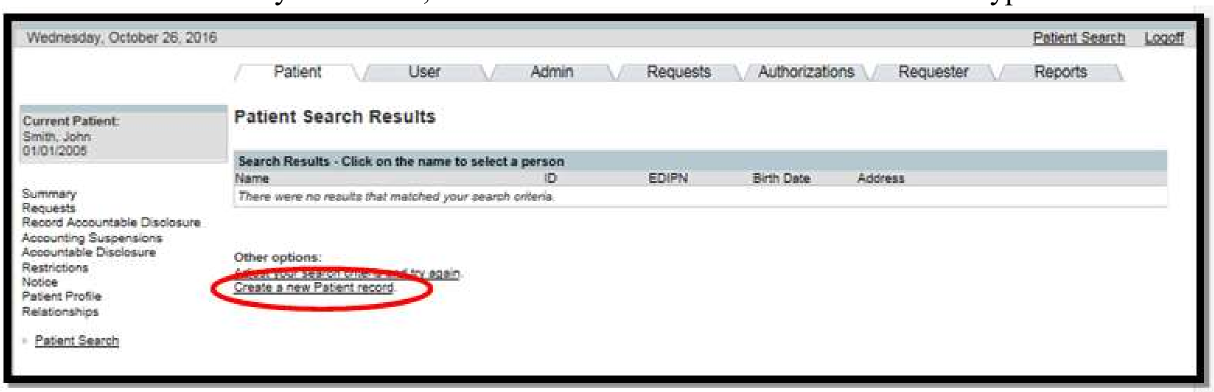
3. Enter the patient search criteria. (You can search for a patient by the Sponsor's SSN, by the patient's name/state, SSN, EDIPN or System ID).

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.*

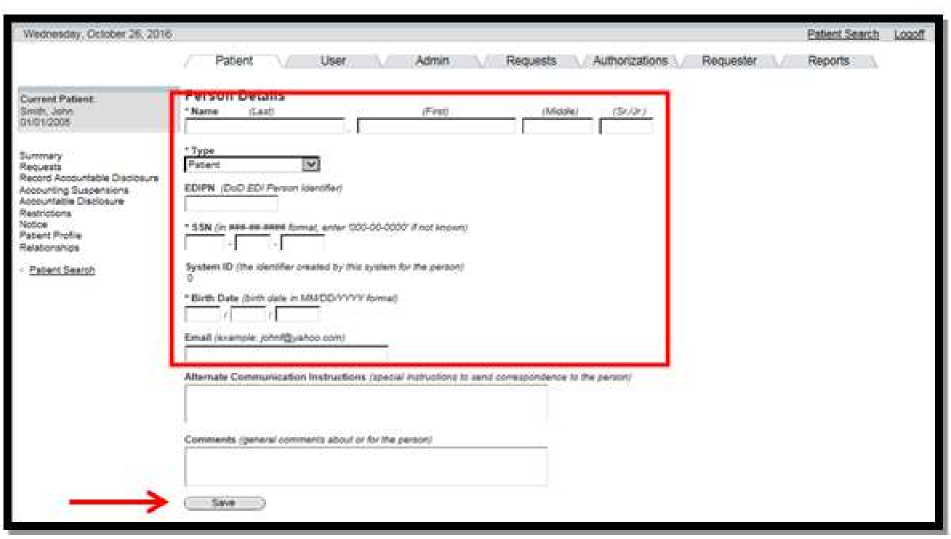


4. Click on the Search button.

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



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

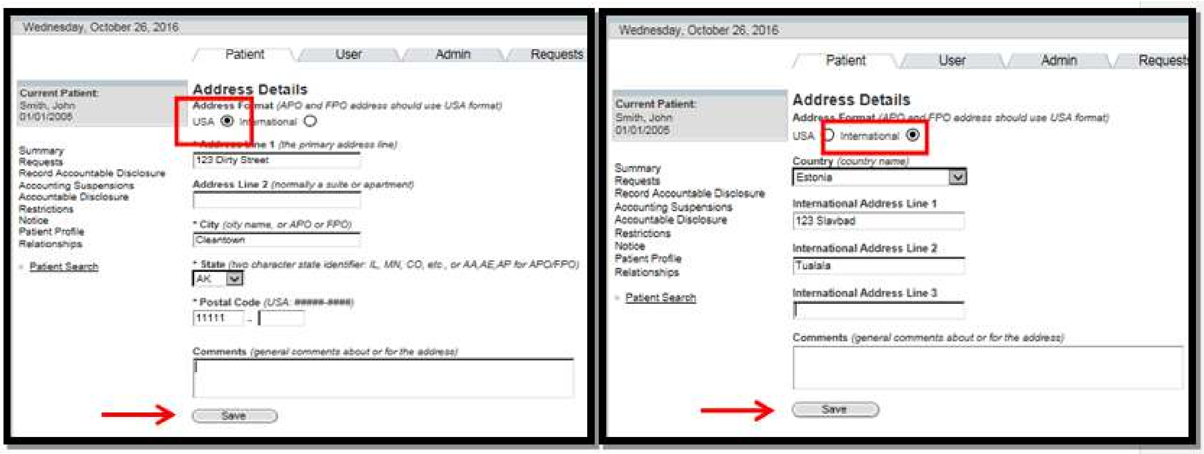


7. Click on the Save button.

<u>NOTE:</u> *All required fields are marked with an asterisk.*

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

9. Click on the Save button.



- 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

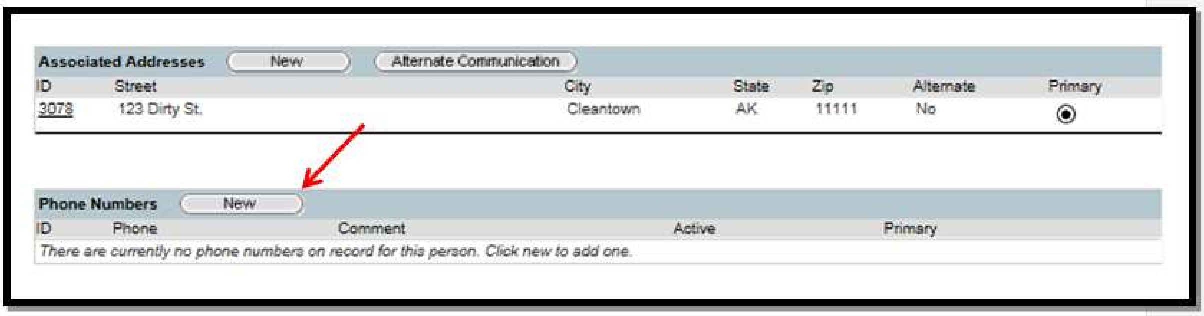
Individuals have the right to request an alternative telephone number for receiving communications related to their PHI. An alternative telephone number can be created by Regular Users and Privacy Specialists.

Steps to create an alternative telephone number:

1. From the patient Summary screen, click Patient Profile.

2. Scroll to the bottom of the Patient Profile/Patient Details screen.

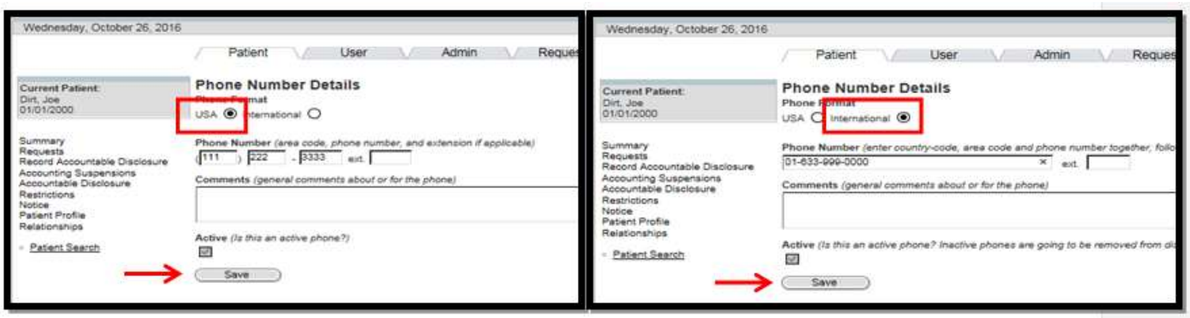
3. Click on the New button next to Phone Numbers.



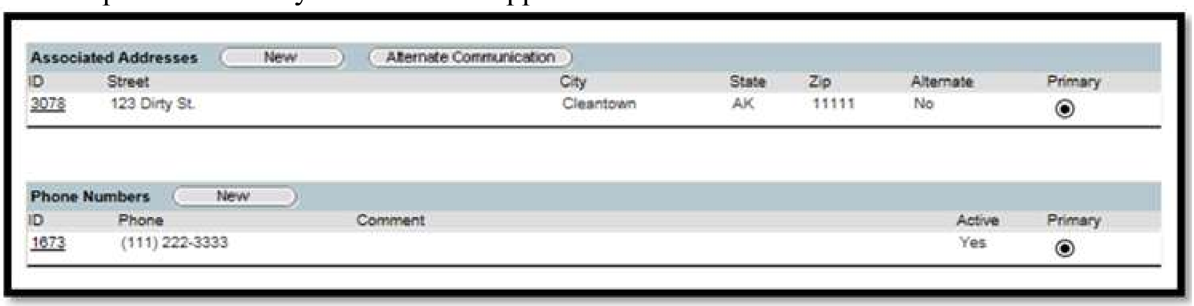
- The Phone Number Details screen will display (choose the USA or International format).

4. Enter the phone number and enter any comments.

5. 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.

5.3.1 Record a Single Accountable Disclosure

The Privacy Specialist can use the Record Accountable Disclosure hyperlink to record disclosures. The Record Accountable Disclosure hyperlink allows for immediate approval or denial.

Steps 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).

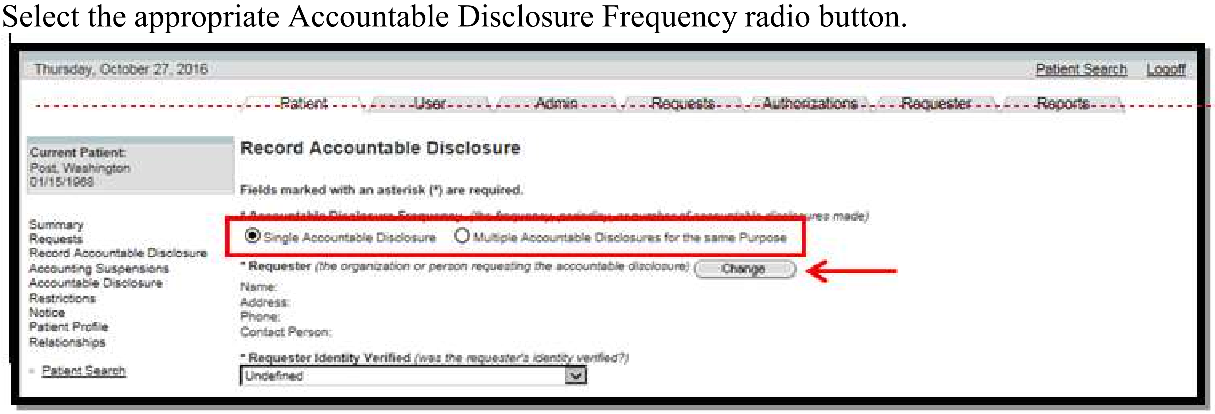
3. Click on the Search button.

4. Select the patient from the Patient Search Results screen by clicking the Name hyperlink.

<u>NOTE:</u> *The steps 1-5 for recording a disclosure are the same as steps 1-4 in section 5.2.1 Patient Search. Refer to section 5.2.1 Patient Search for screen displays of steps 1-5.*

5. Select the Record Accountable Disclosure hyperlink on the Patient Summary screen.

6. Select the appropriate Accountable Disclosure Frequency radio button.

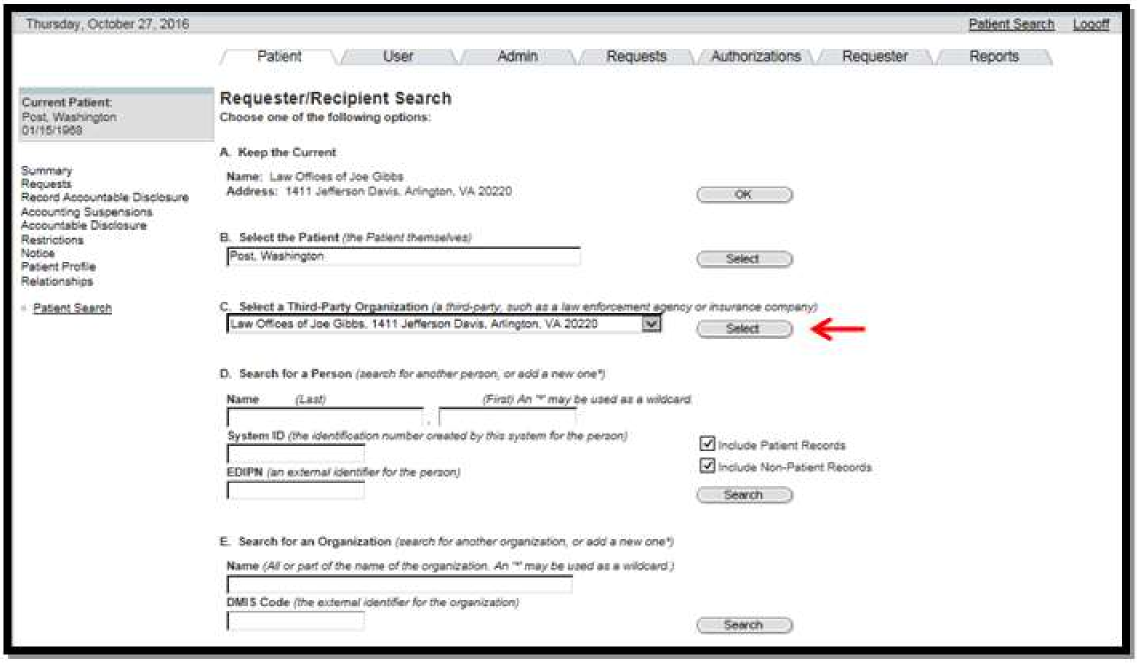


- Single Accountable Disclosure is a single, non-recurring disclosure of PHI
- Multiple Accountable Disclosures are multiple disclosures made to the same person or entity for a single purpose
    - Some examples of multiple disclosures include: recurring monthly medical readiness status, dental class reports, or pre-deployment preparation reports to a commander or the commander's designee(s). Multiple Disclosures are 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.

7. Click on the Change button to add, change, or update the requester.

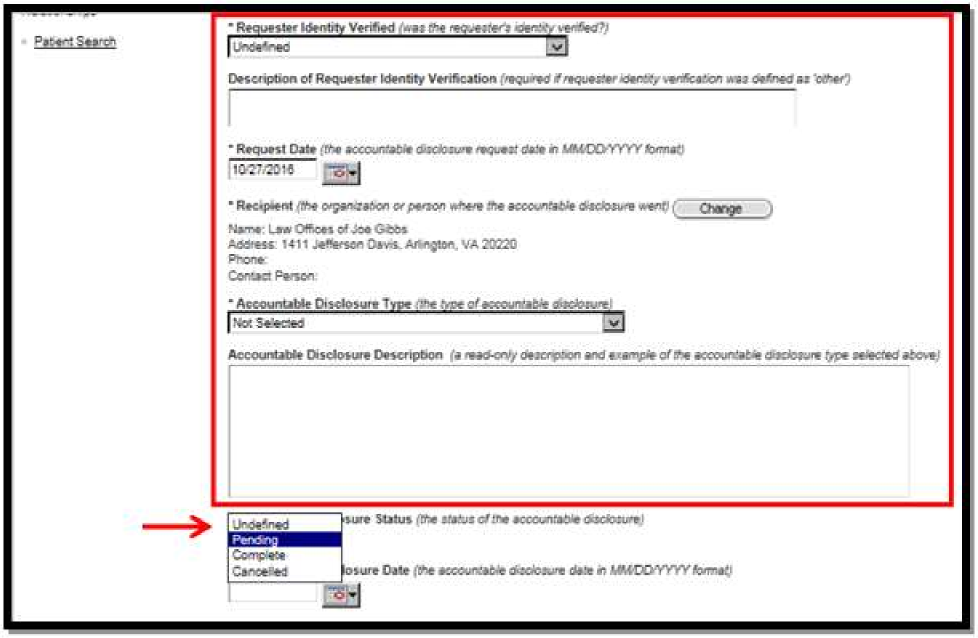
8. Select the requester.



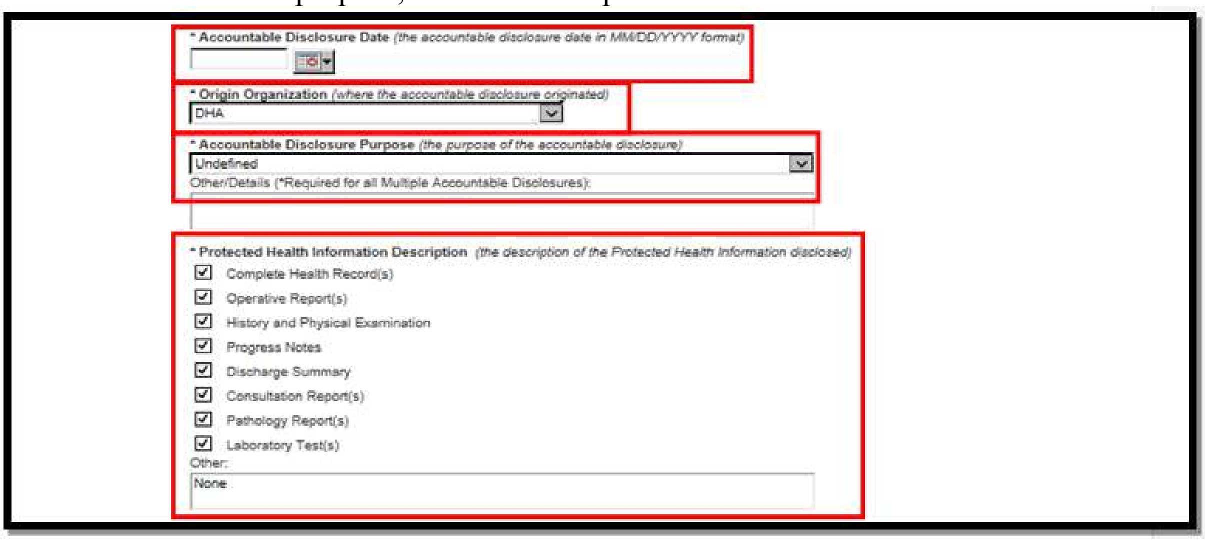
9. Complete required fields, as marked with an asterisk.

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

10. Select the Accountable Disclosure Status from the drop-down box

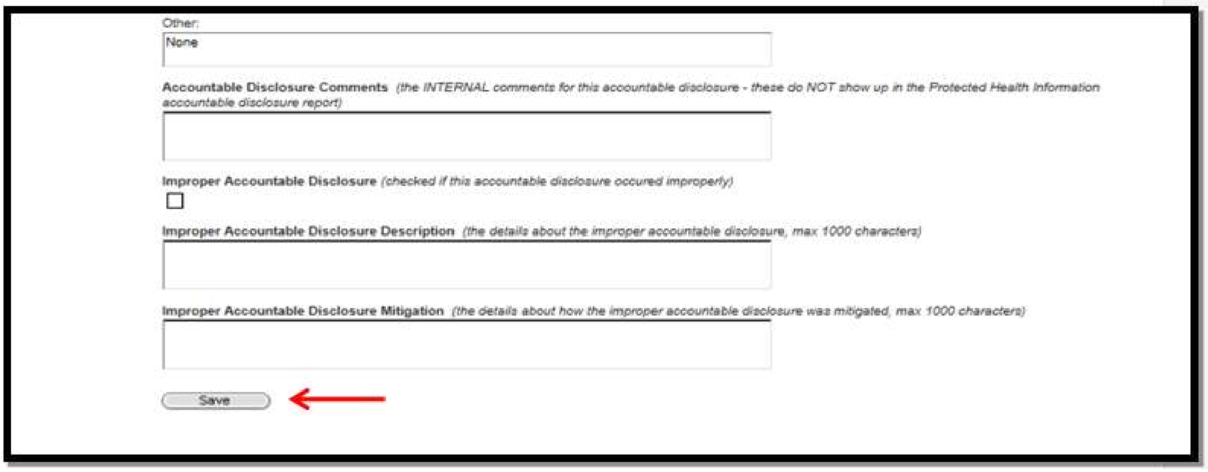


11. Scroll down the screen and enter: accountable disclosure date, origin organization, accountable disclosure purpose, and PHI description.

