



Defense Health Agency

**Protected Health Information Management Tool
(PHIMT)**

**Training Reference: User Guide
Version 5.0**

December 2016

*This document contains proprietary information and will be handled within Government regulations.
It is intended solely for the use and information of the Military Health System.*

Last Edited: 12/12/2016

Protected Health Information Management Tool
User Manual

TABLE OF CONTENTS

<u>1.0 INTRODUCTION TO PHIMT</u>	4
1.1 <u>PHIMT User Permissions</u>	5
1.2 <u>PHIMT User Roles</u>	5
1.2.1 <u>Privacy Specialist</u>	6
1.2.2 <u>Regular User</u>	6
1.2.3 <u>User Admin</u>	7
1.3 <u>PHIMT SYSTEM REQUIREMENTS</u>	7
1.3.1 <u>Browser Requirements</u>	7
1.3.2 <u>Plug-Ins</u>	7
<u>2.0 ACCESSING AND USING PHIMT</u>	7
<u>3.0 UNDERSTANDING PHIMT SCREENS</u>	10
3.1 <u>SCREEN FEATURES</u>	10
3.1.1 <u>Date</u>	10
3.1.2 <u>Navigational Options</u>	10
3.1.3 <u>Status Box</u>	11
3.1.4 <u>Activity Hyperlinks</u>	11
3.1.5 <u>PHIMT Screen Tabs</u>	12
3.1.6 <u>Screen Title</u>	12
3.1.7 <u>Display Screen/Application Window</u>	13
3.2 <u>PHIMT ERROR MESSAGES</u>	14
<u>4.0 MHS DATA REPOSITORY</u>	14
4.1 <u>ACCESSING PATIENT ACCOUNTS</u>	14
4.2 <u>DUPLICATE ACCOUNTS</u>	15
4.3 <u>PATIENT PROFILE</u>	15
<u>5.0 PRIVACY SPECIALIST FUNCTIONALITY</u>	16
5.1 <u>USER TAB ACTIVITIES</u>	16
5.1.2 <u>My Profile</u>	16
5.1.3 <u>My Requests</u>	18
5.1.4 <u>My Worklist</u>	18
5.1.5 <u>Switch Organization</u>	19
5.2 <u>PATIENT TAB ACTIVITIES</u>	20
5.2.1 <u>Patient Search</u>	20
5.2.2 <u>Create a Patient</u>	22
5.2.3 <u>Create an Alternative Phone Number</u>	24
5.3 <u>PRIVACY SPECIALIST ACTIVITIES</u>	25
5.3.1 <u>Record a Single Accountable Disclosure</u>	25
5.3.2 <u>Record a Mutliple Accountable Disclosure</u>	30
5.3.3 <u>Approve Disclosures</u>	33
5.3.4 <u>Amend a Disclosure</u>	34
5.3.5 <u>Record a Request for an Accounting of Disclosures</u>	36
5.3.6 <u>Approve Accounting of Disclosures Request</u>	40
5.3.7 <u>Generate an Accounting of Disclosures Report</u>	41
5.3.8 <u>Create a Suspension</u>	43
5.3.9 <u>Record Complaints</u>	46

Protected Health Information Management Tool
User Manual

5.3.10 Record a Disclosure Restriction	55
5.3.11 Generate Authorizations	58
5.3.12 Sign an Authorization	62
5.3.13 Revoke an Authorization	64
5.3.14 Administrative Summary Reports	65
5.4 REGULAR USER ACTIVITIES	67
5.4.1 Regular User Access to Record a Disclosure	67
6.0 GLOSSARY	69
7.0 USER ROLE PERMISSIONS	73

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

Protected Health Information Management Tool User Manual

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

Protected Health Information Management Tool User Manual

- **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

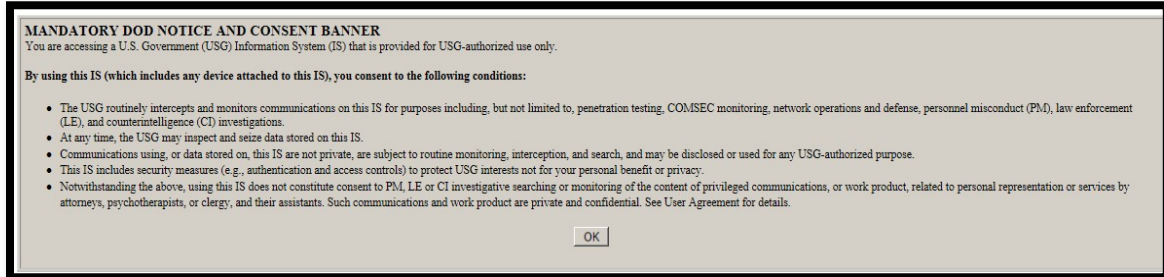
Now that you have an understanding of why PHIMT was developed, are familiar with its capabilities and system requirements, and understand your role, you are ready to access the application.

To login to the PHIMT application:

Protected Health Information Management Tool User Manual

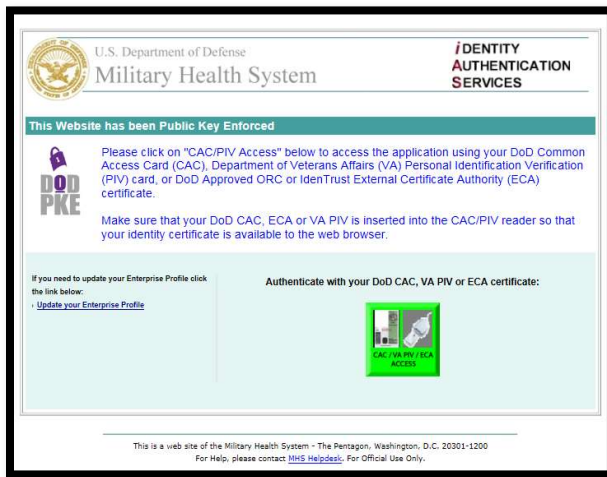
1. Enter the URL for PHIMT into the address bar in your Web browser:
<https://tma-phimt.csd.disa.mil/hipaax>

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.

Protected Health Information Management Tool
User Manual



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

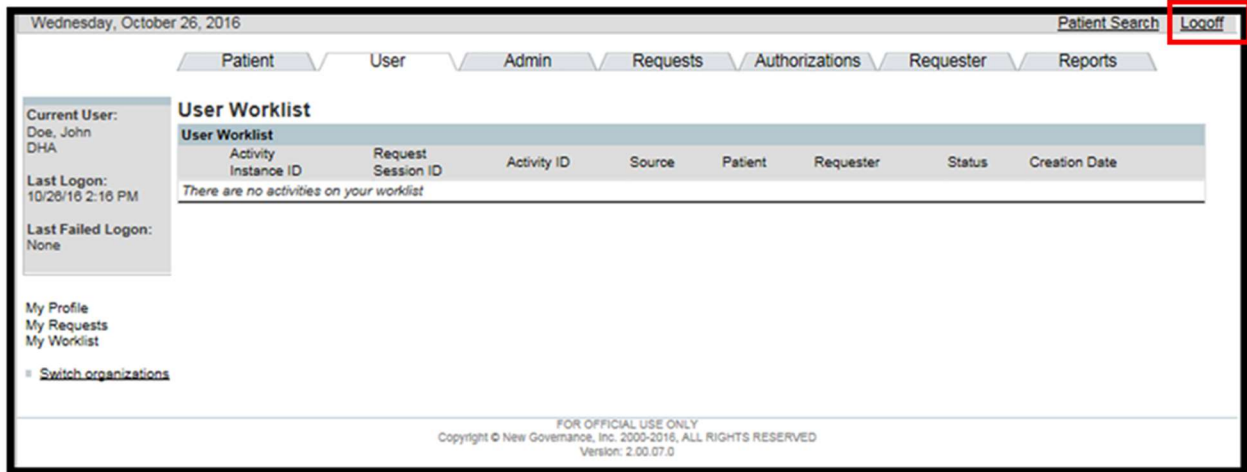
The date feature displays the current weekday, month, day, and year in the upper left corner of the PHIMT screen.