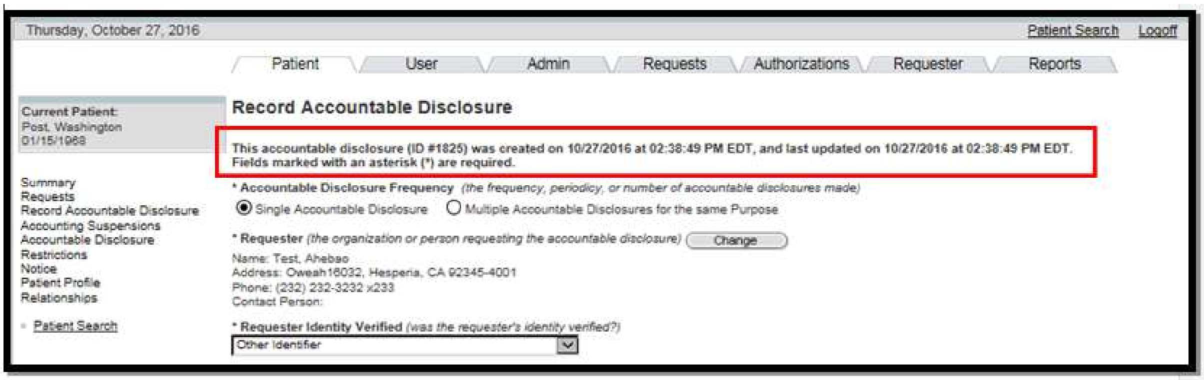


NOTE: *The Accountable Disclosure Type and Accountable Disclosure Purpose cannot be set to Undefined.*

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



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



NOTE: *To view the disclosure:*

- *Select the user tab*
- *Select My Requests hyperlink*
- *Enter year or date parameters, as applicable, and click Search*
- *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 5.3.3 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.

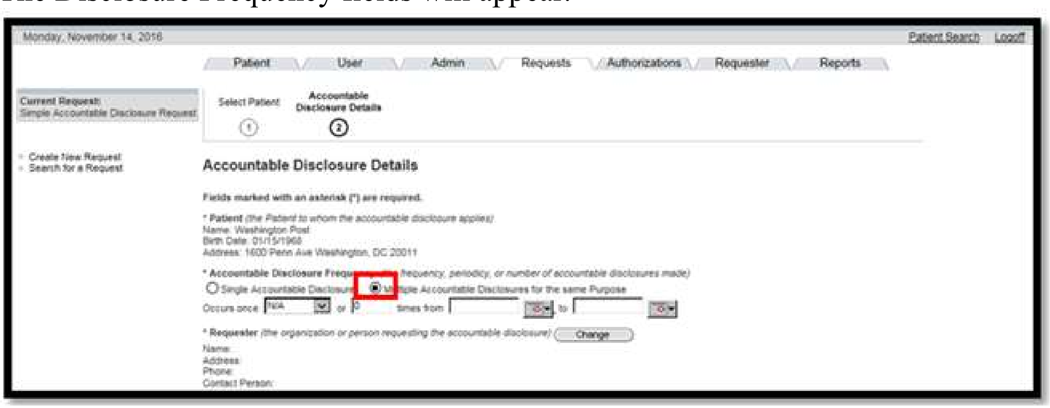
Guidance for Completing Disclosure with Special Circumstances	
Data Field	**Data to be Provided**
Information Start Date	Provide the date for which the disclosure request begins
Information End Date	Leave blank if unknown or insert the date for one year later
Disclosure Date	Insert the date of the first 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

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

5.3.2 Record a Multiple Accountable Disclosure

Steps to record a Disclosure:

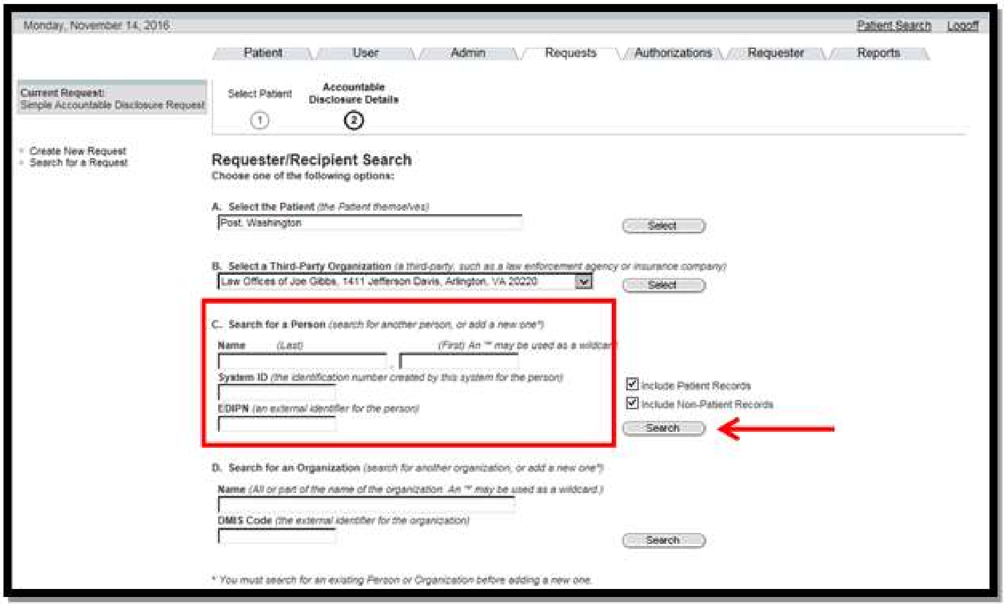
1. Select the Patient Tab.
2. Enter the patient search criteria. (You can search for a patient by the Sponsor's SSN, by the patient's name/state, SSN, EDIPN or System ID).
3. Click on the Search button.
4. Select the patient from the Patient Search Results screen by clicking the Name hyperlink.
5. Select the Record Accountable Disclosure hyperlink on the Patient Summary screen.
6. Click on the Multiple Accountable Disclosures, as applicable.
7. The Disclosure Frequency fields will appear.



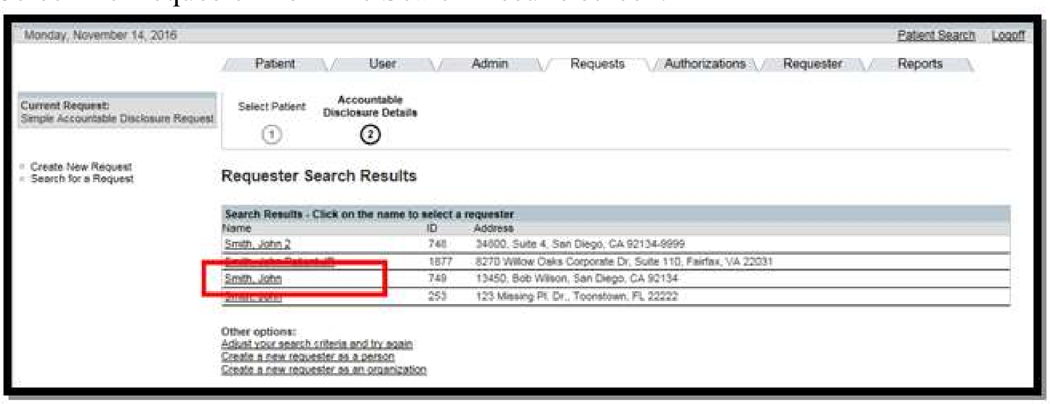
8. Select the occurrence, start date, and end date. (Users can select from the drop-down, which includes: weekly, monthly, or annually, or they have the option to put how many times the disclosure occurs in a specified time period.)

9. Click on the Requester Change button.

10. Search for the Requester.



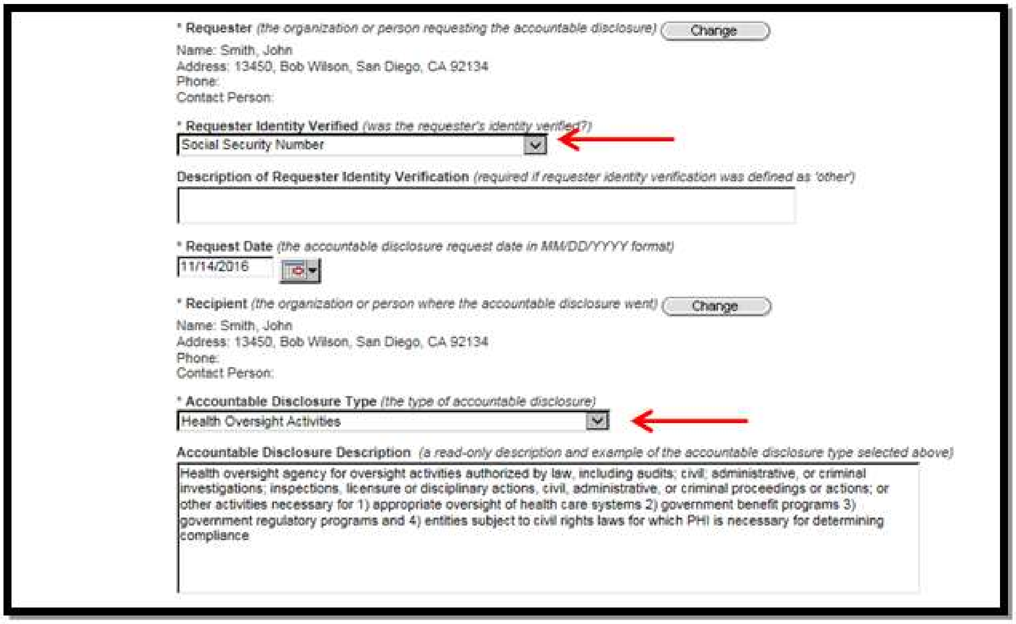
11. Select the Requester from the Search Results screen.



12. Select the Requester Identity Verified drop-down.

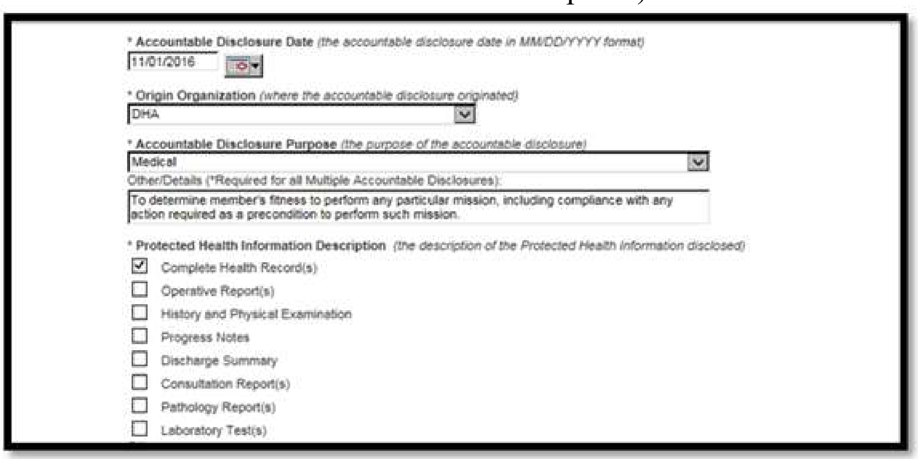
13. Select the Disclosure Type from the drop-down.

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



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.)



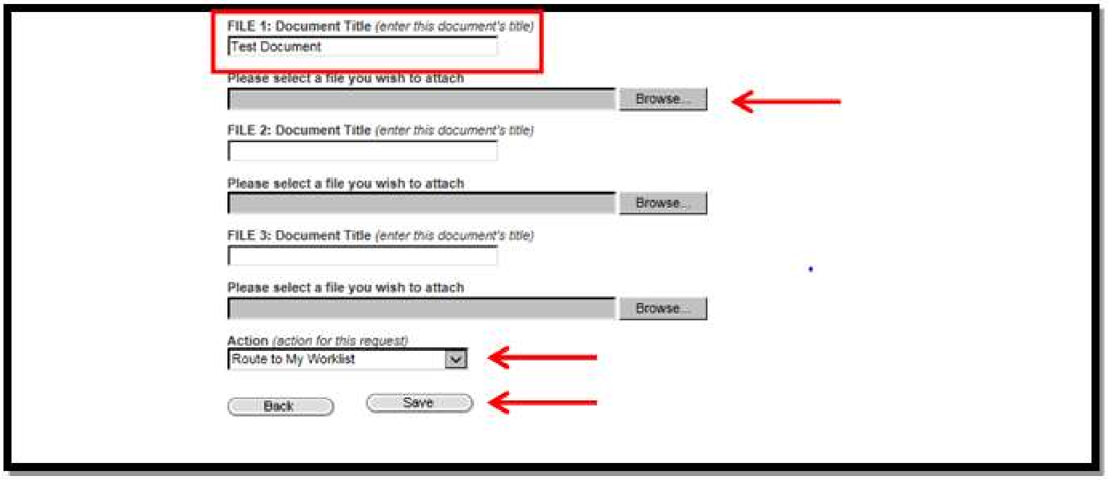
16. Scroll down the screen and enter: PHI description and disclosure comments.

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

17. Type the document title.

18. Click on the browse button to attach the document.

19. Click on the Save button.



5.3.3 Approve Disclosures

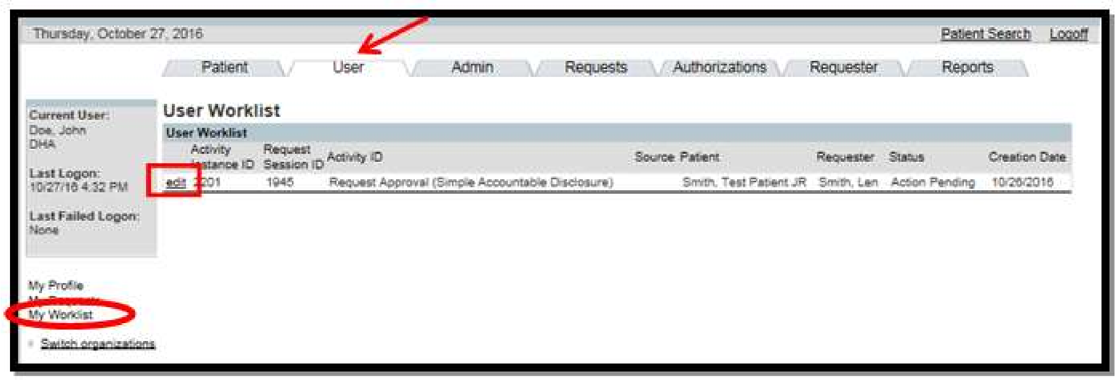
NOTE: *Those disclosures recorded by you using the Record Disclosure hyperlink have already been approved. This approval activity is for those disclosures that were developed using the Record Disclosure wizard and routed to your worklist for later action.*

Steps to approve a disclosure:

1. Select the User Tab.

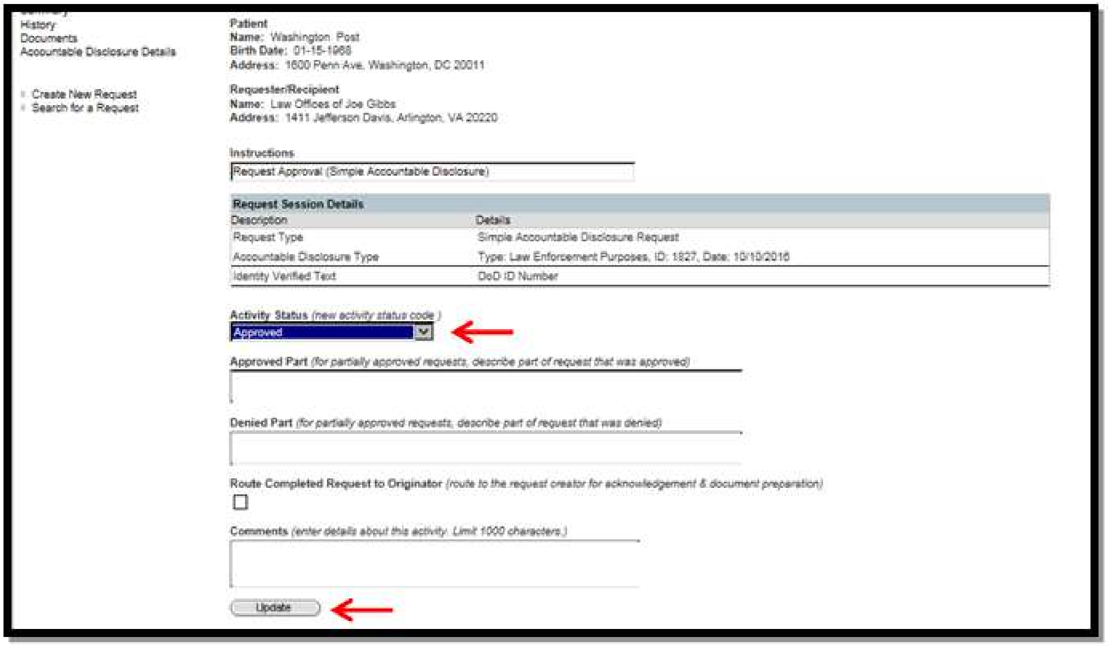
2. Select the My Worklist hyperlink.

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



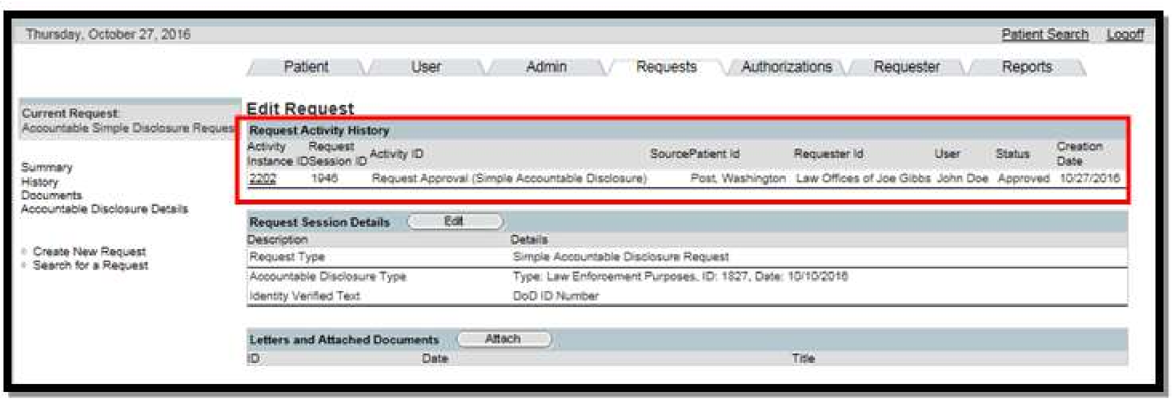
4. Select Approved from the Activity Status drop-down box.

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.

NOTE: *The disclosure is no longer shown in your User Worklist.*



5.3.4 Amend a Disclosure

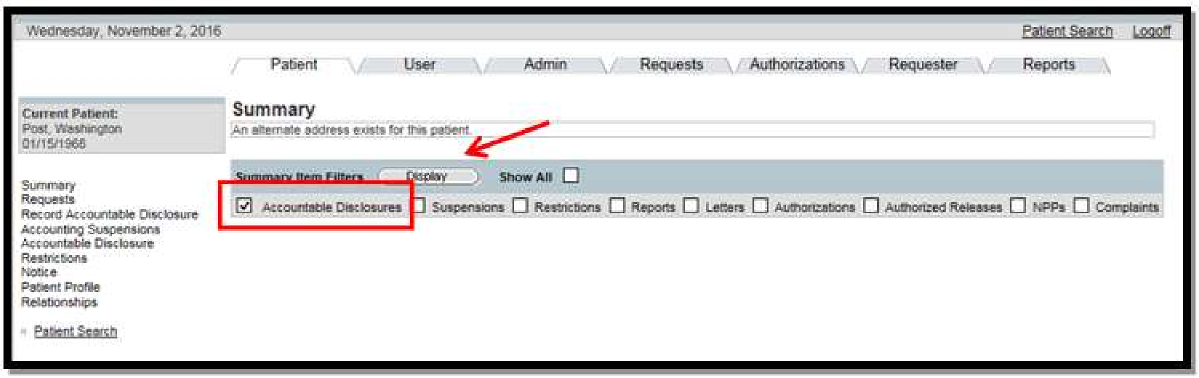
As a Privacy Specialist you are authorized to label a disclosure as Improper. Once a Disclosure status is marked as completed, it can only be amended by marking it as an Improper Disclosure, which means the disclosure was made incorrectly.

Steps to amend a disclosure:

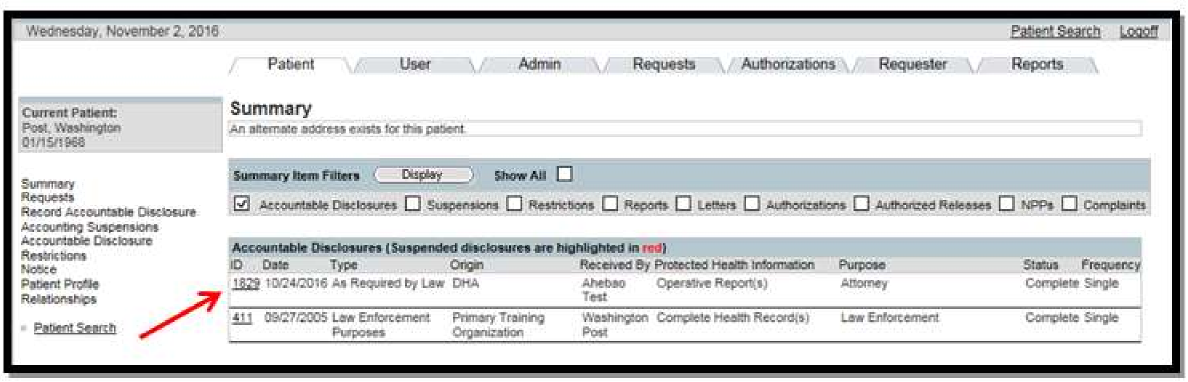
1. Select the Patient Tab.

2. Search for and select the patient (see 5.2.1).

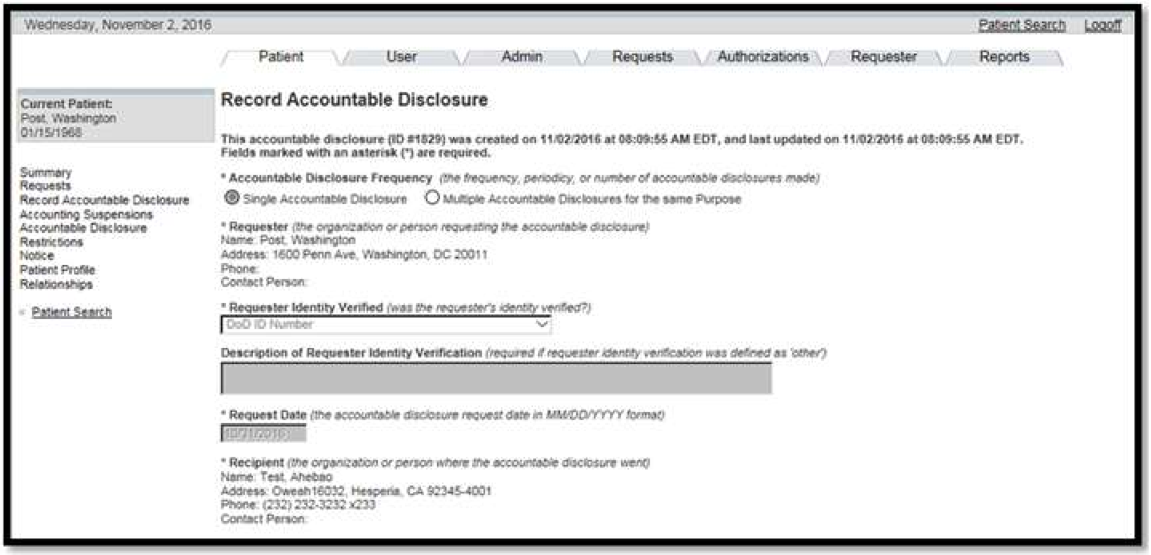
3. Place a check in the Disclosures box and click on the Display button.



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



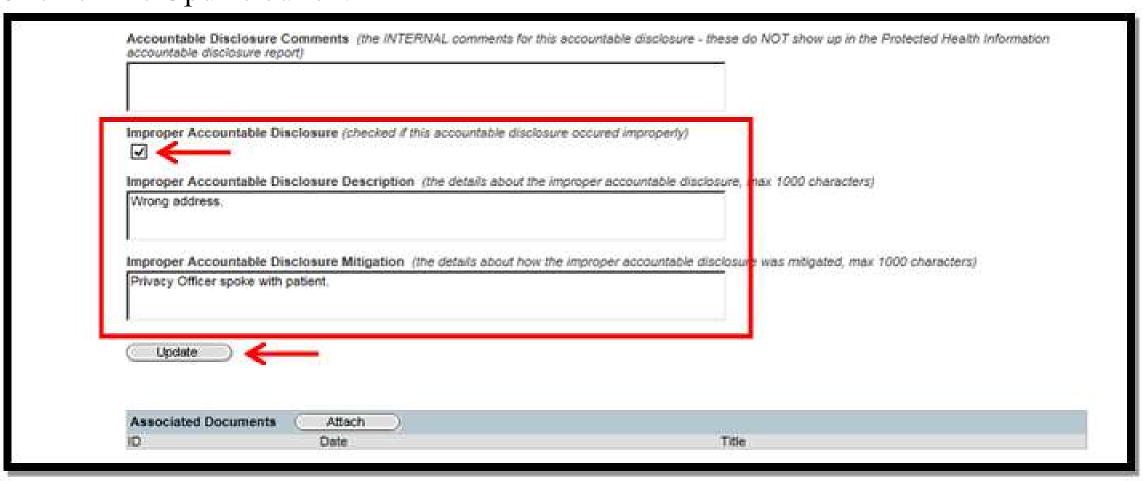
- The Record Disclosure screen will display.



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.



5.3.5 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.

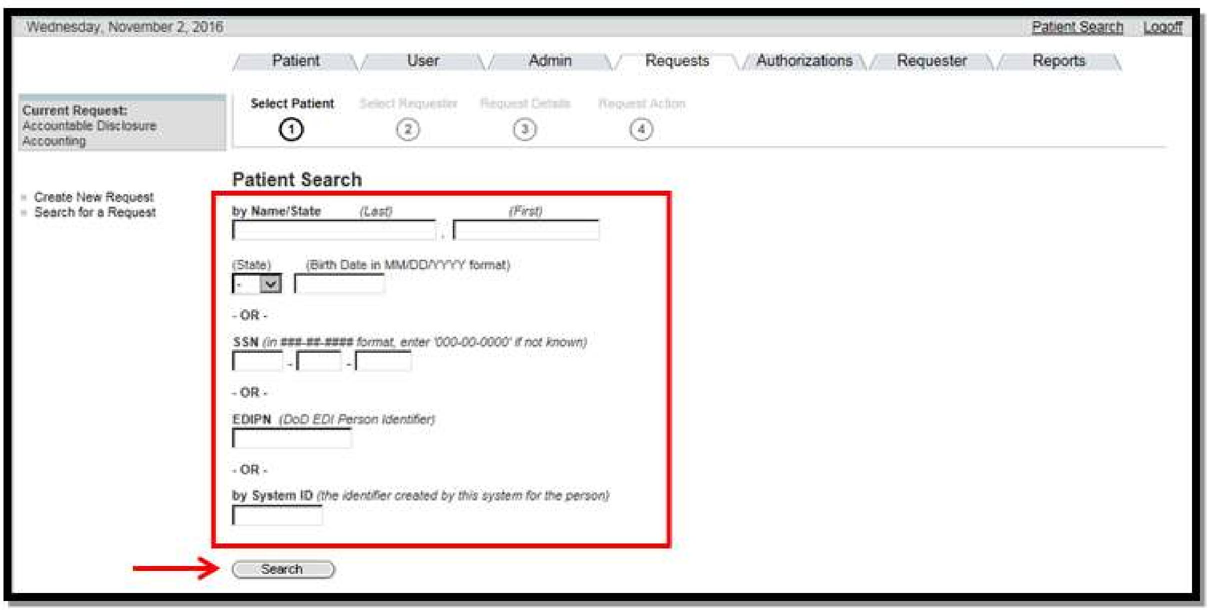
Steps to record a request for an accounting of disclosures:

1. Select the Requests Tab.

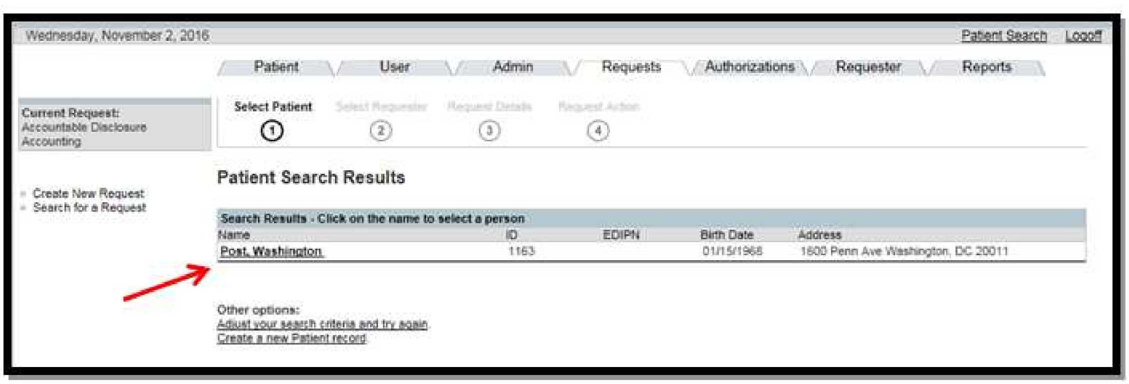
2. Click on the radio button for Accountable Disclosure Accounting.

3. Click on the Next button.

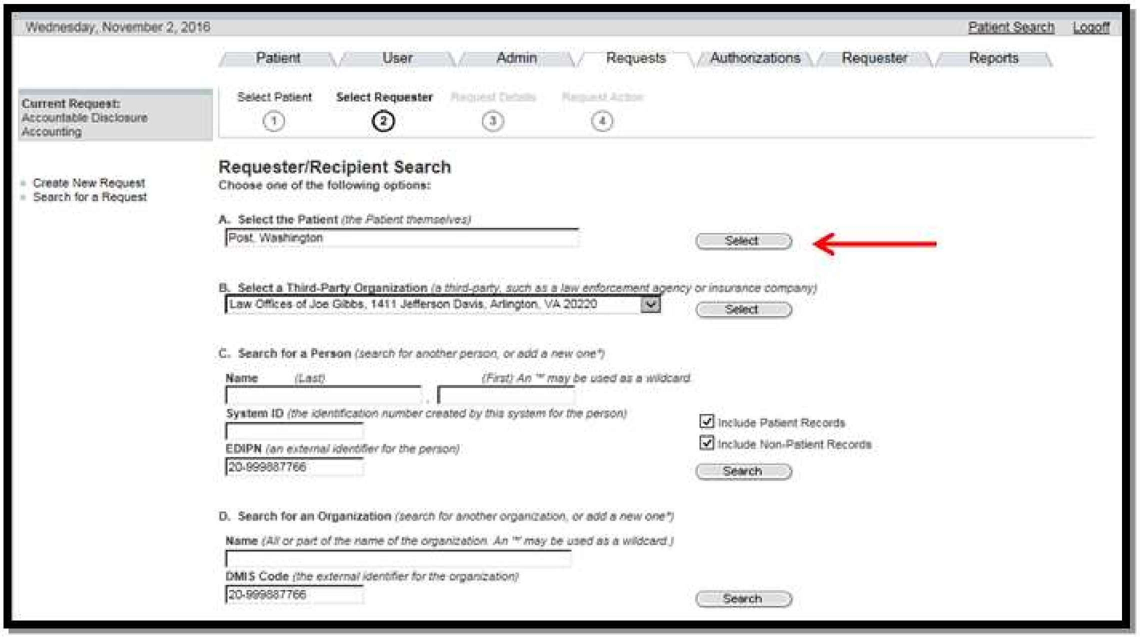
4. Search for the patient.



5. Select the Patient.

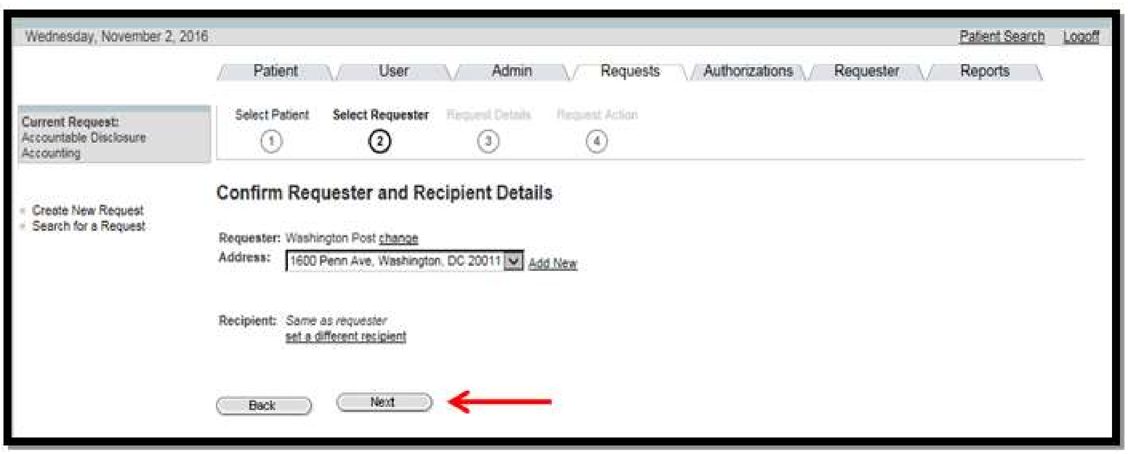


6. Select the Requester.

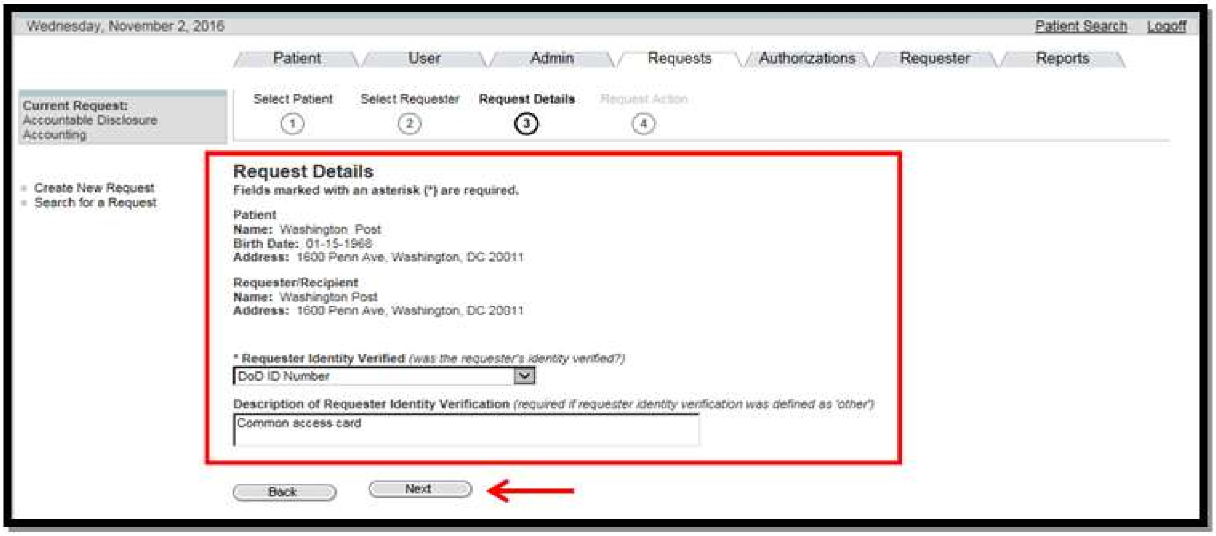


7. Confirm the requester and recipient details.

8. Click on the Next button.



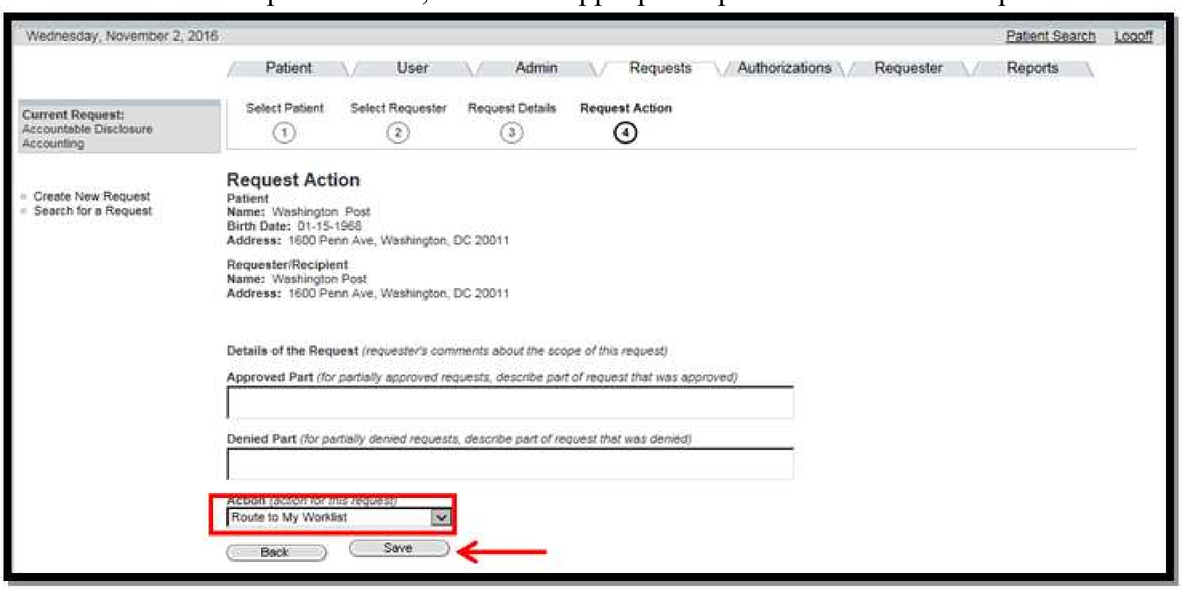
9. Enter the Request Details: requester identity verification, and description of verification, as applicable.



10. Click on the Next button.

11. Enter in the Details of the Request, to include Approved Part/Denied Part.

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



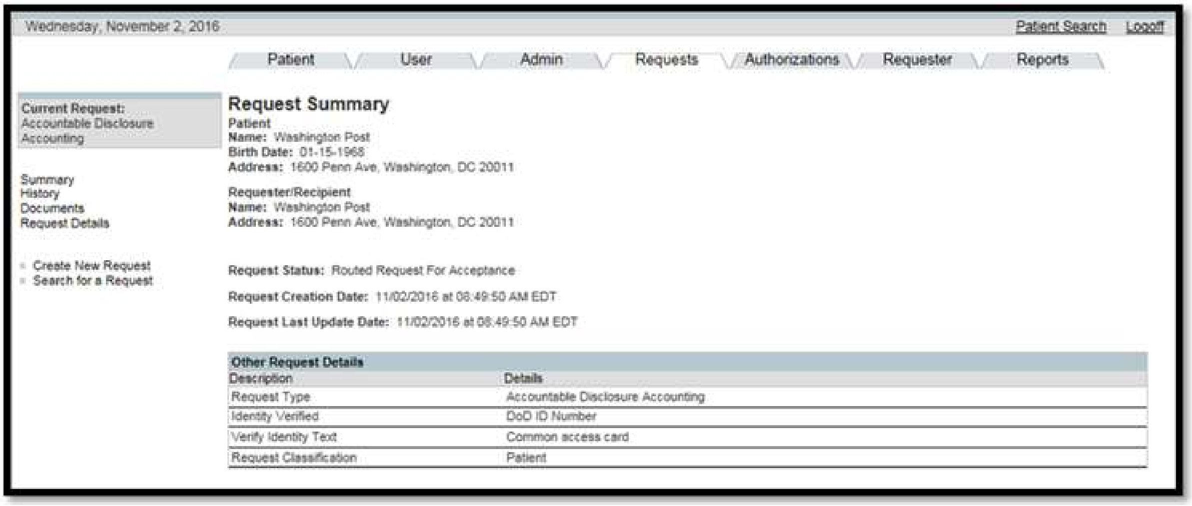
The Request Action window provides you with various accounting disclosure actions, which are shown in this table:

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.