3.1.2 Navigational Options

Protected Health Information Management Tool User Manual

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.

Protected Health Information Management Tool User Manual



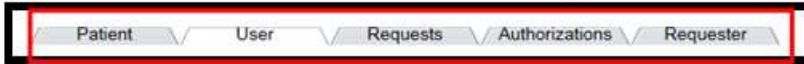
3.1.5 PHIMT Screen Tabs

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).

Protected Health Information Management Tool User Manual



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.

<u>Test, Tonya</u>	new	224414478	224664223	1973-09-15	P.O. Box 42 Howardsville, VA 24562-0042
		EDIPN:1046194728			
<u>Test, Vanessa</u>		121489	538394984	1998-04-16	125 Granby Pl Portland, TX 78374-1407
		EDIPN:1086820702			
<u>Test, Virginia</u>		62141	177308169	1939-12-27	12475 Highgate Ln Gloucester, VA 23061-2649
		EDIPN:1034250320			
<u>Test, Weekend</u>		62139	266090002	1965-10-01	Undefined
		EDIPN:1268571627			
<u>Test, William</u>		121488	318743051	318743051	1982-07-01 527 I Ave Sheppard Afb, TX 78311-2502
		EDIPN:1264557700			

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.

Protected Health Information Management Tool User Manual

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.”

The screenshot shows the 'Patient Search Results' page. The current patient is 'Test, Rebecca' with birth date '03/13/1984' and EDIPN '1385132766'. A table of search results is displayed with the following data:

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

Below the table, the EDIPN '1385132766' is displayed. Other options include 'Adjust your search criteria and try again' and 'Create a new Patient record'.

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.

The screenshot shows the 'Patient Search Results' page with an error message: 'Error(s) have occurred: At least one record already exists that appears to be the same person'. Two tables are displayed, both with the following data:

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

The second table is titled 'Create a new Record' and shows the ID as 'new'.

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.

Protected Health Information Management Tool User Manual

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

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

Patient Profile \ Person Details

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

* Type
Patient

EDIPI (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)
316 - 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: john@yahoo.com)

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

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

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)

Protected Health Information Management Tool User Manual

- 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.

Protected Health Information Management Tool User Manual

Wednesday, October 26, 2016 Patient Search Logoff

Patient User Admin Requests Authorizations Requester Reports

Current User: **User Profile**
Doe, John
DHA

Last Logon: 10/25/16 3:30 PM

Last Failed Logon: None

My Profile
My Requests
My Worklist

Switch organizations

* Name (Last) (First) (Middle) (Sr./Jr.)
Doe John

Phone Number (area code, phone number(XXX-XXXX), and extension if applicable)
(Please note, this phone number will be displayed on letters as contact information.)
ext.

System ID (the identifier created by this system for the person)
1840

* User EDIPN (user asso login id)

Email (example: johnf@yahoo.com)

Email Notification (check to provide email notifications when tasks are added to your WorkQueue)

Signature Block (Please note, this text will display in a letter's signature block.)

Comments (general comments about or for the user)

User Roles
Organization: DHA
Regular User User Admin Privacy Specialist Primary

Update

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.

Protected Health Information Management Tool User Manual



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.

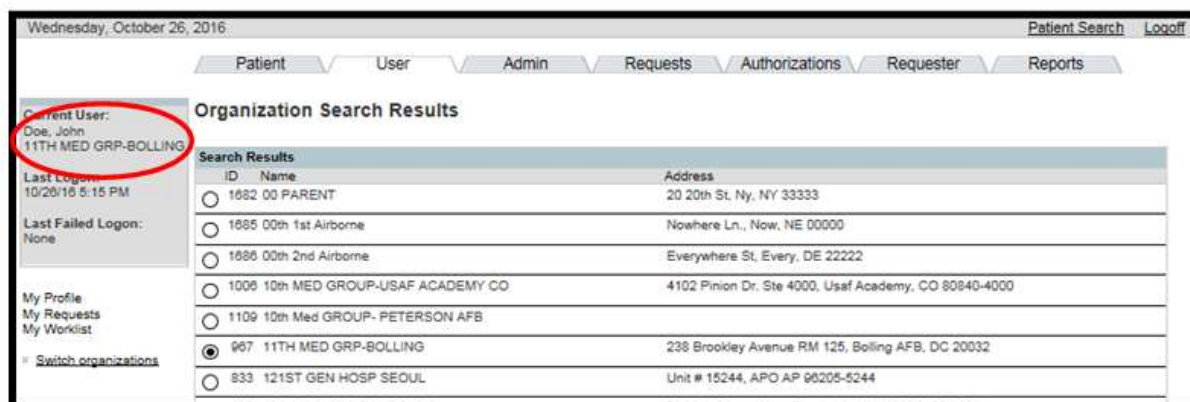
Steps to switch your organization:

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.

Protected Health Information Management Tool User Manual



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.

Protected Health Information Management Tool User Manual

Wednesday, October 26, 2016 Patient Search Logoff

Patient User Admin Requests Authorizations Requester Reports

Current Patient: None

Patient Search

by Name/State (Last) (First)

(State) (Birth Date in MM/DD/YYYY format)

- OR -

SSN (in ###-##-#### format, enter '000-00-0000' if not known)

- OR -

EDIPN (DoD EDI Person Identifier)

- OR -

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

Search

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.

Wednesday, October 26, 2016 Patient Search Logoff

Patient User Admin Requests Authorizations Requester Reports

Current Patient: None

Patient Search Results

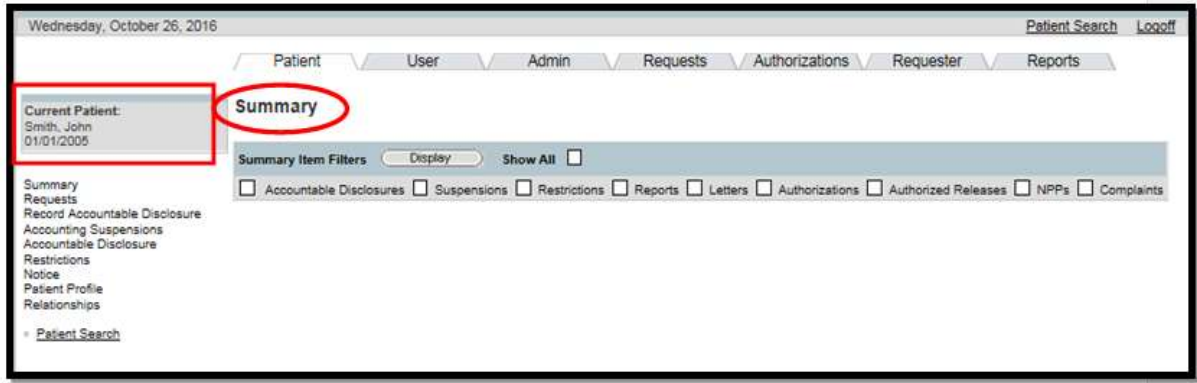
Search Results - Click on the name to select a person

Name	ID	EDIPN	Birth Date	Address
Smith, John 2	748		02/28/1940	34800 Suite 4 San Diego, CA 92134-9999
Smith, John Patient JR	1877		01/01/1991	8270 Willow Oaks Corporate Dr Suite 110 Fairfax, VA 22031
Smith, John	749		01/01/2005	13450 Bob Wilson San Diego, CA 92134
Smith, John	253		10/28/1958	123 Missing Pl. Dr. Toonstown, FL 22222

Other options:
[Adjust your search criteria and try again.](#)
[Create a new Patient record](#)