5.3.6 Approve Accounting of Disclosures Request

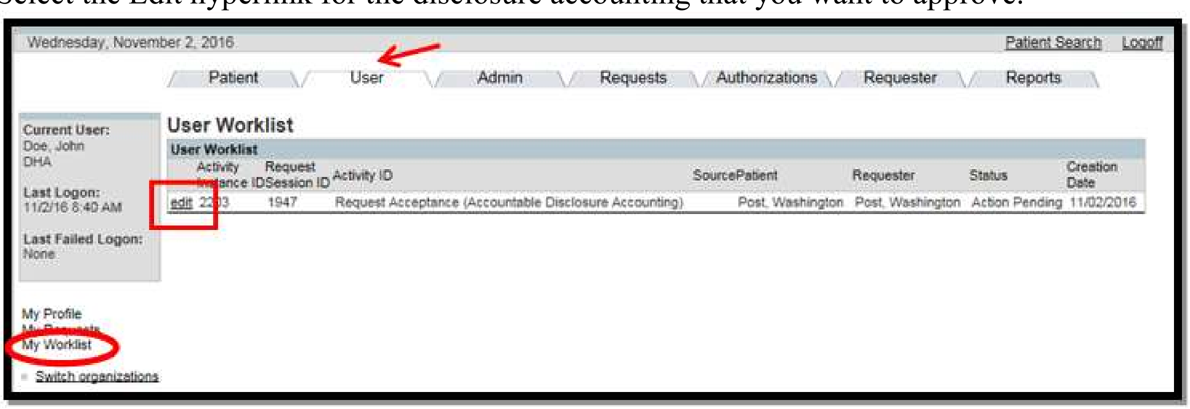
A patient may ask for an Accounting of Disclosures at any time. PHIMT allows for a quick reporting of this accounting.

Steps to approve an accounting of a disclosure:

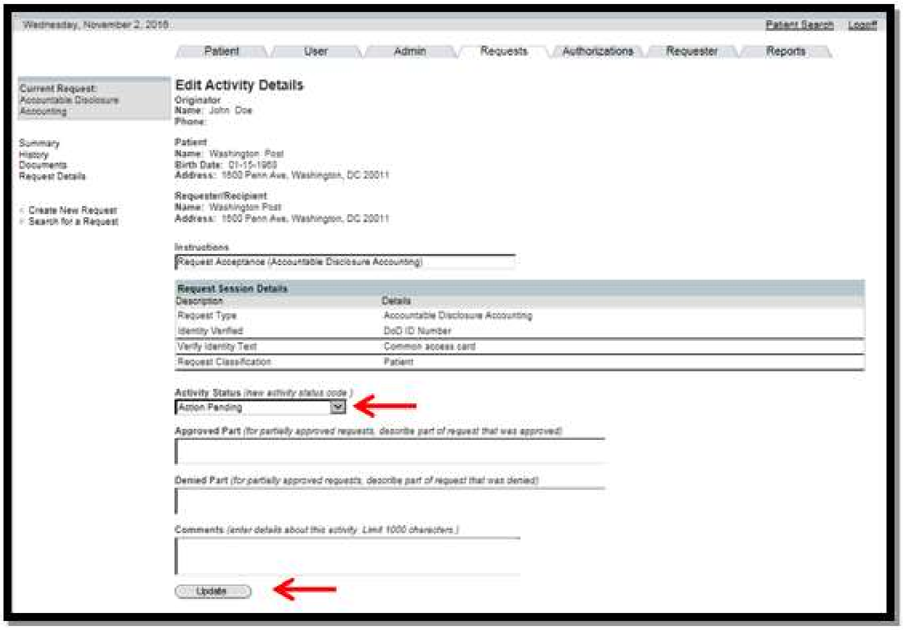
1. Select the User Tab.

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.

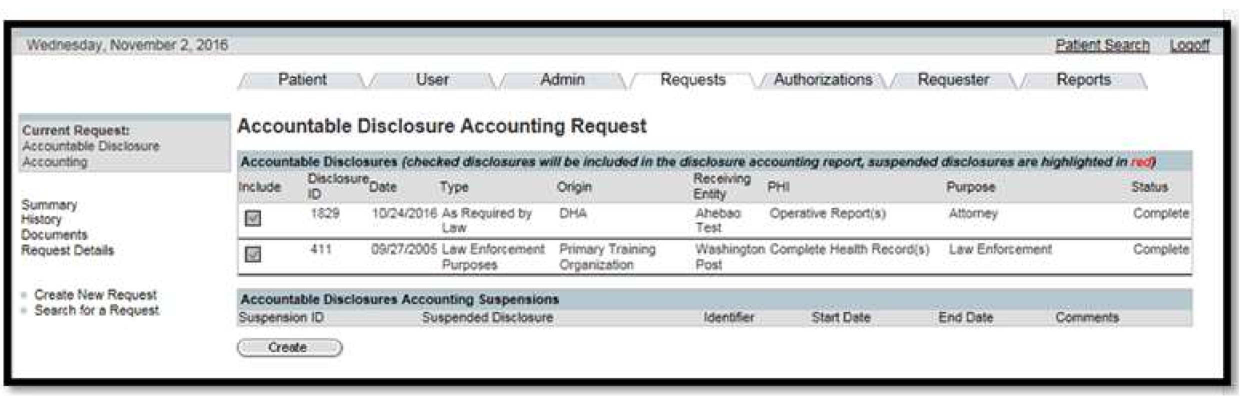


4. Select Accepted from the Activity Status drop-down box.

5. Click on the Update button.

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

NOTE: *The accounting disclosure is no longer shown in your User Worklist.*



5.3.7 Generate an Accounting of Disclosures Report

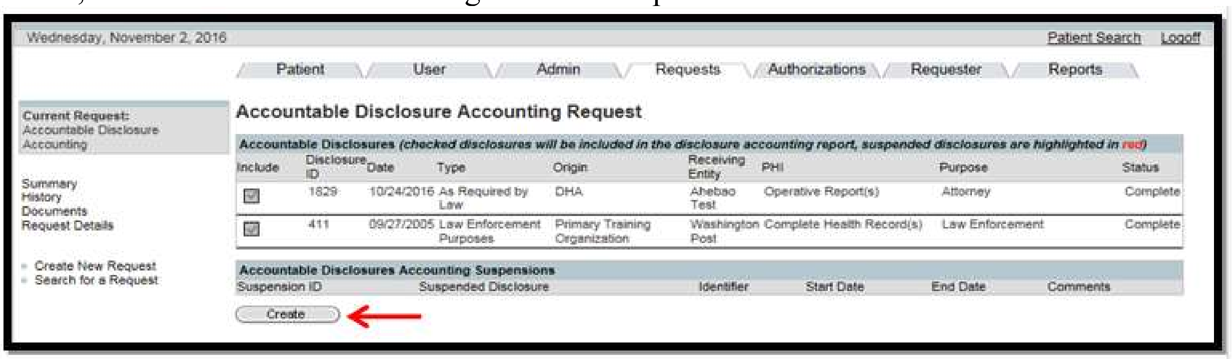
An accounting of disclosures report is a summary of all of the disclosures made for a particular patient. Once a request has been approved, an accounting of disclosures report can be generated. Pending disclosures will not display in the report.

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

Steps to generate an Accounting of Disclosures Report:

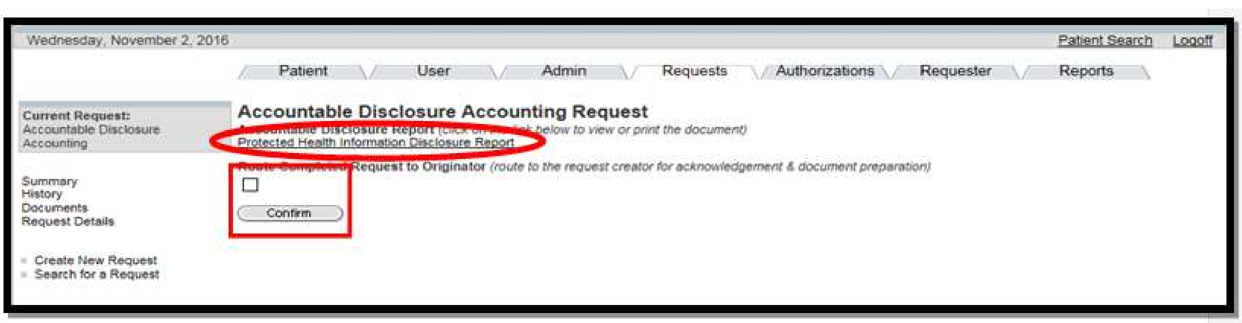
1. From the Requests Tab, follow steps 5.3.5 to create a new request.

2. Once the patient has been selected, from the Accountable Disclosure Accounting Request screen, click on the Create button to generate the report.



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

<u>NOTE:</u> *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 in PDF.

Protected Health Information Disclosure Report

Prepared for: Washington Post

Requested from: DHA

Generated on: 11-02-2016

Disclosure ID:	1829
Date of Disclosure:	2016-10-24
Accountable Disclosure Type:	As Required by Law
Disclosure Purpose:	Attorney
Disclosed Health Information:	Operative Report(s)
Disclosure Originated From:	DHA Five Skyline Place, 5111 Leesburg Pike, Falls Church, VA 22041-3206
Disclosure Recipient:	Test, Ahebao Oweah16032, Hesperia, CA 92345-4001
Disclosure Requester:	Post, Washington 1600 Penn Ave, Washington, DC 20011

Disclosure ID:	411
Date of Disclosure:	2005-09-27
Accountable Disclosure Type:	Law Enforcement Purposes
Disclosure Purpose:	Law Enforcement
Disclosed Health Information:	Complete Health Record(s)
Disclosure Originated From:	Primary Training Organization Skyline Pl., Falls Church, VA 20110
Disclosure Recipient:	Post, Washington 1600 Penn Ave, Washington, DC 20011
Disclosure Requester:	Post, Washington 1600 Penn Ave, Washington, DC 20011

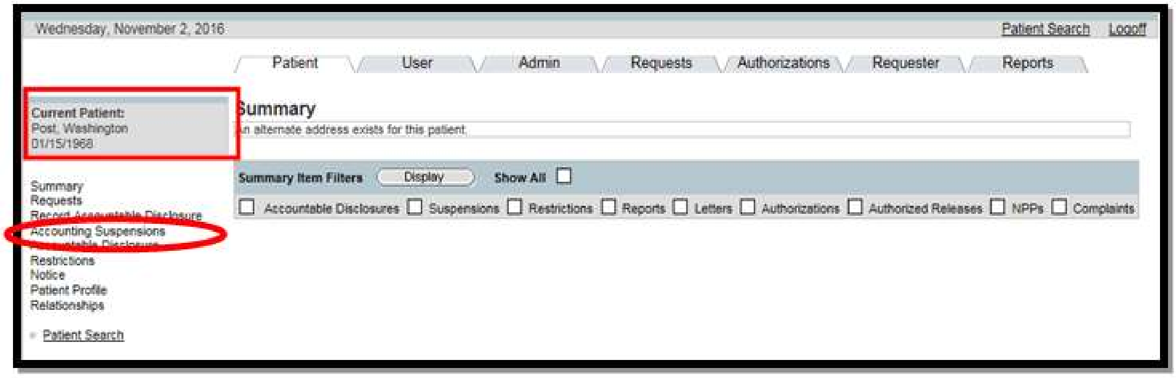
5.3.8 Create a Suspension

Per DoD 6025.18-R C13.1.2.1, "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." 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.

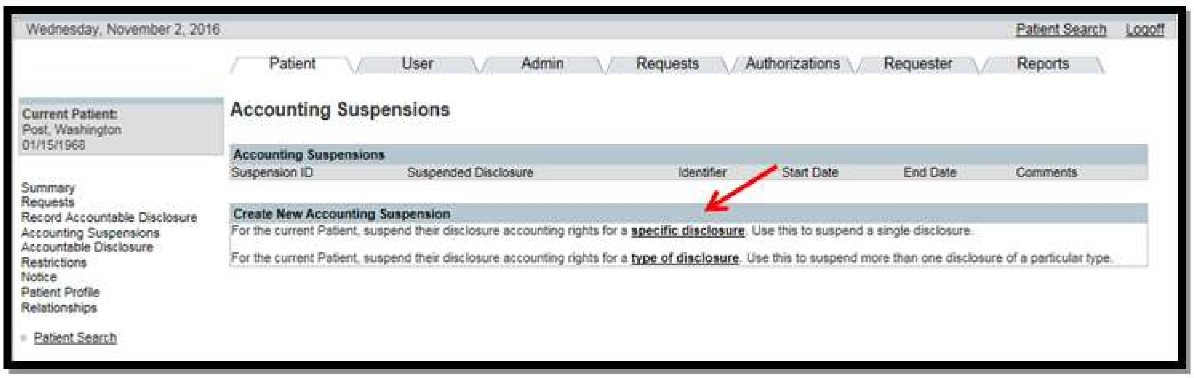
Steps to create a suspension:

1. Search for and select a patient record.

2. Select the Accounting Suspensions hyperlink.



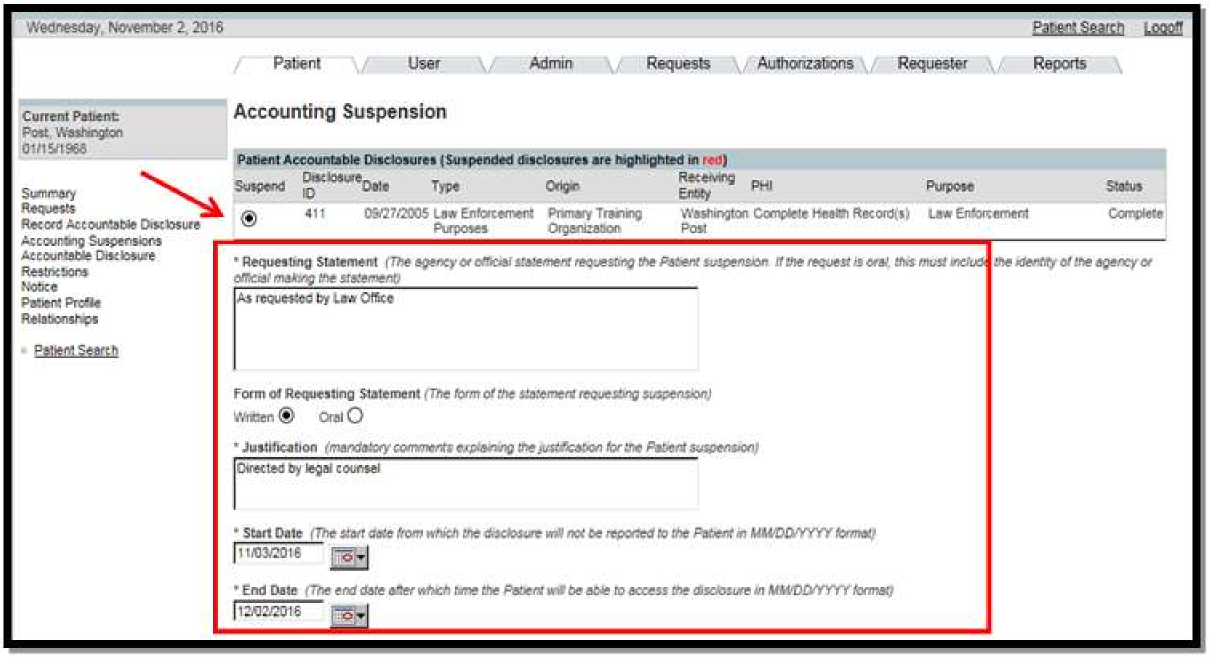
3. Select the Specific Disclosure hyperlink.



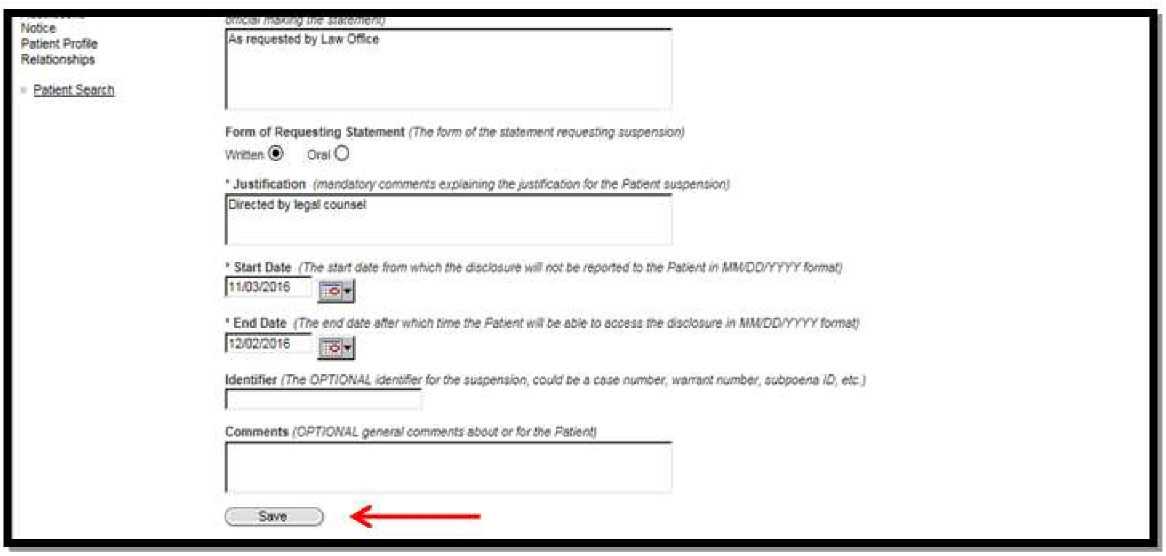
4. Click on the radio button for the disclosure you want to suspend.

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.

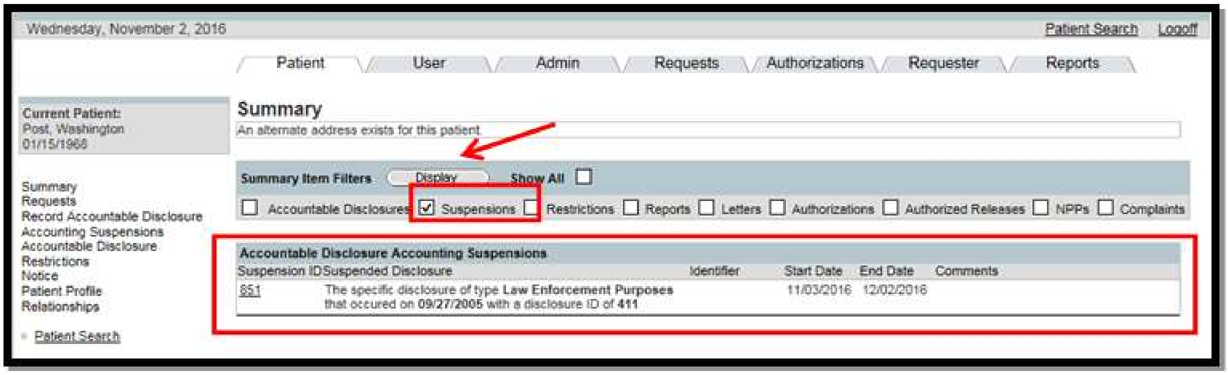


7. Select from the left column the Summary hyperlink.

8. Check the Suspensions checkbox.

9. Click on the Display button.

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



5.3.9 Record Complaints

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.

Steps to Record a Complaint:

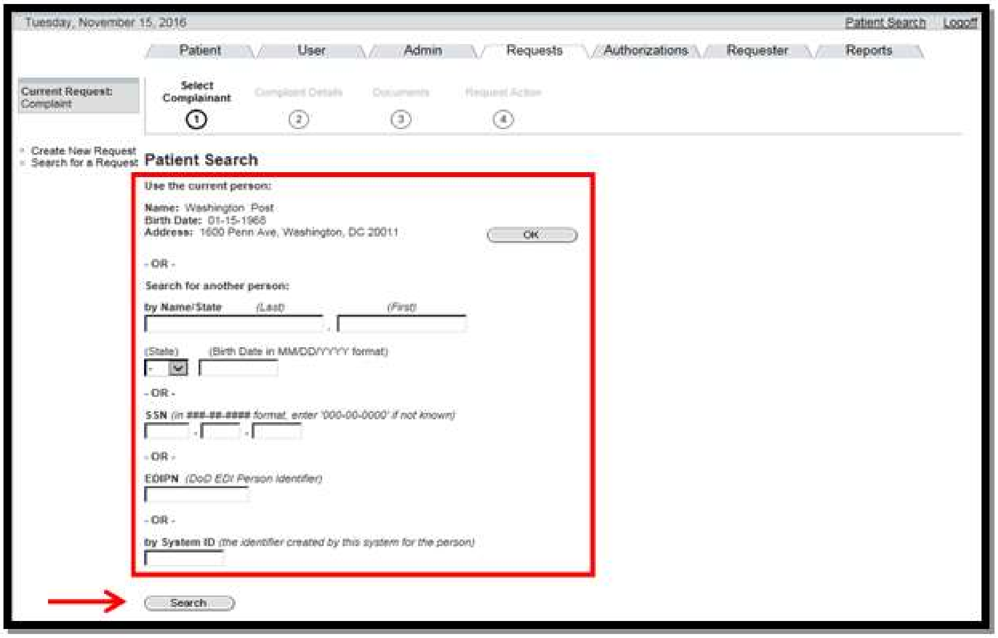
1. Select the Requests Tab.

- The Create New Request Screen will appear.

2. Click the Complaint radio button.

3. Click on the Next button.

- The Select Complainant Screen will appear.

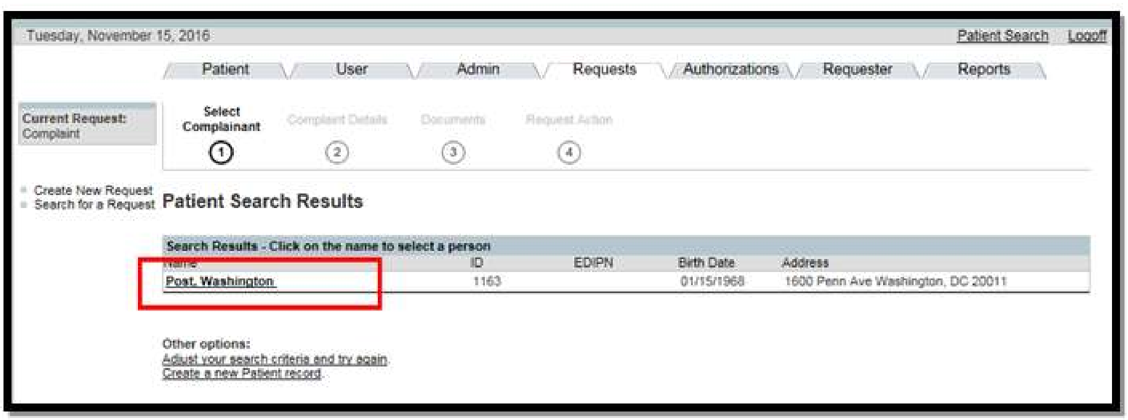


4. Search for the patient.

5. Click on the Search button.

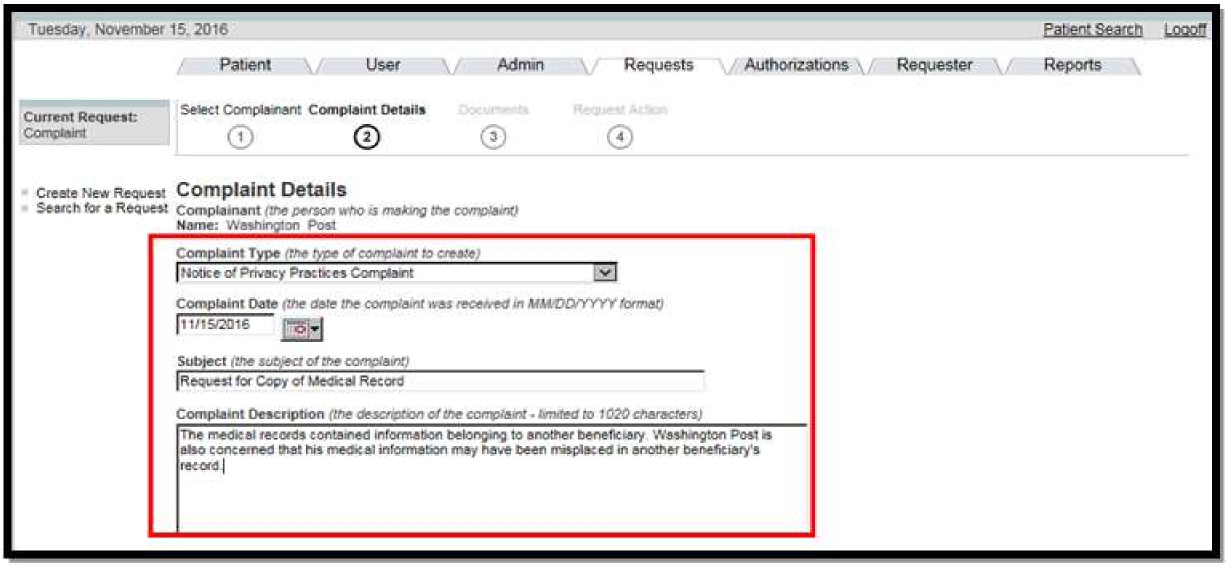
   - The Patient Search Results Screen will appear.

6. Select the Patient.

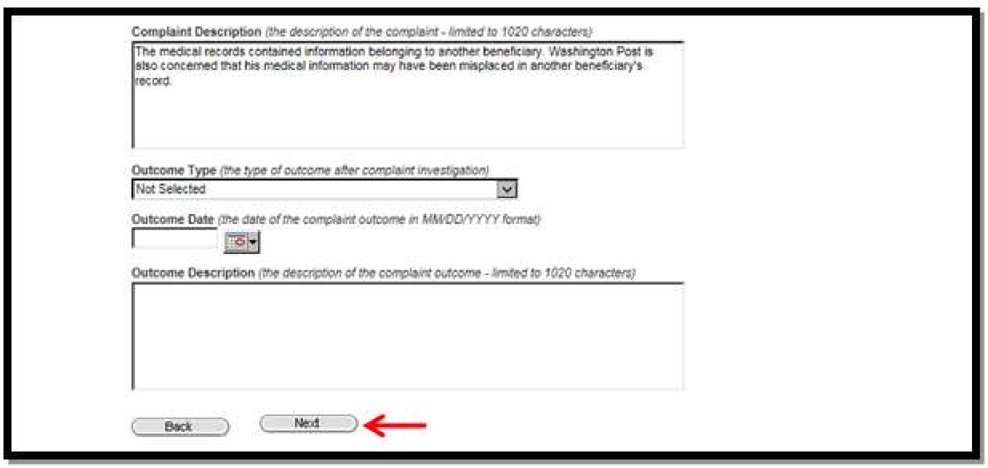


- The Complaint Details Screen will appear.

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



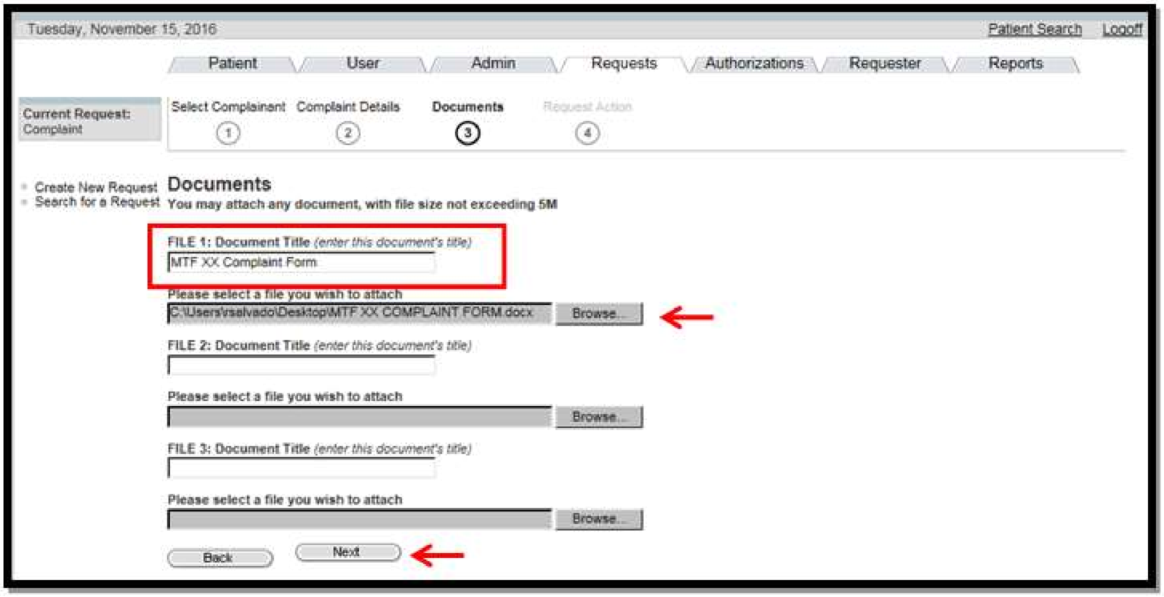
8. Scroll to the bottom of the screen and click on the Next button.



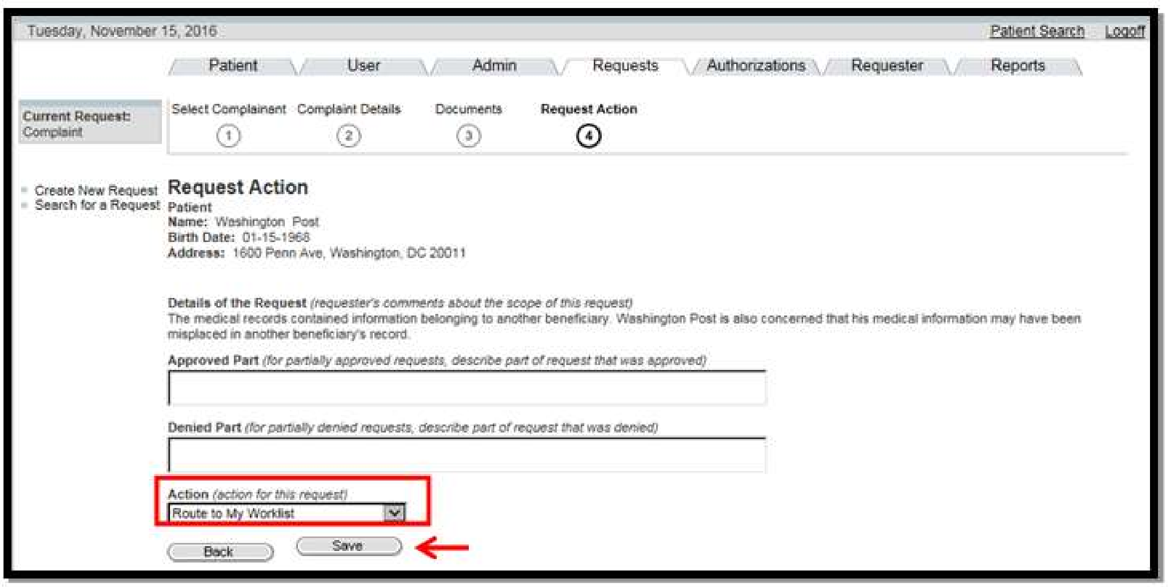
9. To attach any documents, type in the document title.

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

11. Click on the Next button.



- The Request Action screen will appear.



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

13. Click on the Save button.

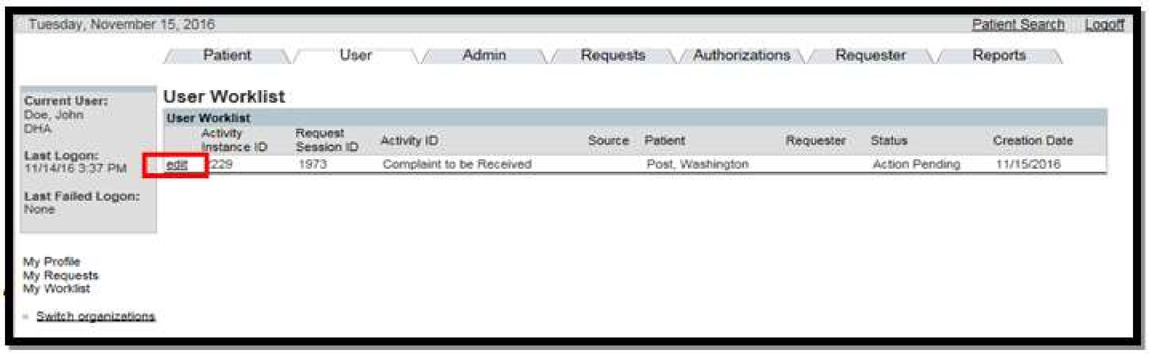
    - The Request Summary screen will display.

Steps to Receive a Complaint:

1. Select the User Tab.

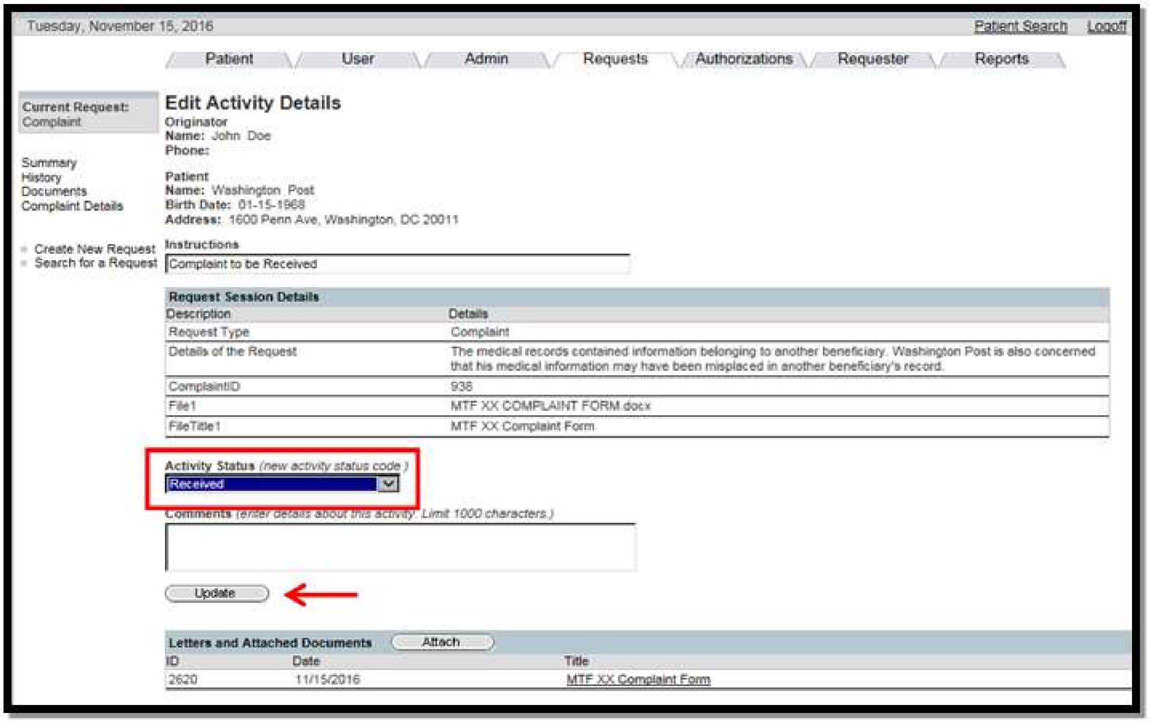
- The complaint will appear in the User Worklist.

2. Select the Edit hyperlink.

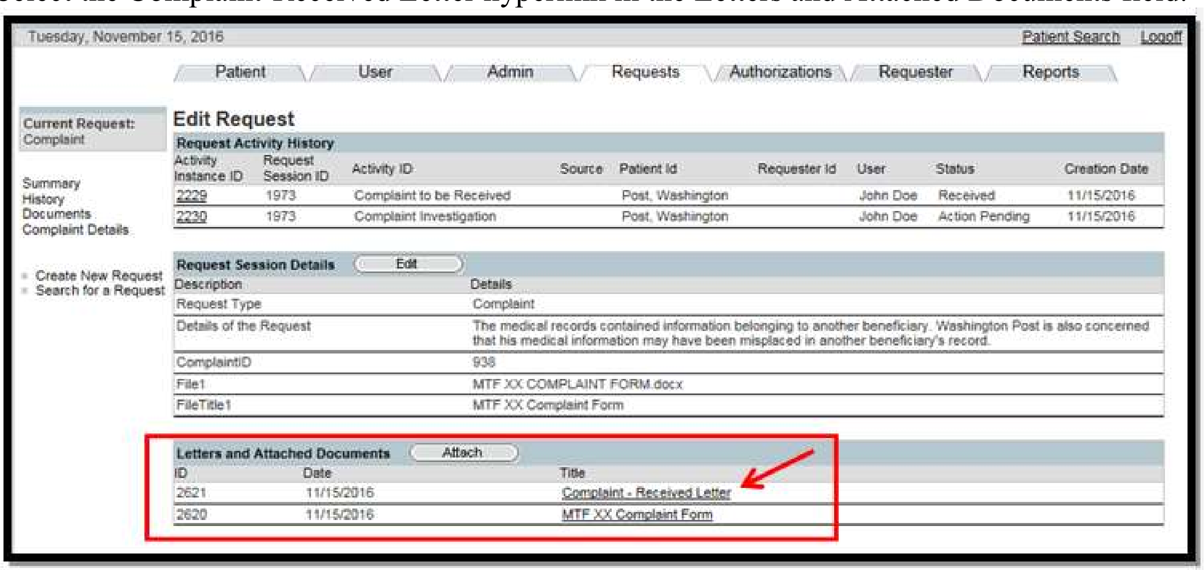


- The Edit Activity Details Screen will appear.

3. From the Activity Status drop-down box, select Received.



4. Click on the Update button.
   - The Edit Request screen will appear.
5. Select the Complaint-Received Letter hyperlink in the Letters and Attached Documents field.



- The Complaint Received Letter is generated.

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

15 Nov 16

Washington Post
1600 Penn Ave
Washington, DC 20011

Dear Washington Post

Your Health Information Complaint Form, dated 11/15/2016 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 DHA, Five Skyline Place, 5111 Leesburg Pike, Falls Church, VA 22041-3206, .

Sincerely

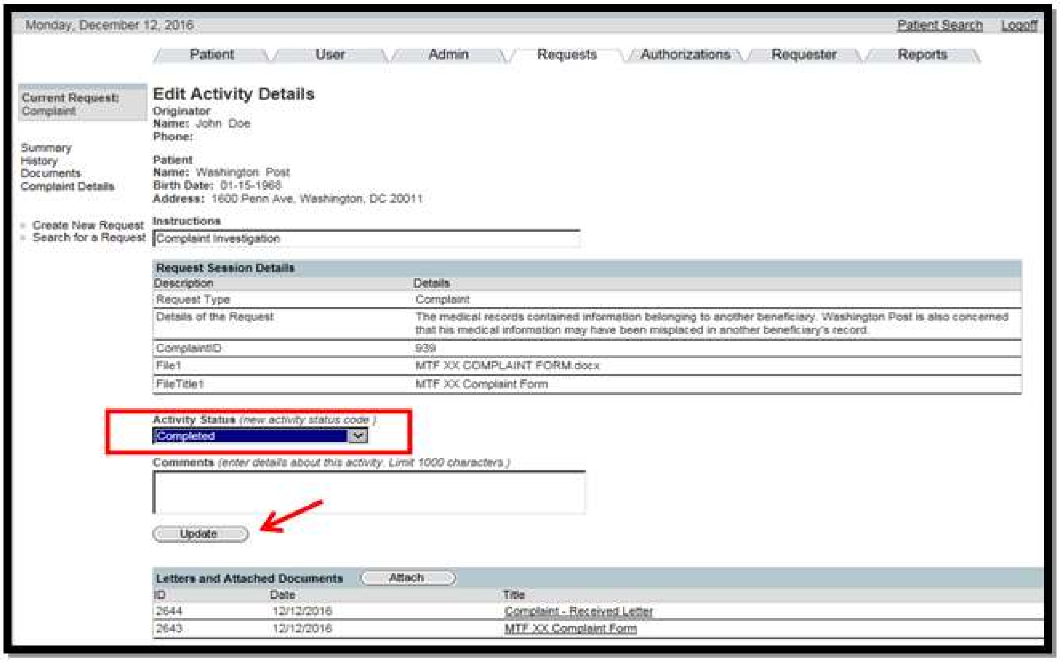
Privacy Officer

Steps to Update the Complaint:

1. Select the User Tab.

2. Select the Edit hyperlink.

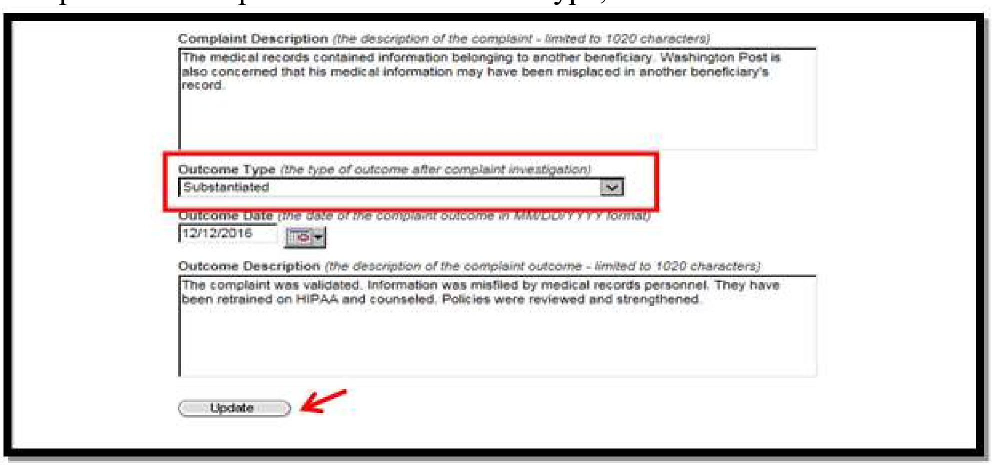
3. From the Activity Status drop-down box, select Completed.