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

Protected Health Information Management Tool User Manual

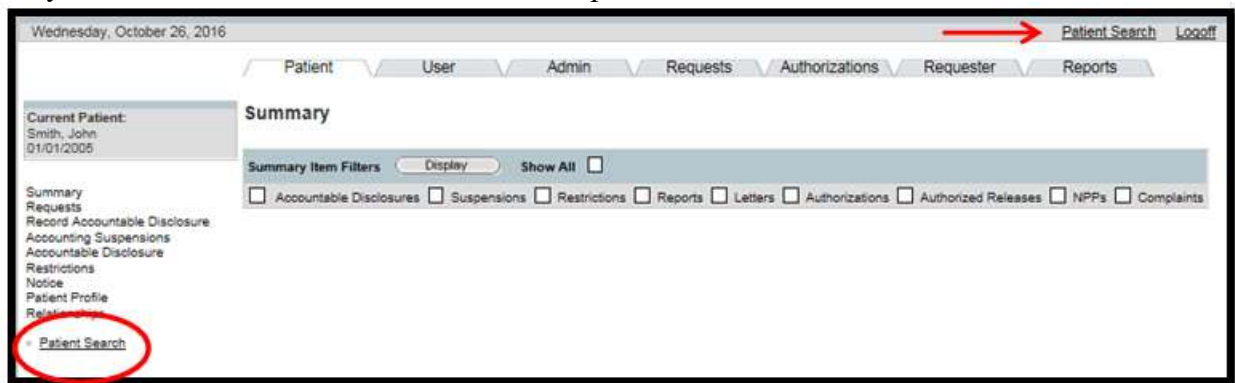


5.2.2 Create a Patient

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.*

Protected Health Information Management Tool User Manual

Wednesday, October 26, 2016 Patient Search Logoff

Patient User Admin Requests Authorizations Requester Reports

Current Patient:
Smith, John
01/01/2005

Summary
Requests
Record Accountable Disclosure
Accounting Suspensions
Accountable Disclosure
Restrictions
Notice
Patient Profile
Relationships

• Patient Search

Patient Search

Use the current person:
Name: John Smith
Birth Date: 01-01-2005
Address: 13450, Bob Wilson, San Diego, CA 92134

- OR -

Search for another person:

by Name/State (Last) (First)
(State) (Birth Date in MM/DD/YYYY format)

- OR -

SSN (in ###-##-#### format; enter '000-00-0000' if not known)

- OR -

EDIPN (DoD EDI Person Identifier)

- OR -

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

Search

4. Click on the Search button.
5. If no results matched your search, select the “Create a New Patient Record” hyperlink.

Wednesday, October 26, 2016 Patient Search Logoff

Patient User Admin Requests Authorizations Requester Reports

Current Patient:
Smith, John
01/01/2005

Summary
Requests
Record Accountable Disclosure
Accounting Suspensions
Accountable Disclosure
Restrictions
Notice
Patient Profile
Relationships

• Patient Search

Patient Search Results

Search Results - Click on the name to select a person

Name	ID	EDIPN	Birth Date	Address
There were no results that matched your search criteria.				

Other options:
[Create a new Patient record](#)

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

Wednesday, October 26, 2016 Patient Search Logoff

Patient User Admin Requests Authorizations Requester Reports

Current Patient:
Smith, John
01/01/2005

Summary
Requests
Record Accountable Disclosure
Accounting Suspensions
Accountable Disclosure
Restrictions
Notice
Patient Profile
Relationships

• Patient Search

PERSON DETAILS

* Name (Last) (First) (Middle) (Sr./Jr.)

* Type
Patient

EDIPN (DoD EDI Person Identifier)

* SSN (in ###-##-#### format; enter '000-00-0000' if not known)

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

* Birth Date (birth date in MM/DD/YYYY format)

Email (example: john@yahoo.com)

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

Comments (general comments about or for the person)

Save

Protected Health Information Management Tool User Manual

7. Click on the Save button.

NOTE: All required fields are marked with an asterisk.

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

9. Click on the Save button.

The image contains two side-by-side screenshots of the 'Address Details' form. Both screenshots show the 'Current Patient' as 'Smith, John' with a birth date of '01/01/2005'. The left screenshot shows the 'Address Format' set to 'USA' (selected with a radio button) and the 'International' option unselected. The right screenshot shows the 'Address Format' set to 'International' (selected with a radio button) and the 'USA' option unselected. In both screenshots, a red box highlights the selected radio button, and a red arrow points to the 'Save' button at the bottom of the form.

- 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.

The image is a screenshot of the 'Patient Summary' screen. The 'Current Patient' information is 'Dirt, Joe' with a birth date of '01/01/2000'. The 'Summary' tab is selected and circled in red. Below the patient information, there is a 'Summary Item Filters' section with a 'Display' button and a 'Show All' checkbox. A list of summary items is shown with checkboxes: 'Accountable Disclosures', 'Suspensions', 'Restrictions', 'Reports', 'Letters', 'Authorizations', 'Authorized Releases', 'NPPs', and 'Complaints'. The 'Patient Search' and 'Logoff' links are visible in the top right corner.

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.

Protected Health Information Management Tool User Manual

- Click on the New button next to Phone Numbers.

The screenshot shows the 'Associated Addresses' table with one entry: ID 3078, Street 123 Dirty St., City Cleantown, State AK, Zip 11111, Alternate No, Primary (selected). Below it is the 'Phone Numbers' section with a 'New' button. A red arrow points to this button. The text below the table reads: 'There are currently no phone numbers on record for this person. Click new to add one.'

- The Phone Number Details screen will display (choose the USA or International format).
- Enter the phone number and enter any comments.
 - Click on the Save button.

The left screenshot shows the 'Phone Number Details' form with 'USA' selected. The phone number field contains '(111) 222-3333'. The right screenshot shows the 'International' radio button selected. The phone number field contains '01-633-999-0000'. Both screenshots have a red arrow pointing to the 'Save' button.

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

The screenshot shows the 'Associated Addresses' table with one entry: ID 3078, Street 123 Dirty St., City Cleantown, State AK, Zip 11111, Alternate No, Primary (selected). Below it is the 'Phone Numbers' section with a 'New' button and one entry: ID 1673, Phone (111) 222-3333, Active Yes, Primary (selected).

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.

Protected Health Information Management Tool User Manual

Steps to record a Disclosure:

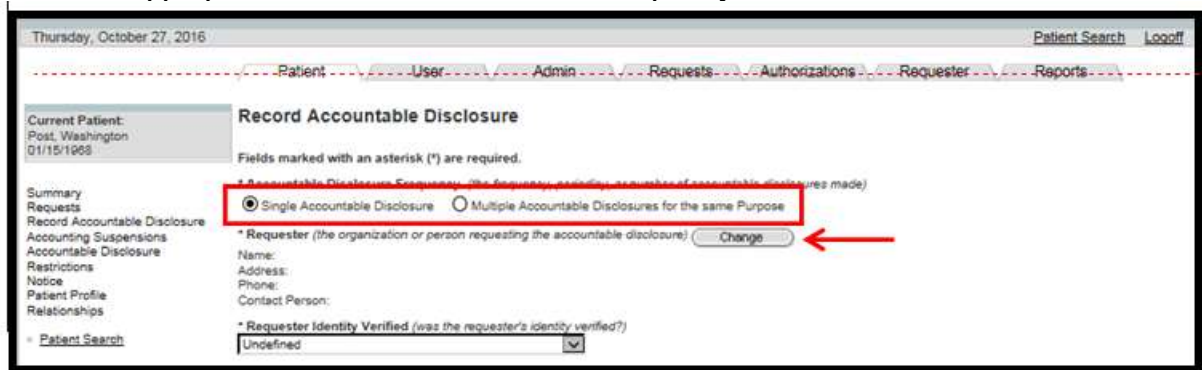
1. Select the Patient Tab.
2. Enter the patient search criteria. (You can search for a patient by the Sponsor's SSN, by the patient's name/state, SSN, EDIPN or System ID).
3. Click on the Search button.
4. Select the patient from the Patient Search Results screen by clicking the Name hyperlink.

NOTE: 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

Protected Health Information Management Tool User Manual

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.

Thursday, October 27, 2016 Patient Search Logoff

Patient User Admin Requests Authorizations Requester Reports

Requester/Recipient Search
Choose one of the following options:

A. Keep the Current
Name: Law Offices of Joe Gibbs
Address: 1411 Jefferson Davis, Arlington, VA 20220 OK

B. Select the Patient (the Patient themselves)
Post, Washington Select

C. Select a Third-Party Organization (a third-party, such as a law enforcement agency or insurance company)
Law Offices of Joe Gibbs, 1411 Jefferson Davis, Arlington, VA 20220 Select

D. Search for a Person (search for another person, or add a new one*)
Name (Last) (First) An "*" may be used as a wildcard
System ID (the identification number created by this system for the person)
EDIPI (an external identifier for the person)
 Include Patient Records
 Include Non-Patient Records
Search

E. Search for an Organization (search for another organization, or add a new one*)
Name (All or part of the name of the organization. An "*" may be used as a wildcard)
DMIS Code (the external identifier for the organization)
Search

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

Protected Health Information Management Tool User Manual

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

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

* Request Date (the accountable disclosure request date in MMDD/YYYY format)
10/27/2016

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

* Accountable Disclosure Type (the type of accountable disclosure)
Not Selected

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

Request Status (the status of the accountable disclosure)
Pending

Disclosure Date (the accountable disclosure date in MMDD/YYYY format)

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

* Accountable Disclosure Date (the accountable disclosure date in MMDD/YYYY format)
10/27/2016

* Origin Organization (where the accountable disclosure originated)
DHA

* Accountable Disclosure Purpose (the purpose of the accountable disclosure)
Undefined
Other/Details (*Required for all Multiple Accountable Disclosures):

* Protected Health Information Description (the description of the Protected Health Information disclosed)
 Complete Health Record(s)
 Operative Report(s)
 History and Physical Examination
 Progress Notes
 Discharge Summary
 Consultation Report(s)
 Pathology Report(s)
 Laboratory Test(s)
Other:
None

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.

Protected Health Information Management Tool User Manual

Other:
None

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

Improper Accountable Disclosure (checked if this accountable disclosure occurred improperly)

Improper Accountable Disclosure Description (the details about the improper accountable disclosure, max 1000 characters)

Improper Accountable Disclosure Mitigation (the details about how the improper accountable disclosure was mitigated, max 1000 characters)

Save

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

Thursday, October 27, 2016 Patient Search Logoff

Patient User Admin Requests Authorizations Requester Reports

Current Patient: Post, Washington 01/15/1968

Record Accountable Disclosure

This accountable disclosure (ID #1825) was created on 10/27/2016 at 02:38:49 PM EDT, and last updated on 10/27/2016 at 02:38:49 PM EDT. Fields marked with an asterisk (*) are required.

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

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

Name: Test, Ahebao
Address: Oweah19032, Hesperia, CA 92345-4001
Phone: (232) 232-3232 x233
Contact Person:

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

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.

Monday, November 14, 2016

Patient | User | Admin | Requests | Authorizations | Requester | Reports

Current Request: Simple Accountable Disclosure Request

Select Patient | Accountable Disclosure Details

Accountable Disclosure Details

Fields marked with an asterisk (*) are required.

* Patient (the Patient to whom the accountable disclosure applies)
Name: Washington Post
Birth Date: 01/15/1968
Address: 1600 Penn Ave Washington, DC 20011

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

Occurs once: PER or times from to

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

Name:
Address:
Phone:
Contact Person:

Protected Health Information Management Tool User Manual

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.

Monday, November 14, 2016

Patient Search Logout

Patient User Admin Requests Authorizations Requester Reports

Current Request: Simple Accountable Disclosure Request

Select Patient Accountable Disclosure Details

1 2

Create New Request Search for a Request

Requester/Recipient Search

Choose one of the following options:

A. Select the Patient (the Patient themselves)
Post, Washington Select

B. Select a Third-Party Organization (a third-party, such as a law enforcement agency or insurance company)
Law Offices of Joe Gibbs, 1411 Jefferson Davis, Arlington, VA 22202 Select

C. Search for a Person (search for another person, or add a new one*)
Name (Last) (First An * may be used as a wildcard)
System ID (the identification number created by this system for the person)
EDIPN (an external identifier for the person)
Include Patient Records
Include Non-Patient Records
Search

D. Search for an Organization (search for another organization, or add a new one*)
Name (All or part of the name of the organization. An * may be used as a wildcard.)
OMS Code (the external identifier for the organization)
Search

* You must search for an existing Person or Organization before adding a new one.

11. Select the Requester from the Search Results screen.

Monday, November 14, 2016

Patient Search Logout

Patient User Admin Requests Authorizations Requester Reports

Current Request: Simple Accountable Disclosure Request

Select Patient Accountable Disclosure Details

1 2

Create New Request Search for a Request

Requester Search Results

Search Results - Click on the name to select a requester

Name	ID	Address
Smith, John 2	748	34300, Suite 4, San Diego, CA 92134-9999
Smith, John	1877	8273 Willow Oaks Corporate Dr, Suite 110, Fairfax, VA 22031
Smith, John	749	13450, Bob Wilson, San Diego, CA 92134
Smith, John	253	123 Measing Pl. Dr., Toonstown, FL 22222

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

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.

Protected Health Information Management Tool User Manual

* Requester (the organization or person requesting the accountable disclosure) Change
Name: Smith, John
Address: 13450, Bob Wilson, San Diego, CA 92134
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 accountable disclosure request date in MM/DD/YYYY format)
11/14/2016 📅

* Recipient (the organization or person where the accountable disclosure went) Change
Name: Smith, John
Address: 13450, Bob Wilson, San Diego, CA 92134
Phone:
Contact Person:

* Accountable Disclosure Type (the type of accountable disclosure)
Health Oversight Activities ▼ ←

Accountable Disclosure Description (a read-only description and example of the accountable disclosure type selected above)
Health oversight agency for oversight activities authorized by law, including audits, civil, administrative, or criminal investigations, inspections, licensure or disciplinary actions, civil, administrative, or criminal proceedings or actions; or other activities necessary for 1) appropriate oversight of health care systems 2) government benefit programs 3) government regulatory programs and 4) entities subject to civil rights laws for which PHI is necessary for determining compliance

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.)

* Accountable Disclosure Date (the accountable disclosure date in MM/DD/YYYY format)
11/01/2016 📅

* Origin Organization (where the accountable disclosure originated)
DHA ▼

* Accountable Disclosure Purpose (the purpose of the accountable disclosure)
Medical ▼

Other/Details (*Required for all Multiple Accountable Disclosures):
To determine member's fitness to perform any particular mission, including compliance with any action required as a precondition to perform such mission.

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

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

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.