4. Click on the Update button.

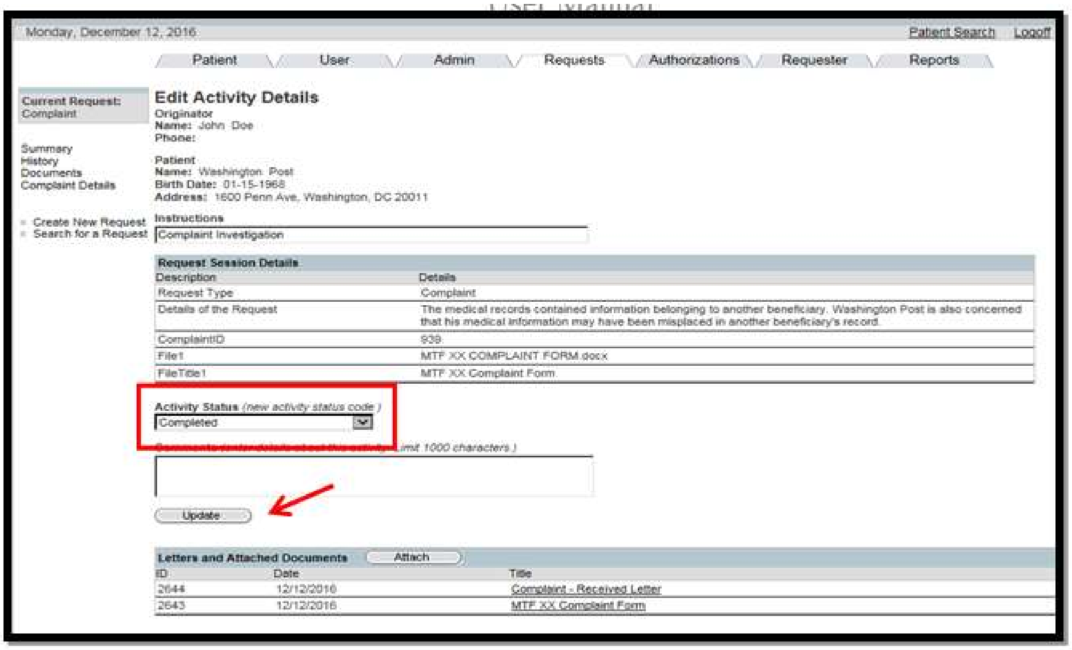
   - The Complaint Details Screen will appear.

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



6. Click on the Update button.

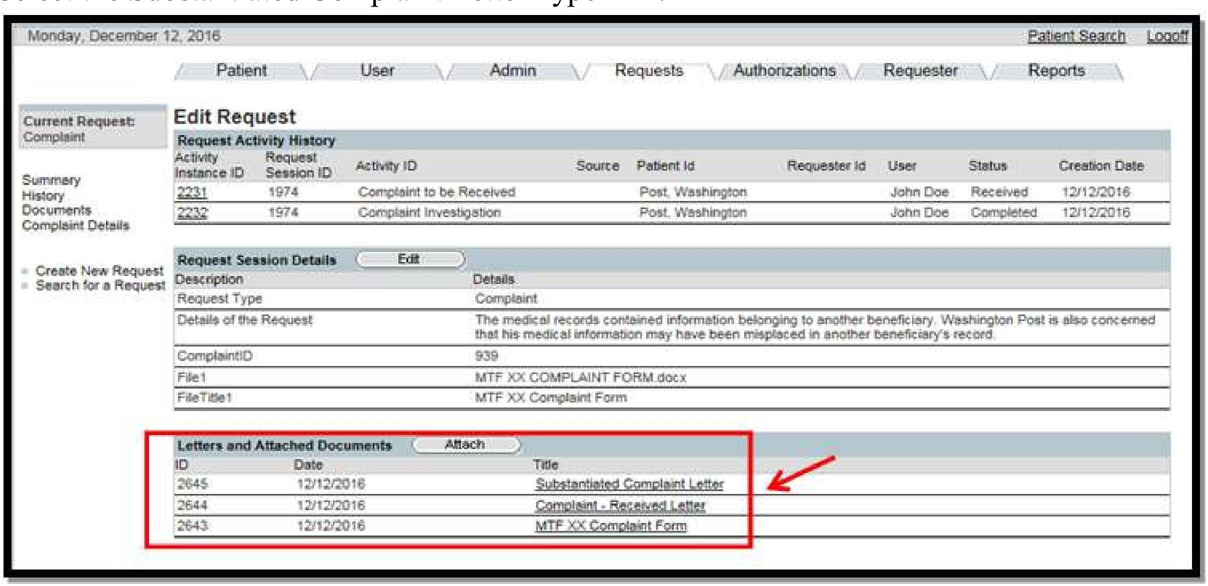
7. Select Completed from the Activity Status drop-down box.



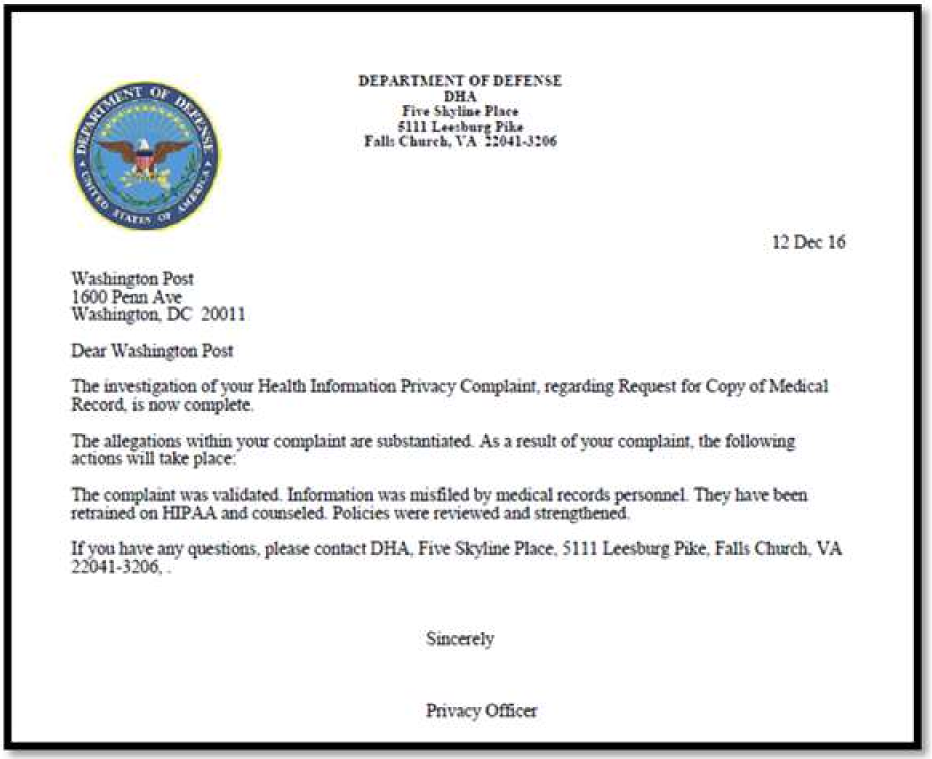
8. Click on the Update button.

- The Edit Request Screen will appear.

9. Select the Substantiated Complaint Letter hyperlink.



- The Substantiated Complaint Letter is generated.



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

12 Dec 16

Washington Post
1600 Penn Ave
Washington, DC 20011

Dear Washington Post

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 validated. Information was misfiled by medical records personnel. They have been retrained on HIPAA and counseled. Policies were reviewed and strengthened.

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

Sincerely

Privacy Officer

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

5.3.10 Record a Restriction

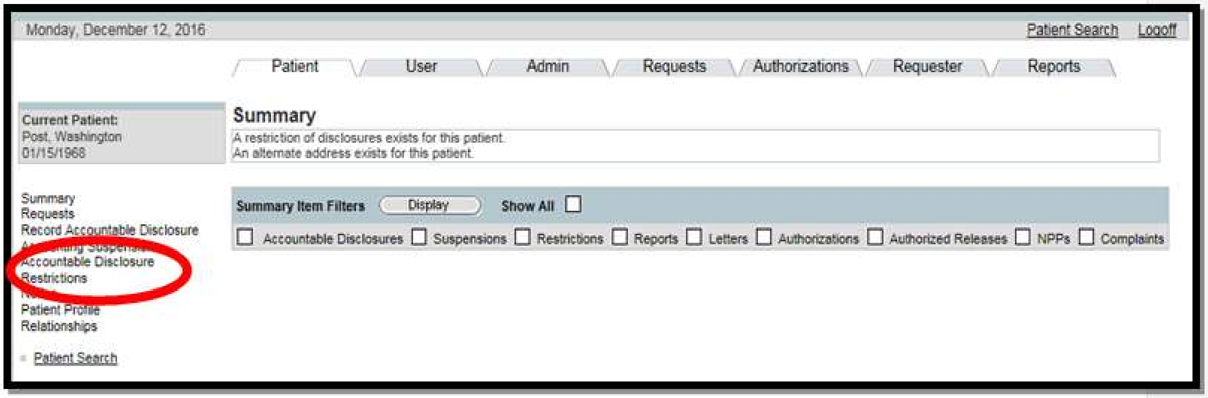
As a Privacy Specialist you are able to enter a Restriction of Disclosure or terminate a Restriction of Disclosure. Restriction of Disclosures allows members to restrict uses and disclosure of their PHI.

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.*

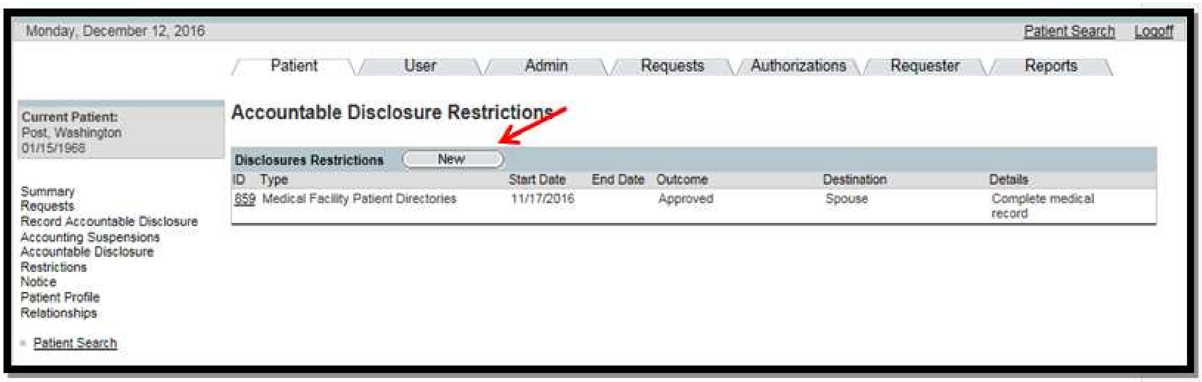
Steps to record a disclosure restriction:

1. From the Patient tab, search for and select a patient record.

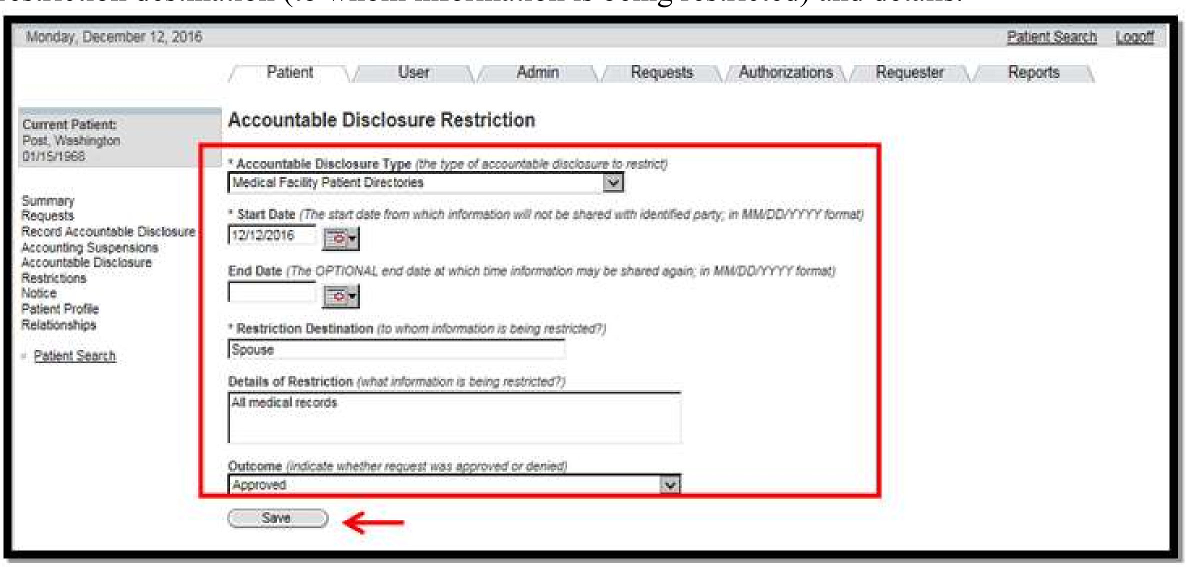
2. Select the Accountable Disclosure Restrictions hyperlink.



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



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



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

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

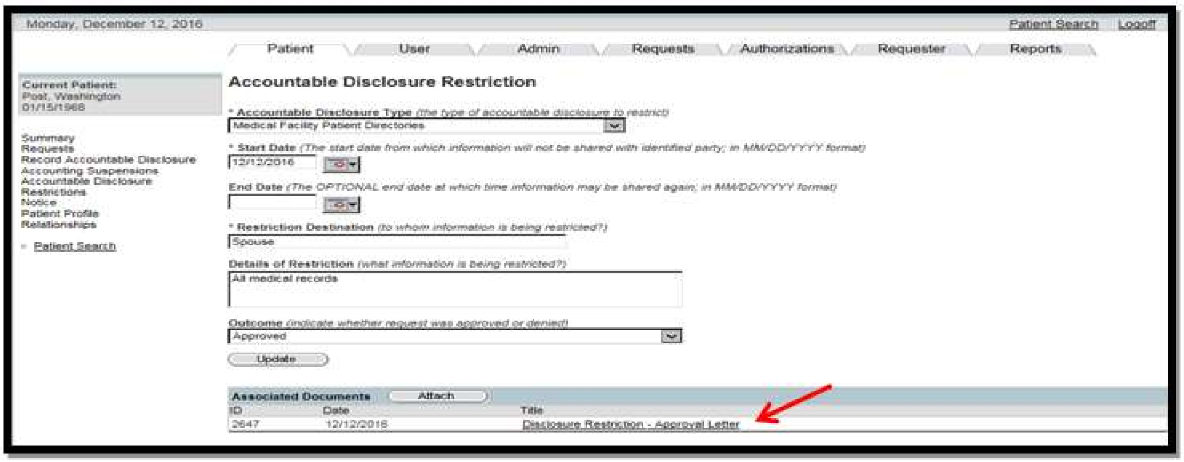
6. Click on the Save button.

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

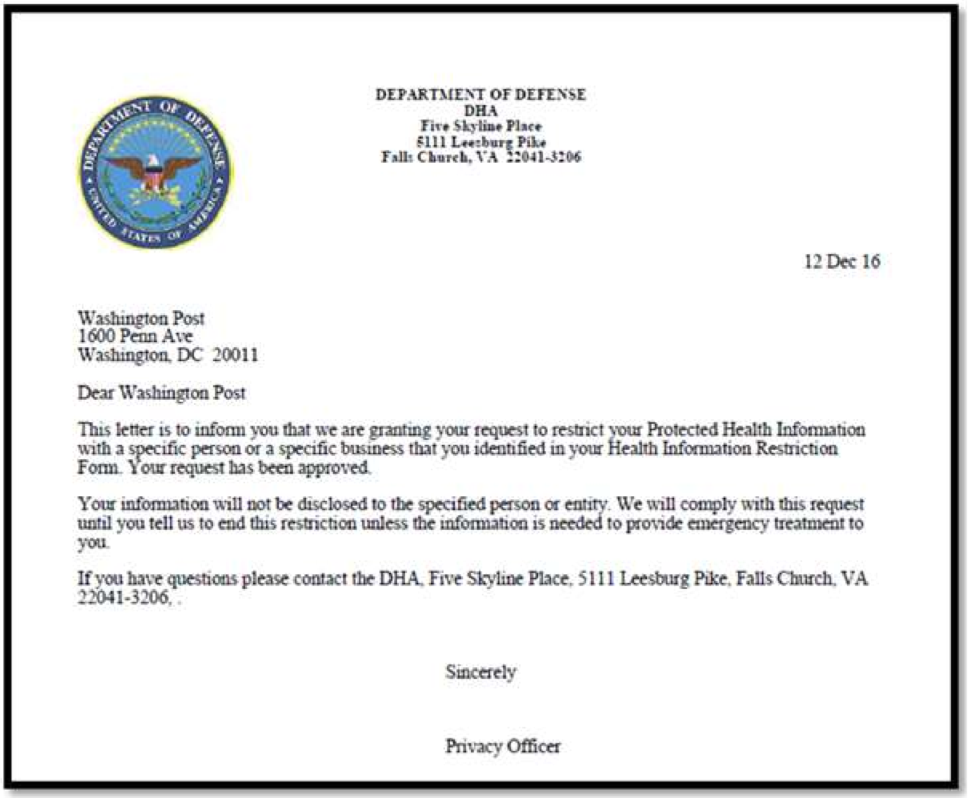
Once you have approved or denied the disclosure restriction you have the ability to generate an approval or denial letter. The letter will be pre-populated with the information that you entered for that particular restriction.

Steps to print the Approval or Denial Letter:

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



   - The Approval/Denial letter is generated.



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

12 Dec 16

Washington Post
1600 Penn Ave
Washington, DC 20011

Dear Washington Post

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 DHA, Five Skyline Place, 5111 Leesburg Pike, Falls Church, VA 22041-3206, .

Sincerely

Privacy Officer

5.3.11 Documenting Receipt of and Generating an Authorization

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

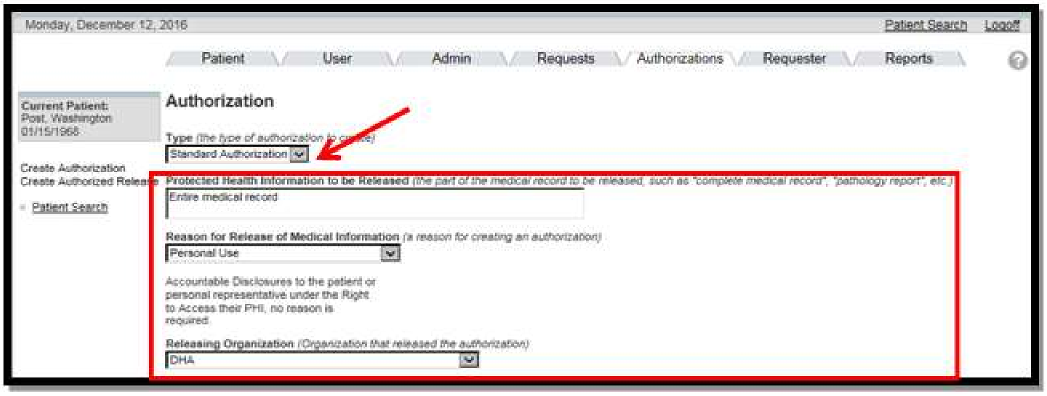
Steps to document receipt of a valid authorization:

1. Select the Patient Tab.

2. Search for and select the patient record.

3. Select the Authorizations tab.

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



5. Enter the Authorization Details: protected health information to be released, reason for release, releasing organization, and recipient.