Protected Health Information Management Tool User Manual

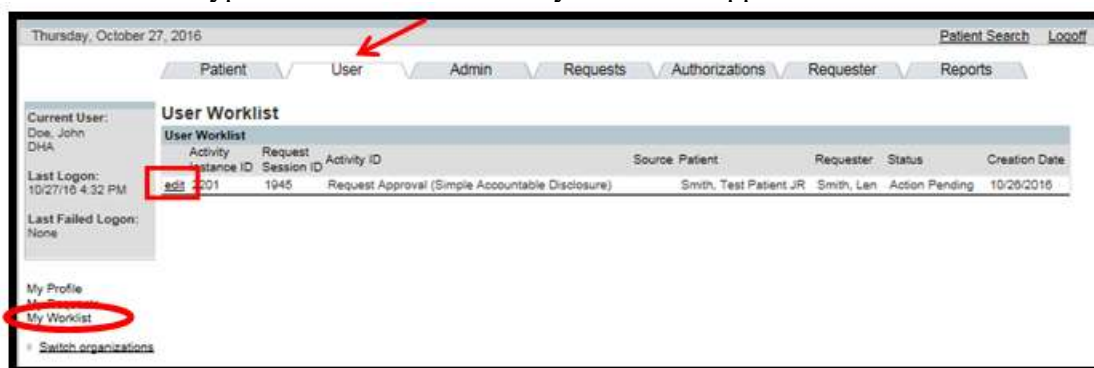
The screenshot shows a form for uploading documents. It contains three sections for file uploads, each with a text input for the document title and a 'Browse...' button. Below these is an 'Action' dropdown menu set to 'Route to My Worklist', and 'Back' and 'Save' buttons. Red arrows point to the 'Browse...' buttons, the 'Action' dropdown, and the 'Save' button. A red box highlights the first document title input field.

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.

Protected Health Information Management Tool User Manual

Summary
History
Documents
Accountable Disclosure Details

Create New Request
Search for a Request

Patient
Name: Washington Post
Birth Date: 01-15-1968
Address: 1600 Penn Ave, Washington, DC 20011

Requester/Recipient
Name: Law Offices of Joe Gibbs
Address: 1411 Jefferson Davis, Arlington, VA 20220

Instructions
Request Approval (Simple Accountable Disclosure)

Request Session Details

Description	Details
Request Type	Simple Accountable Disclosure Request
Accountable Disclosure Type	Type: Law Enforcement Purposes, ID: 1827, Date: 10/10/2016
Identity Verified Text	DoD ID Number

Activity Status (new activity status code)
Approved

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

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

Route Completed Request to Originator (route to the request creator for acknowledgement & document preparation)

Comments (enter details about this activity. Limit 1000 characters.)

Update

- 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.

Thursday, October 27, 2016 Patient Search Logoff

Patient User Admin Requests Authorizations Requester Reports

Current Request: Accountable Simple Disclosure Request

Summary
History
Documents
Accountable Disclosure Details

Create New Request
Search for a Request

Edit Request

Request Activity History

Activity Instance ID	Request ID	Activity ID	Source Patient ID	Requester ID	User	Status	Creation Date
1202	1948	Request Approval (Simple Accountable Disclosure)	Post, Washington	Law Offices of Joe Gibbs	John Doe	Approved	10/27/2016

Request Session Details Edit

Description	Details
Request Type	Simple Accountable Disclosure Request
Accountable Disclosure Type	Type: Law Enforcement Purposes, ID: 1827, Date: 10/10/2016
Identity Verified Text	DoD ID Number

Letters and Attached Documents Attach

ID	Date	Title
----	------	-------

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.

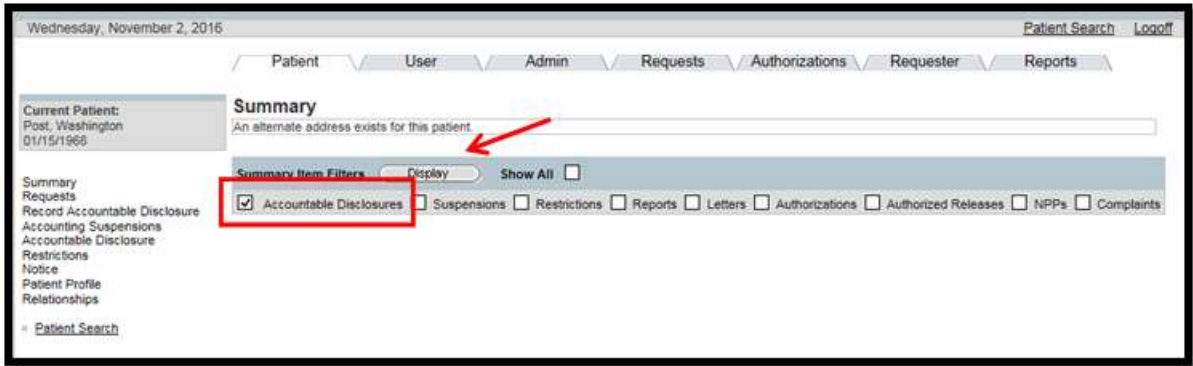
Steps to amend a disclosure:

1. Select the Patient Tab.
2. Search for and select the patient (see 5.2.1).

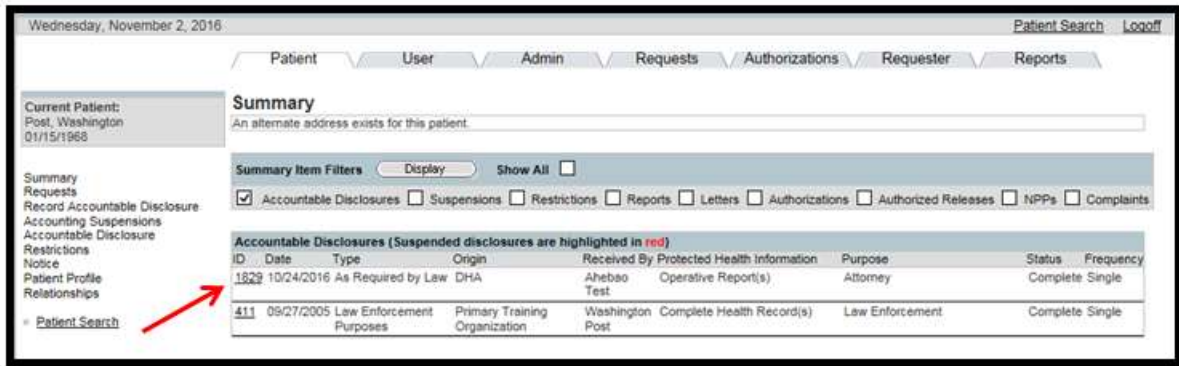
Protected Health Information Management Tool User Manual



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.

Protected Health Information Management Tool User Manual

Wednesday, November 2, 2016 Patient Search Logout

Patient User Admin Requests Authorizations Requester Reports

Current Patient:
Post, Washington
01/15/1968

Record Accountable Disclosure

This accountable disclosure (ID #1829) was created on 11/02/2016 at 08:09:55 AM EDT, and last updated on 11/02/2016 at 08:09:55 AM EDT. Fields marked with an asterisk (*) are required.

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

* Requester (the organization or person requesting the accountable disclosure)
Name: Post, Washington
Address: 1600 Penn Ave, Washington, DC 20011
Phone:
Contact Person:

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

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

* Request Date (the accountable disclosure request date in MM/DD/YYYY format)
11/02/2016

* Recipient (the organization or person where the accountable disclosure went)
Name: Test, Aheba
Address: Oweah16032, Hesperia, CA 92345-4001
Phone: (232) 232-3232 x233
Contact Person:

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.

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

Improper Accountable Disclosure (checked if this accountable disclosure occurred improperly)

Improper Accountable Disclosure Description (the details about the improper accountable disclosure, max 1000 characters)
Wrong address.

Improper Accountable Disclosure Mitigation (the details about how the improper accountable disclosure was mitigated, max 1000 characters)
Privacy Officer spoke with patient.

Update

Associated Documents Attach

ID	Date	Title
----	------	-------

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:

Protected Health Information Management Tool User Manual

1. Select the Requests Tab.
2. Click on the radio button for Accountable Disclosure Accounting.

Wednesday, November 2, 2016 Patient Search Logoff

Patient User Admin Requests Authorizations Requester Reports

Current Request: None

Create New Request

Select Request Type

- Accountable Disclosure
- Accountable Disclosure Accounting
- Complaint
- Simple Accountable Disclosure Request

Next

Annotations: A red circle highlights the 'Create New Request' link. A red box highlights the 'Accountable Disclosure Accounting' radio button. A red arrow points to the 'Next' button. Another red arrow points to the 'Requests' tab in the navigation menu.