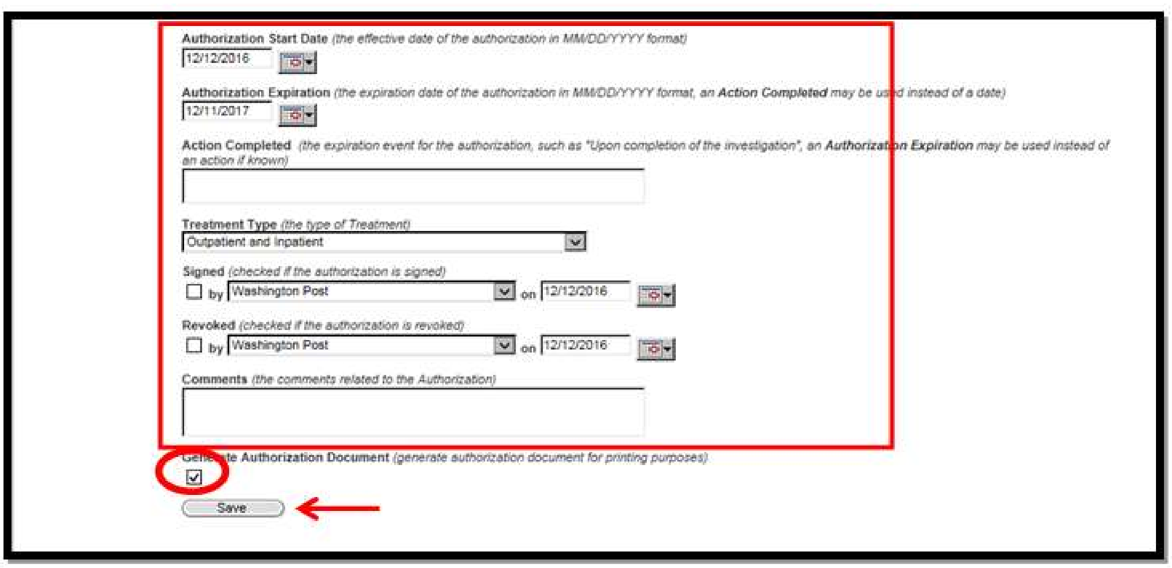
    - Enter PHI to be released as it is written on the actual authorization form.

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

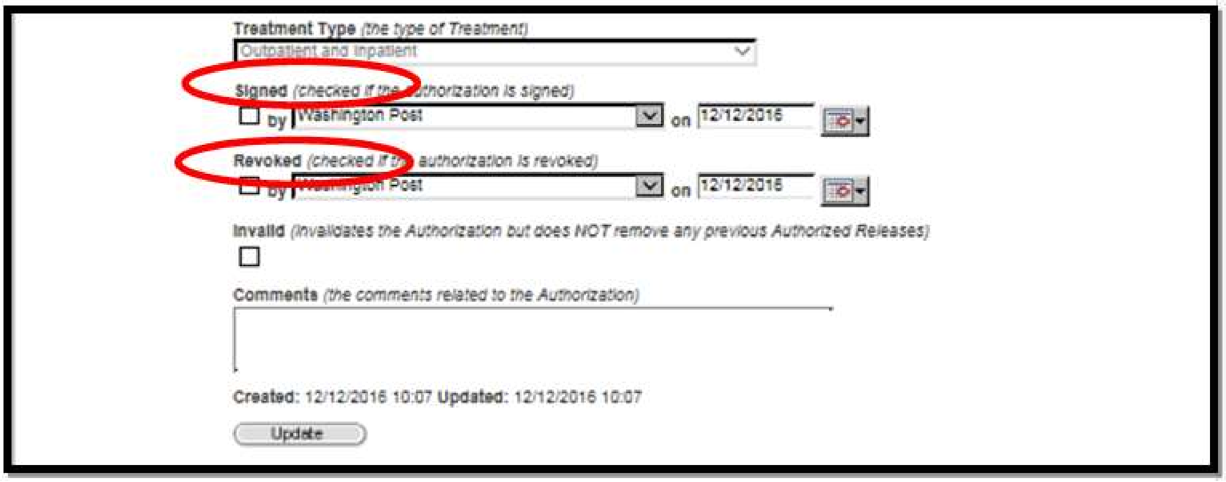
> **NOTE**: *Enter either the Authorization Expiration or an Action Completed date; not both. If there is no expiration date, then enter text in the Action Completed field (ex. Authorization to remain in effect until revoked.)*

7. Place a check in the Generate Authorization checkbox.

8. Click on the Save button.



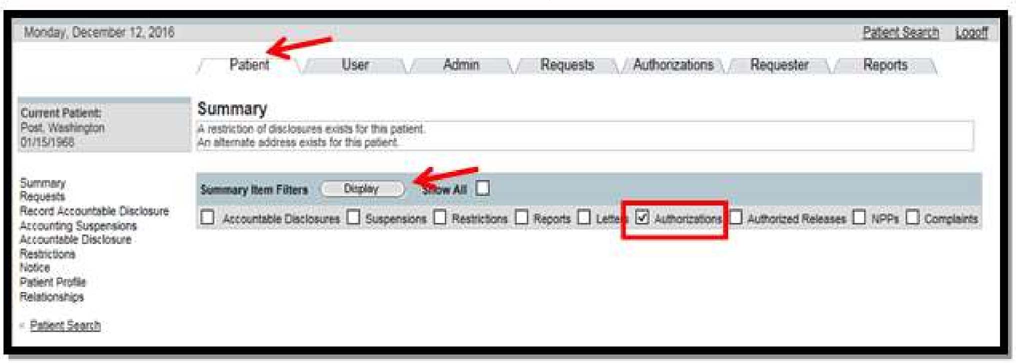
- The Signed Status and Revoked Status boxes on this screen indicate if the DD Form 2870 is signed or revoked.



- Once the authorization is saved, only the “Signed,” “Revoked,” or “Invalid” status fields can be changed.

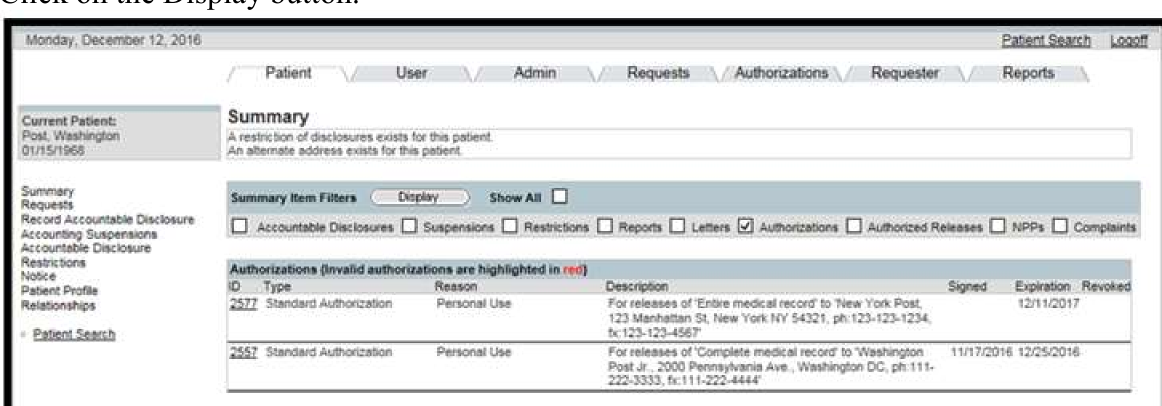
<u>NOTE</u>: *Once the authorization has been manually signed you can go back into the particular authorization and select the Signed checkbox and enter the date of the signature using MM/DD/YYYY format or the calendar icon to select a date.*

9. Select the Patient tab to reveal the Summary screen.



10. Place a check in the Authorizations checkbox.

11. Click on the Display button.



- The new authorization will appear on the Summary screen.

Steps to generate the DD Form 2870 (Adobe Acrobat format):

1. Select the Patient Tab.

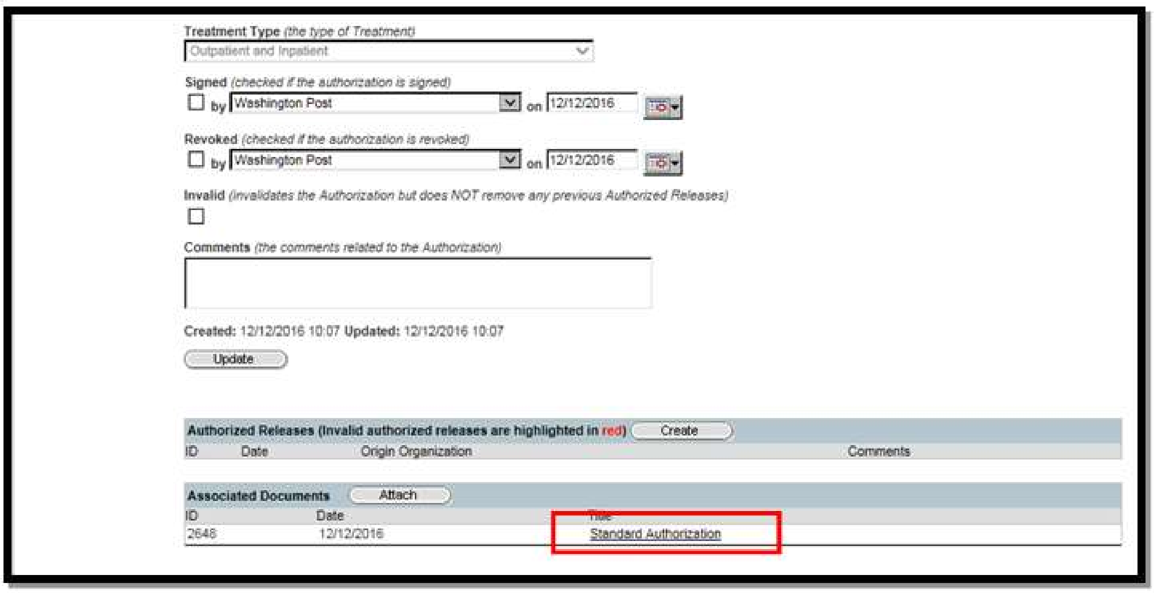
2. Search for and select the patient record.

3. From the Summary screen, check the Authorizations block.

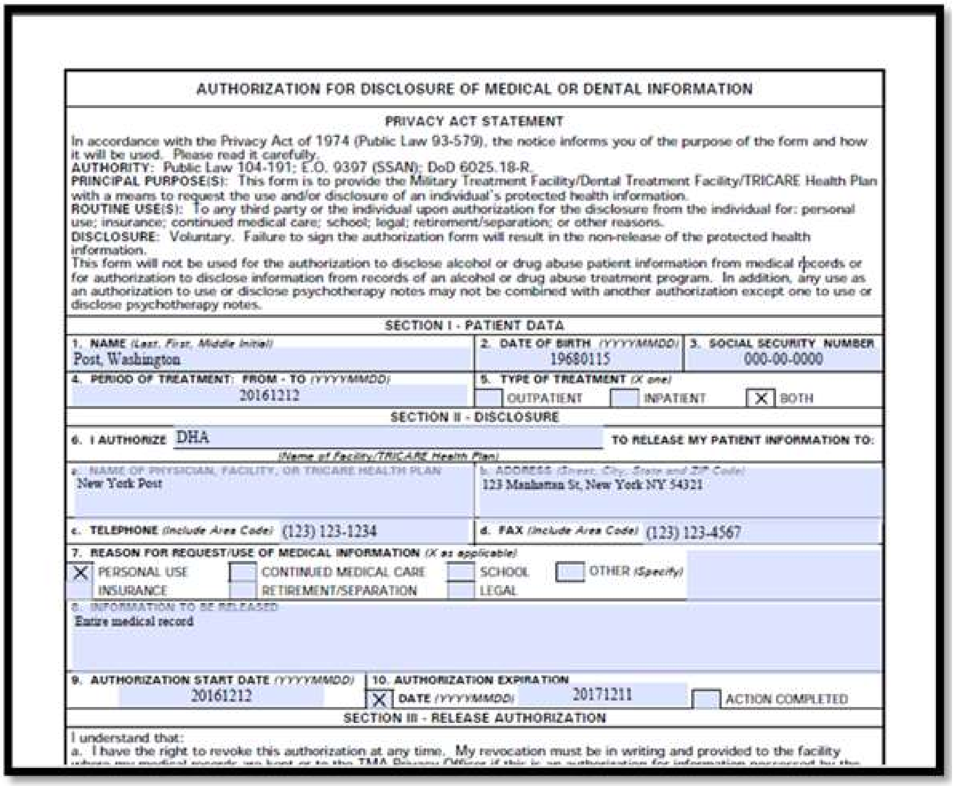
4. Click Display.

5. From the list of Authorizations, click the particular ID hyperlink.

6. Select the Authorizations tab. Scroll down to the bottom of the page and click on Standard Authorization.



7. You may print the form and request the patient’s signature.



AUTHORIZATION FOR DISCLOSURE OF MEDICAL OR DENTAL INFORMATION

PRIVACY ACT STATEMENT

In accordance with the Privacy Act of 1974 (Public Law 93-579), the notice informs you of the purpose of the form and how it will be used. Please read it carefully.
AUTHORITY: Public Law 104-191; E.O. 9397 (SSAN); DoD 6025.18-R.
PRINCIPAL PURPOSE(S): This form is to provide the Military Treatment Facility/Dental Treatment Facility/TRICARE Health Plan with a means to request the use and/or disclosure of an individual's protected health information.
ROUTINE USE(S): To any third party or the individual upon authorization for the disclosure from the individual for: personal use; insurance; continued medical care; school; legal; retirement/separation; or other reasons.
DISCLOSURE: Voluntary. Failure to sign the authorization form will result in the non-release of the protected health information.
This form will not be used for the 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.

SECTION I - PATIENT DATA

1. NAME (Last, First, Middle Initial)	2. DATE OF BIRTH (YYYYMMDD)	3. SOCIAL SECURITY NUMBER
Post, Washington	19680115	000-00-0000
4. PERIOD OF TREATMENT: FROM - TO (YYYYMMDD)	5. TYPE OF TREATMENT (X one)	
20161212	OUTPATIENT / INPATIENT / X BOTH	

SECTION II - DISCLOSURE

6. I AUTHORIZE DHA (Name of Facility/TRICARE Health Plan) TO RELEASE MY PATIENT INFORMATION TO:

a. NAME OF PHYSICIAN, FACILITY, OR TRICARE HEALTH PLAN	b. ADDRESS (Street, City, State and ZIP Code)
New York Post	123 Manhattan St, New York NY 54321
c. TELEPHONE (Include Area Code) (123) 123-1234	d. FAX (Include Area Code) (123) 123-4567

7. REASON FOR REQUEST/USE OF MEDICAL INFORMATION (X as applicable)
X PERSONAL USE; INSURANCE; CONTINUED MEDICAL CARE; RETIREMENT/SEPARATION; SCHOOL; LEGAL; OTHER (Specify)

8. INFORMATION TO BE RELEASED
Entire medical record

9. AUTHORIZATION START DATE (YYYYMMDD)	10. AUTHORIZATION EXPIRATION	
20161212	X DATE (YYYYMMDD) 20171211	ACTION COMPLETED

SECTION III - RELEASE AUTHORIZATION

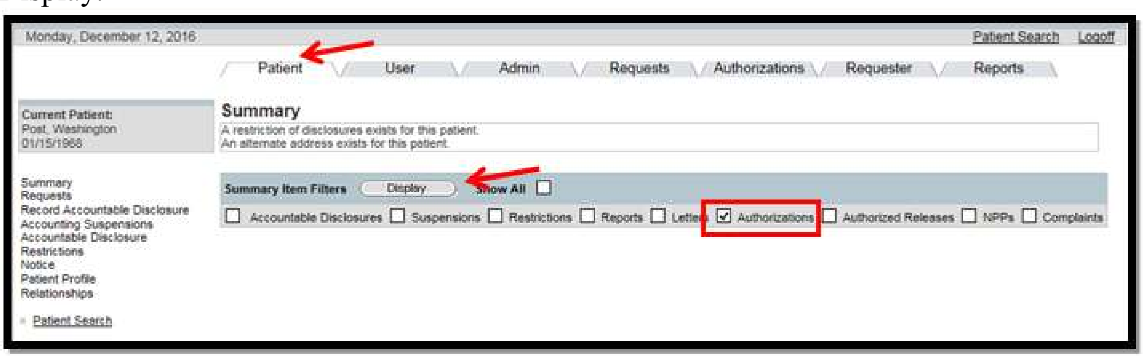
I understand that:
a. I have the right to revoke this authorization at any time. My revocation must be in writing and provided to the facility

5.3.12 Sign an Authorization

In order for an authorization to be valid, it must be signed by the patient. After the authorization is signed by the patient, a user has the ability to document in PHIMT that the signature was obtained.

Steps to document signature for an authorization has been obtained:

1. Select the Patient tab, search for patient (if applicable), check Authorizations box, and click Display.



2. Click on the numerical ID hyperlink.

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

4. Place a check in the Signed Status checkbox.

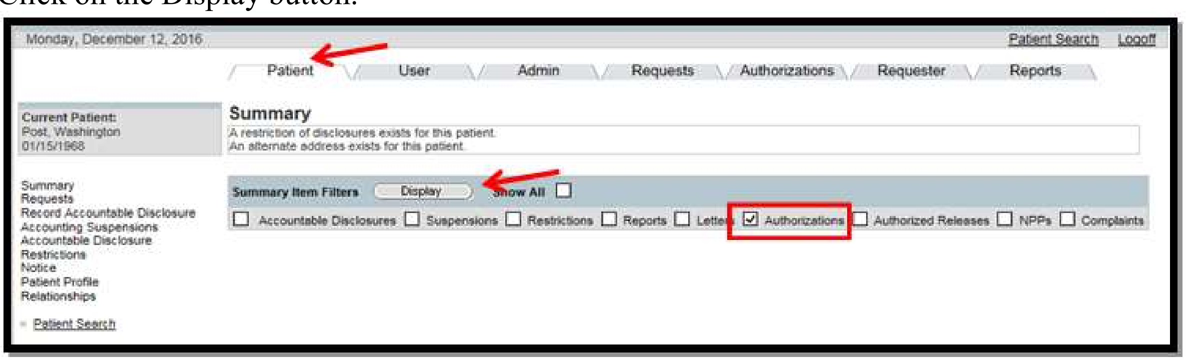
5. Select the date and the authorizing person's identity from the drop-down box.

6. Click on the Update button.

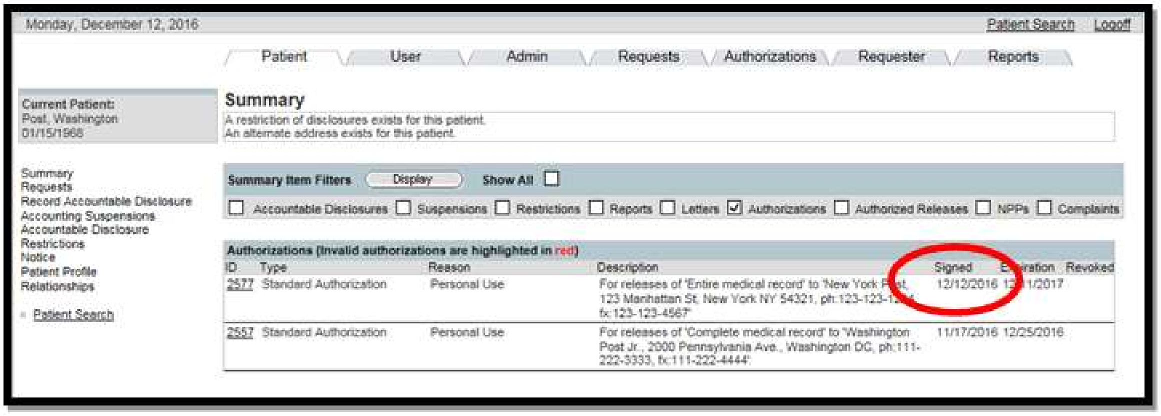
7. Select the Patient tab.

8. Place a check in the Authorizations checkbox.

9. Click on the Display button.



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



5.3.13 Revoke an Authorization

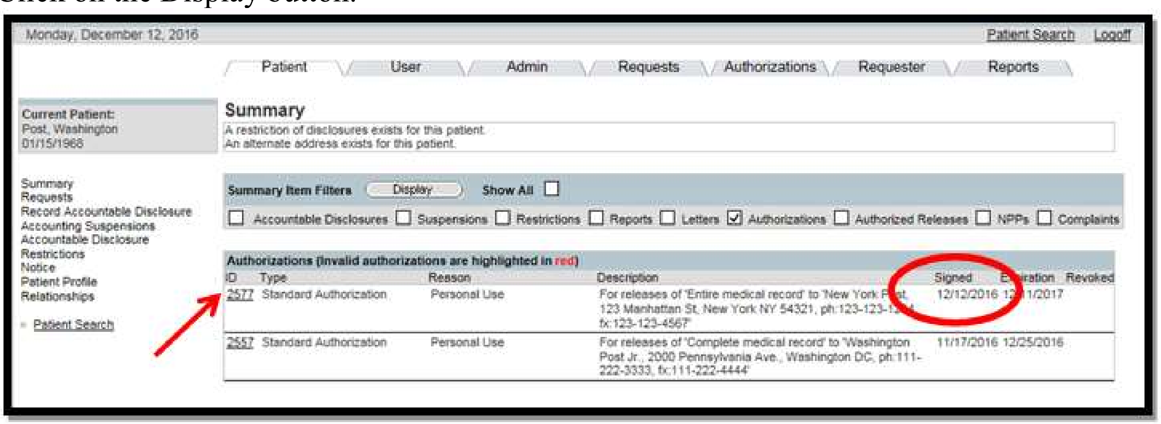
Previously generated authorizations may need to be revoked as a result of legal issues, new information, or for other reasons.

Steps to revoke an authorization:

1. Select the Patient tab and search for patient (if applicable).

2. Place a check in the Authorizations checkbox.

3. Click on the Display button.



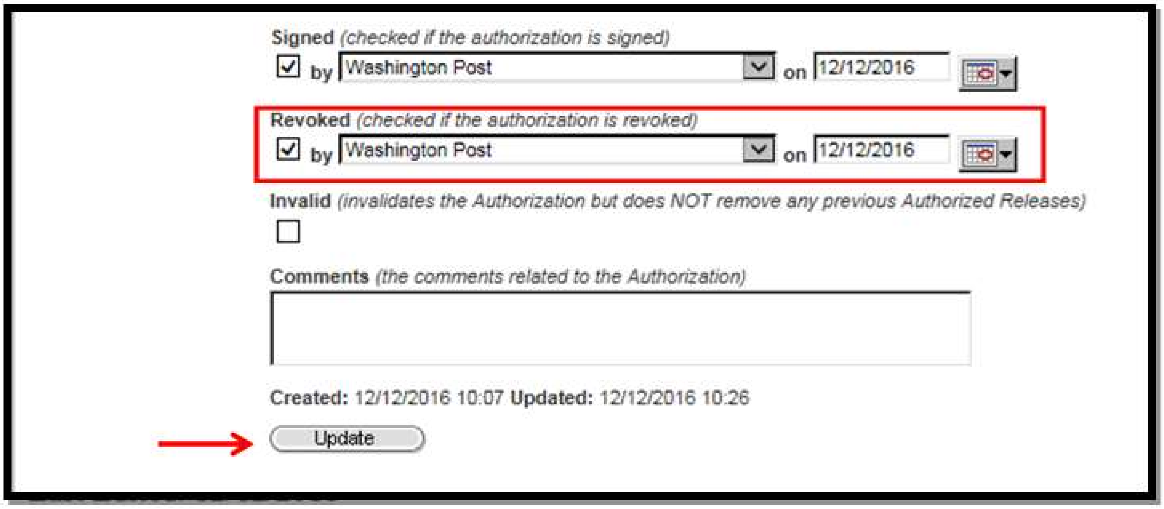
4. Select the Authorization ID hyperlink.

5. 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.

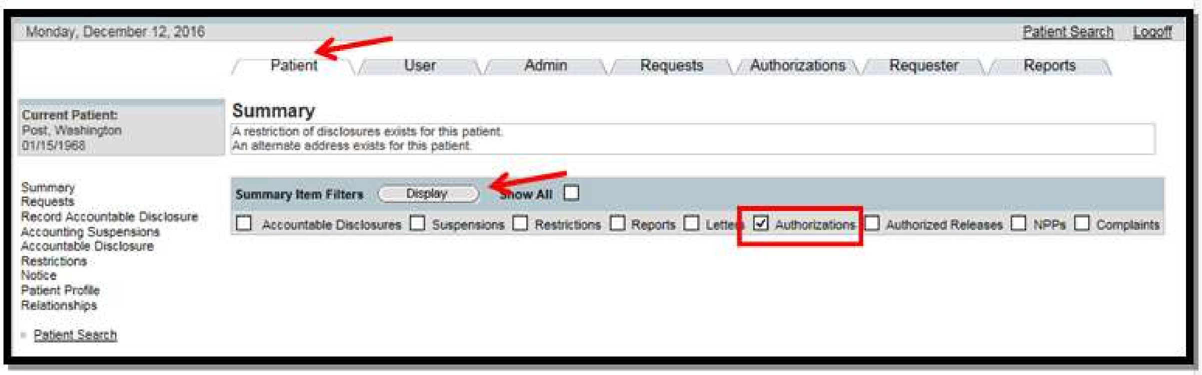
6. Click on the Update button.



7. Click on the Patient tab 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.

5.3.14 Administrative Summary Reports

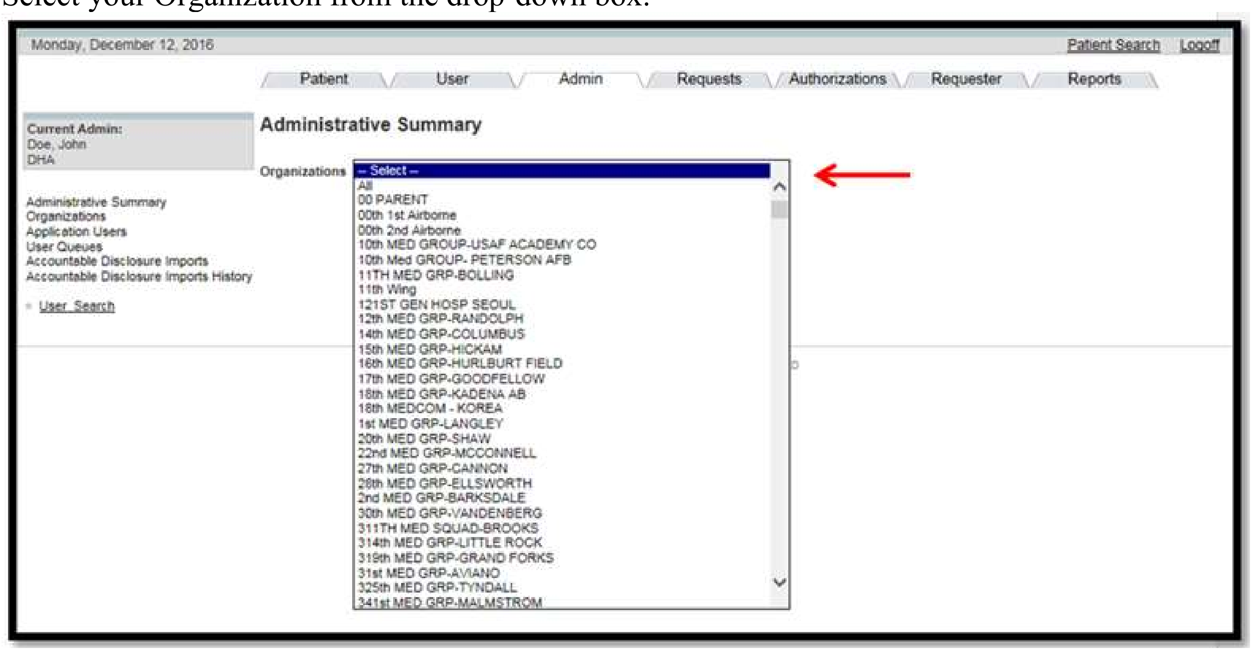
The PHIMT is capable of running several reports, which are called Administrative Summaries. Administrative Summaries provide a visual representation or snapshot view of your facilities disclosure activities.

The Administrative Summary Reports are performed by Privacy Specialists.

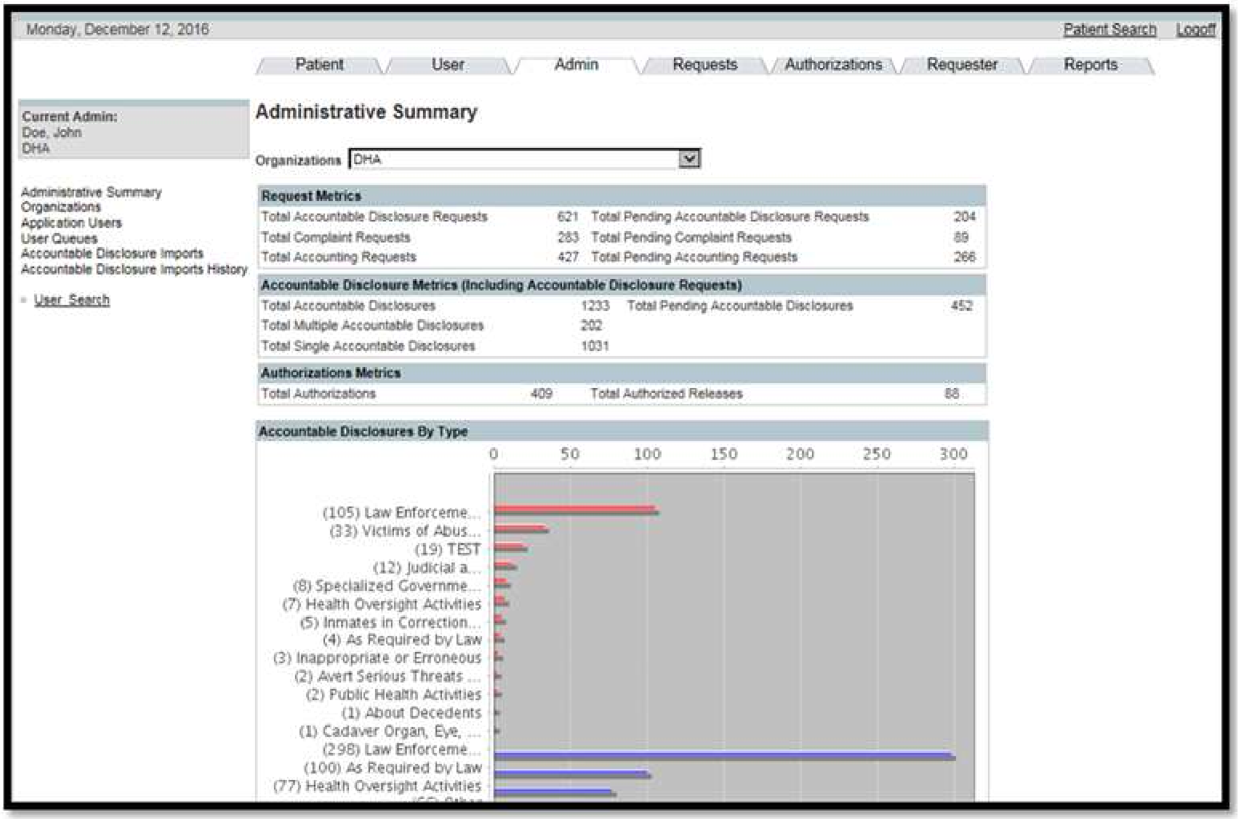
Steps to create an Administrative Summary Report:

1. Select the Admin Tab.

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



- The Administrative Summary reports will display.



5.4 REGULAR USER ACTIVITIES

This section is focused on the steps that a Regular User should perform in order to document an accounting of disclosures in PHIMT. There are many steps that are similar with those of the Privacy Specialist, but the Regular User has limited access to the system functionality requiring they enter the information through a different path. This functionality will be re-aligned in the PHIMT interface enhancements so that in the future, all data entry will follow the same path.

5.4.1 Regular User Access to Record a Disclosure

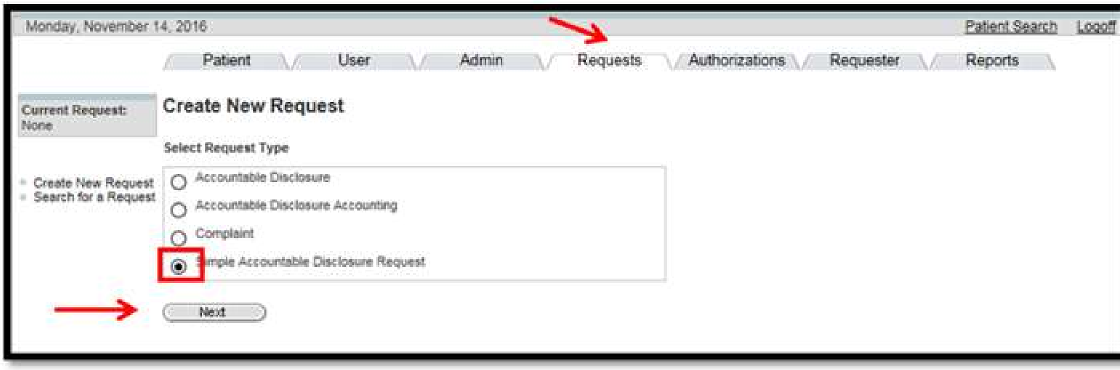
A Regular User has limited access to PHIMT. Utilizing the Requests tab, the Regular User can quickly access the system and enter the disclosure. The Regular User can select either a single accountable disclosure or a multiple accountable disclosure. . Some examples of multiple disclosures include: recurring monthly medical readiness status, dental class reports, or pre-deployment preparation reports to a commander or the commander's designee(s). Multiple Disclosures are 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.

Steps to create Disclosures

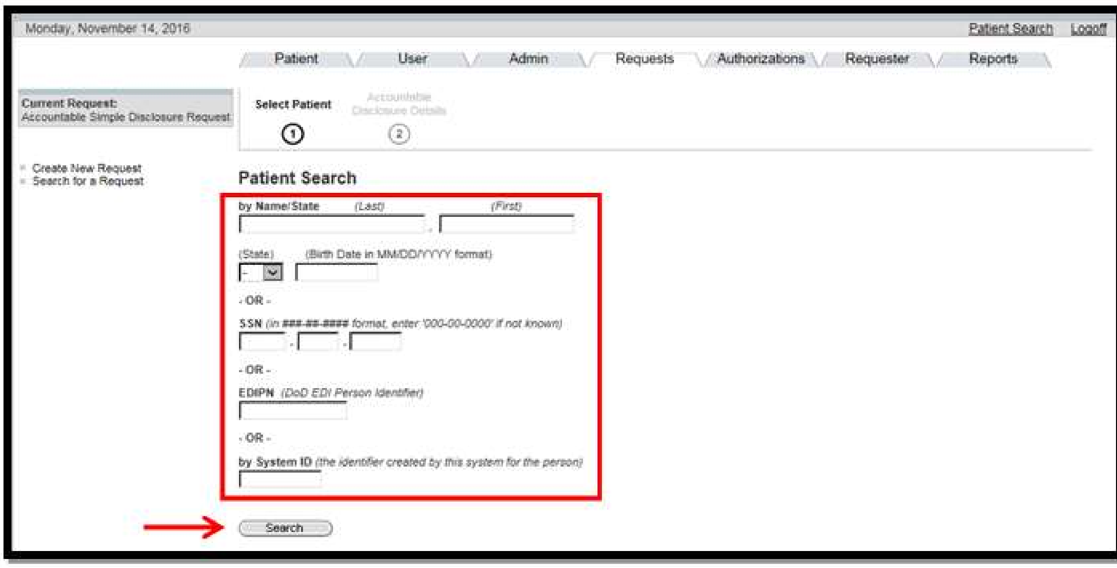
1. Click on the Requests Tab.

2. Click on the Simple Disclosure radio button.

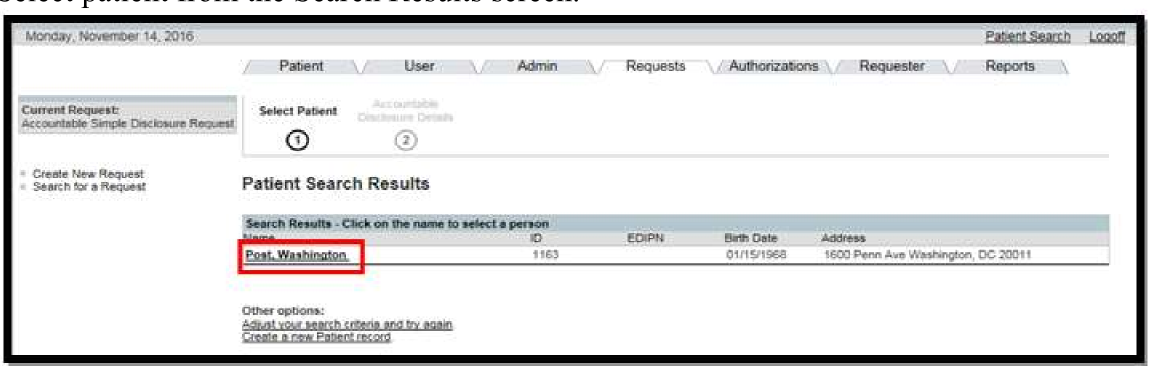
3. Click on the Next button.



4. Search for the Patient.

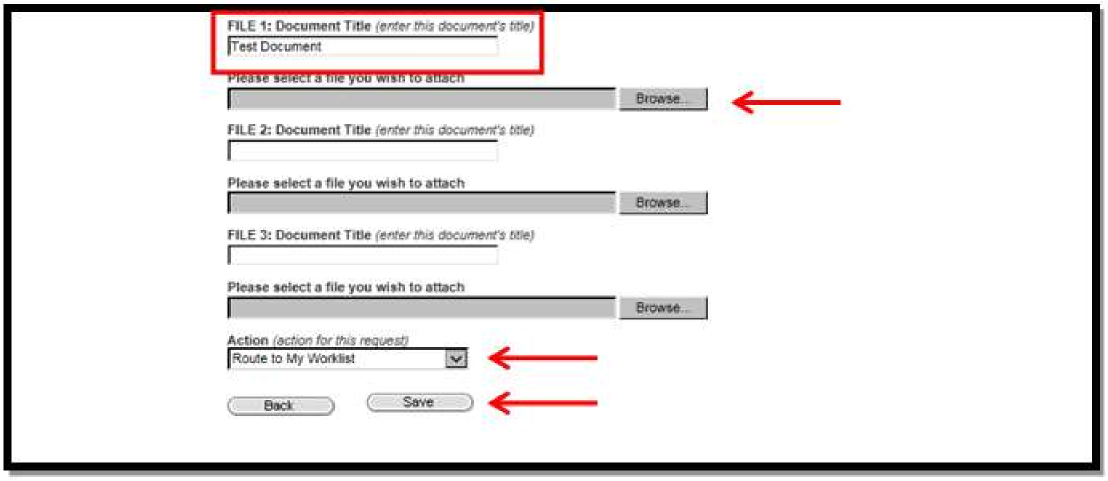


5. Select patient from the Search Results screen.



6. Follow the same steps for entering information in the disclosure details. Refer to Section 5.3.1, starting at Step 6, for a Single Accountable Disclosure or 5.3.2, starting at Step 6, for Multiple Accountable Disclosures.

7. At the bottom of the form, Select Route to Privacy Specialist from the Action drop-down.



8. Click on the Save button.

- The Request Summary screen will display.

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.

TERM	*DEFINITION*
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.
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.

TERM	***DEFINITION***
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	Documentation 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.
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.

TERM	***DEFINITION***
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	A gray 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.
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.

TERM	*DEFINITION*
TCL	The table where the MDR data is stored.
TMA	TRICARE Management Activity.
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
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
PHIMT USER ADMIN PERMISSIONS	
PHIMT User Admin Tab	**Enabled Permissions**

Logon/Logoff	Both
User Tab	Switch to other organizations Update address User profile User workflow User worklist Workflow request
Admin Tab	All users list Attach file Organization management User management
Patient Tab	None (can perform patient profile and patient relationship activities.)
Requests Tab	None (perform new request: route to my worklist activity.)
Requester Tab	None
PHIMT REGULAR USER PERMISSIONS	
PHIMT Regular User Tab	**Enabled Permissions**
Logon/Logoff	Both
Patient Tab	Create patient Generate form Generate letter Patient authorization Patient profile Patient search Patient summary Patient workflow View disclosure
User Tab	Change password Switch to other organizations Update address User profile User workflow User worklist Workflow activity Workflow request Workflows tab
Admin Tab	None (can attach file as part of another activity)