3. Click on the Next button.
4. Search for the patient.

Wednesday, November 2, 2016 Patient Search Logoff

Patient User Admin Requests Authorizations Requester Reports

Current Request: Accountable Disclosure Accounting

Select Patient Select Requester Request Details Request Action

1 2 3 4

Patient Search

by Name/State (Last) (First)

(State) (Birth Date in MM/DD/YYYY format)

- OR -

SSN (in ###-##-#### format, enter '000-00-0000' if not known)

- OR -

EDIPN (DoD EDI Person Identifier)

- OR -

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

Search

Annotation: A red box highlights the search criteria fields. A red arrow points to the 'Search' button.

5. Select the Patient.

Wednesday, November 2, 2016 Patient Search Logoff

Patient User Admin Requests Authorizations Requester Reports

Current Request: Accountable Disclosure Accounting

Select Patient Select Requester Request Details Request Action

1 2 3 4

Patient Search Results

Search Results - Click on the name to select a person

Name	ID	EDIPN	Birth Date	Address
Post, Washington	1163		01/15/1966	1800 Penn Ave Washington, DC 20011

Other options:
[Adjust your search criteria and try again.](#)
[Create a new Patient record.](#)

Annotation: A red arrow points to the name 'Post, Washington' in the search results table.

Protected Health Information Management Tool User Manual

6. Select the Requester.

Wednesday, November 2, 2016 Patient Search Logout

Patient User Admin Requests Authorizations Requester Reports

Current Request: Accountable Disclosure Accounting

Select Patient Select Requester Request Details Request Action

1 2 3 4

Requester/Recipient Search

Choose one of the following options:

A. Select the Patient (the Patient themselves)

Post, Washington ←

B. Select a Third-Party Organization (a third-party, such as a law enforcement agency or insurance company)

Law Offices of Joe Gibbs, 1411 Jefferson Davis, Arlington, VA 20220

C. Search for a Person (search for another person, or add a new one*)

Name (Last) (First) An * may be used as a wildcard

System ID (the identification number created by this system for the person)

EDIPN (an external identifier for the person)

20-999887766 Include Patient Records Include Non-Patient Records

D. Search for an Organization (search for another organization, or add a new one*)

Name (All or part of the name of the organization. An * may be used as a wildcard)

DMIS Code (the external identifier for the organization)

20-999887766

7. Confirm the requester and recipient details.

8. Click on the Next button.

Wednesday, November 2, 2016 Patient Search Logout

Patient User Admin Requests Authorizations Requester Reports

Current Request: Accountable Disclosure Accounting

Select Patient Select Requester Request Details Request Action

1 2 3 4

Confirm Requester and Recipient Details

Requester: Washington Post change

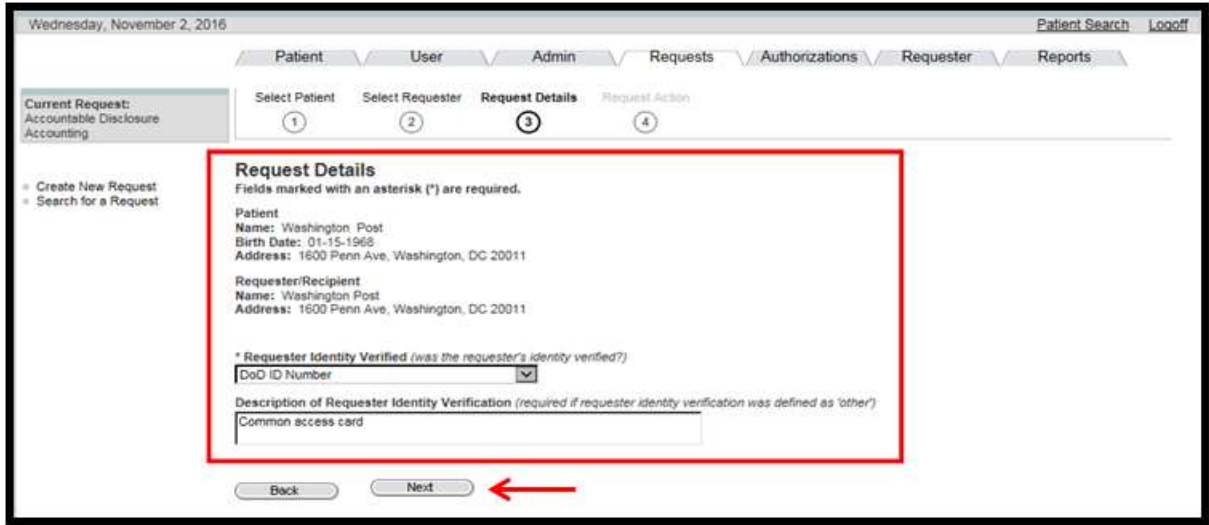
Address: 1600 Penn Ave, Washington, DC 20011

Recipient: Same as requester [set a different recipient](#)

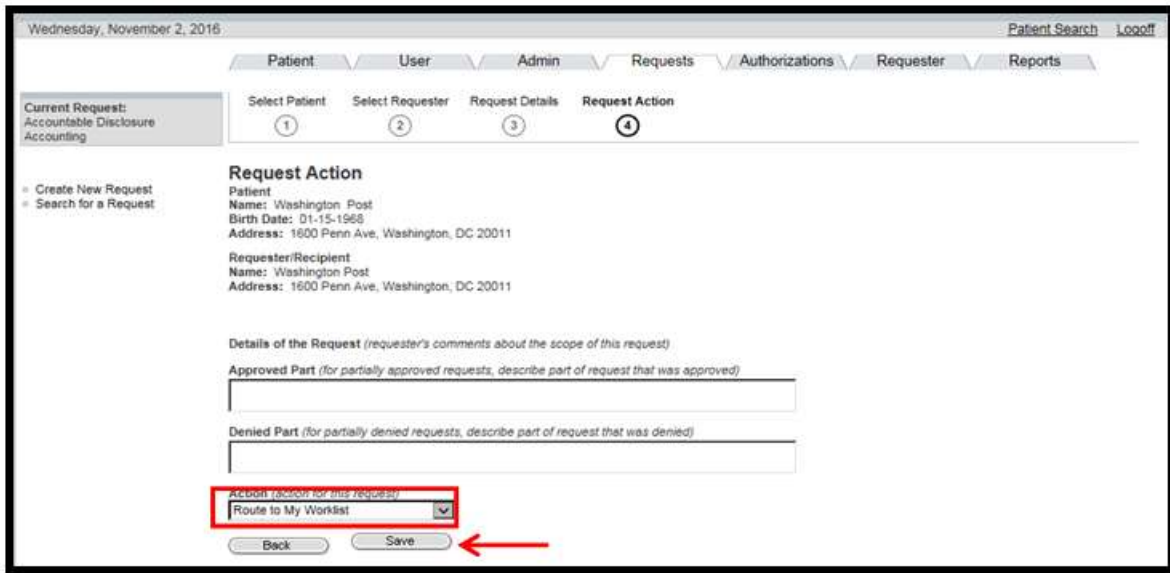
←

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

Protected Health Information Management Tool User Manual



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

Protected Health Information Management Tool
User Manual

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.

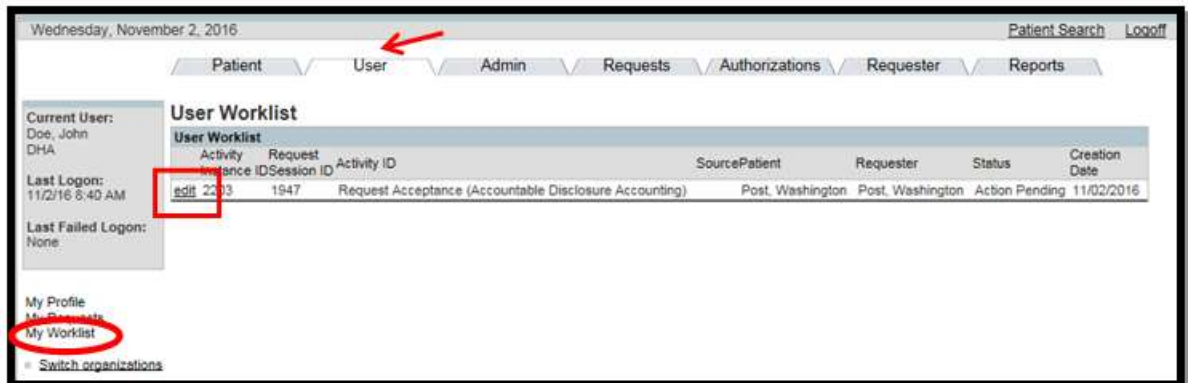


5.3.6 Approve Accounting of Disclosures Request

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.



Protected Health Information Management Tool User Manual

- The Edit Activity Details screen will display.

Wednesday, November 2, 2016

Patient Search Logout

Patient User Admin Requests Authorizations Requester Reports

Current Request: Accountable Disclosure Accounting

Edit Activity Details

Originator
Name: John Doe
Phone:

Patient
Name: Washington Post
Birth Date: 01-15-1983
Address: 1500 Penn Ave, Washington, DC 20011

Requester/Recipient
Name: Washington Post
Address: 1500 Penn Ave, Washington, DC 20011

Instructions
Request Acceptance (Accountable Disclosure Accounting)

Description	Details
Request Type	Accountable Disclosure Accounting
Identity Verified	DoD ID Number
Verify Identity Test	Common access card
Request Classification	Patient

Activity Status (new activity status code)
Action Pending

Approved Part (for partially approved requests; describe part of request that was approved):

Denied Part (for partially approved requests; describe part of request that was denied):

Comments (enter details about this activity. Limit 1000 characters.)

Update

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.*

Wednesday, November 2, 2016

Patient Search Logout

Patient User Admin Requests Authorizations Requester Reports

Current Request: Accountable Disclosure Accounting

Accountable Disclosure Accounting Request

Accountable 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
<input checked="" type="checkbox"/>	1829	10/24/2016	As Required by Law	DHA	Ahebae Test	Operative Report(s)	Attorney	Complete
<input checked="" type="checkbox"/>	411	09/27/2005	Law Enforcement Purposes	Primary Training Organization	Washington Post	Complete Health Record(s)	Law Enforcement	Complete

Accountable Disclosures Accounting Suspensions

Suspension ID	Suspended Disclosure	Identifier	Start Date	End Date	Comments
---------------	----------------------	------------	------------	----------	----------

Create

5.3.7 Generate an Accounting of Disclosures Report

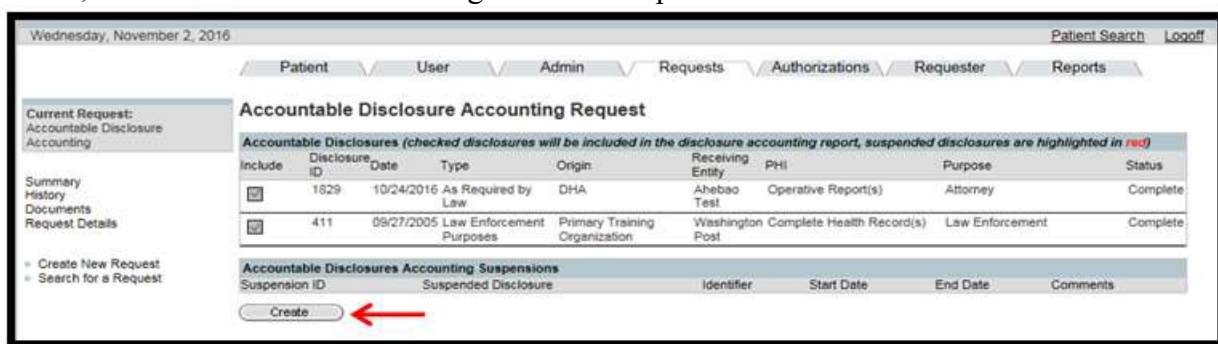
An accounting of disclosures report is a summary of all of the disclosures made for a particular patient. Once a request has been approved, an accounting of disclosures report can be generated. Pending disclosures will not display in the report.

Protected Health Information Management Tool User Manual

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

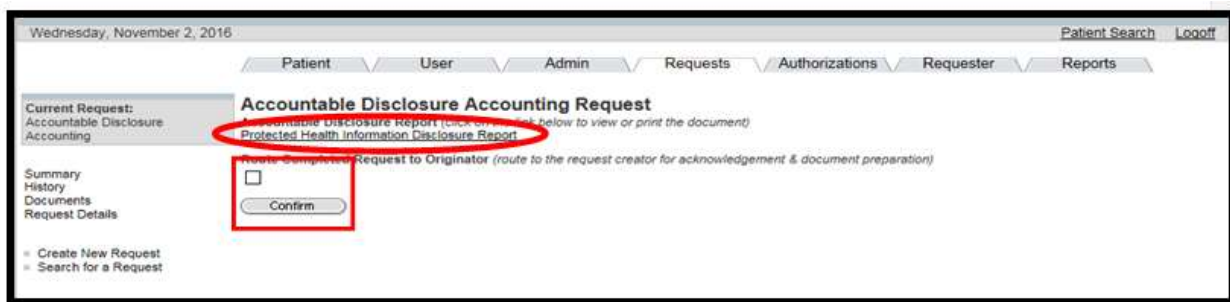
Steps to generate an Accounting of Disclosures Report:

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.

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 in PDF.

Protected Health Information Management Tool User Manual

Protected Health Information Disclosure Report	
Prepared for:	Washington Post
Requested from:	DHA
Generated on:	11-02-2016
<hr/>	
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
<hr/>	
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.

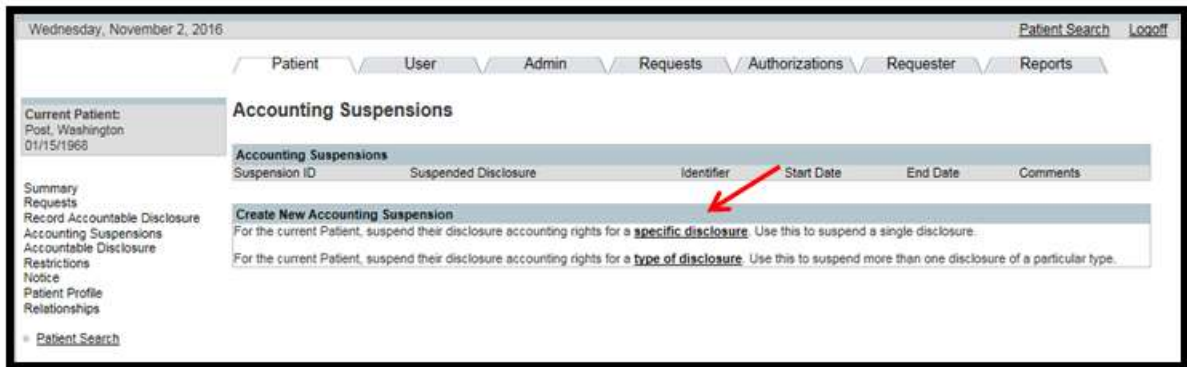
Steps to create a suspension:

1. Search for and select a patient record.
2. Select the Accounting Suspensions hyperlink.

Protected Health Information Management Tool User Manual



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.

Protected Health Information Management Tool User Manual

Wednesday, November 2, 2016 Patient Search Logoff

Patient User Admin Requests Authorizations Requester Reports

Current Patient: Post, Washington 01/15/1968

Accounting Suspension

Patient Accountable Disclosures (Suspended disclosures are highlighted in red)

Suspend	Disclosure ID	Date	Type	Origin	Receiving Entity	PHI	Purpose	Status
<input checked="" type="checkbox"/>	411	05/27/2005	Law Enforcement Purposes	Primary Training Organization	Washington Post	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 Law Office

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 legal counsel

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

11/03/2016

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

12/02/2016

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

Notice Patient Profile Relationships Patient Search

As requested by Law Office

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 legal counsel

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

11/03/2016

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

12/02/2016

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

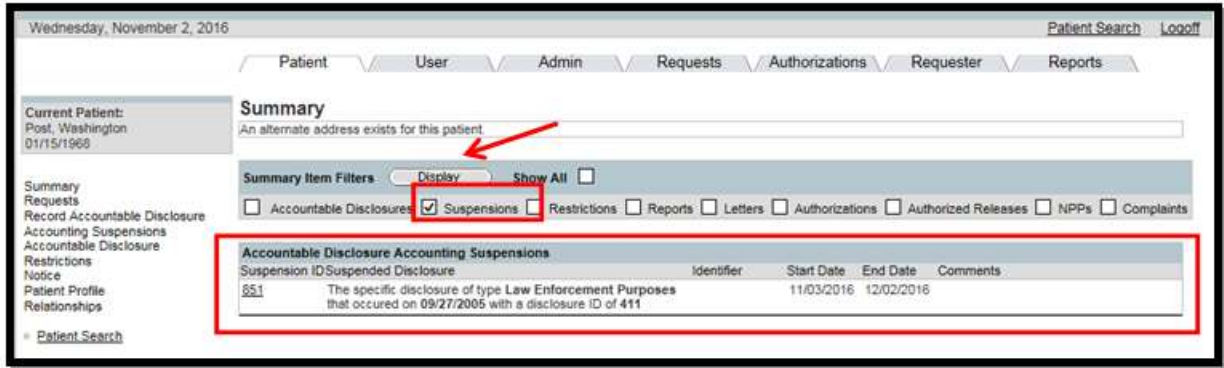
7. Select from the left column the Summary hyperlink.

8. Check the Suspensions checkbox.

9. Click on the Display button.

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

Protected Health Information Management Tool User Manual

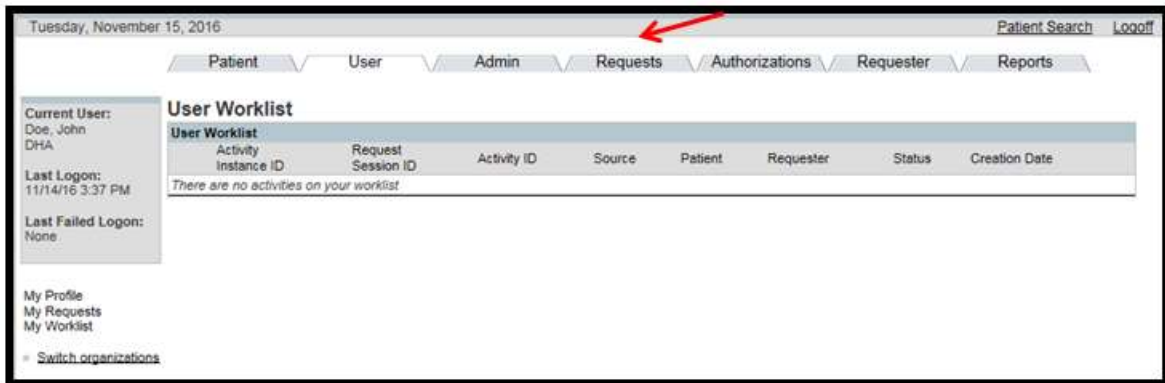


5.3.9 Record Complaints

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:

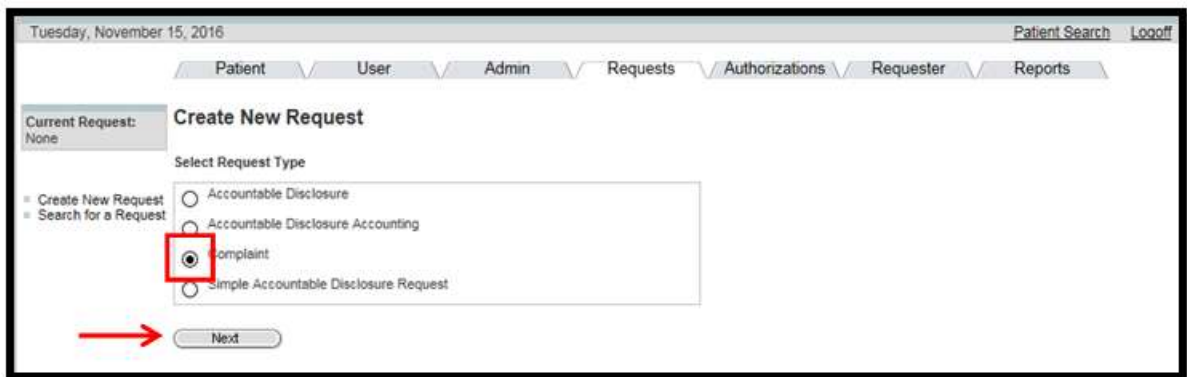
1. Select the Requests Tab.



- The Create New Request Screen will appear.

2. Click the Complaint radio button.

3. Click on the Next button.



Protected Health Information Management Tool User Manual

- The Select Complainant Screen will appear.

Tuesday, November 15, 2016 Patient Search [Logout](#)

Patient User Admin Requests Authorizations Requester Reports

Current Request: Complainant

Select Complainant Complainant Details Documents Request Action

1 2 3 4

Create New Request
Search for a Request

Patient Search

Use the current person:
Name: Washington Post
Birth Date: 01-15-1968
Address: 1600 Penn Ave, Washington, DC 20011

-OR-

Search for another person:
by Name/State (Last) (First)
(State) (Birth Date in MM/DD/YYYY format)

-OR-

SSN (in ###-##-#### format, enter '000-00-0000' if not known)

-OR-

EDIPN (DoD EDI Person Identifier)

-OR-

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

4. Search for the patient.
5. Click on the Search button.
 - The Patient Search Results Screen will appear.
6. Select the Patient.

Tuesday, November 15, 2016 Patient Search [Logout](#)

Patient User Admin Requests Authorizations Requester Reports

Current Request: Complainant

Select Complainant Complainant Details Documents Request Action

1 2 3 4

Create New Request
Search for a Request

Patient Search Results

Search Results - Click on the name to select a person

Name	ID	EDIPN	Birth Date	Address
Post, Washington	1163		01/15/1968	1600 Penn Ave Washington, DC 20011

Other options:
[Adjust your search criteria and try again](#)
[Create a new Patient record](#)

- The Complaint Details Screen will appear.

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

Protected Health Information Management Tool User Manual

Tuesday, November 15, 2016 Patient Search Logoff

Patient User Admin Requests Authorizations Requester Reports

Current Request: Complaint

Select Complainant **Complaint Details** Documents Request Action

1 2 3 4

Create New Request
Search for a Request

Complaint Details

Complainant (the person who is making the complaint)
Name: Washington Post

Complaint Type (the type of complaint to create)
Notice of Privacy Practices Complaint

Complaint Date (the date the complaint was received in MM/DD/YYYY format)
11/15/2016

Subject (the subject of the complaint)
Request for Copy of Medical Record

Complaint Description (the description of the complaint - limited to 1020 characters)
The medical records contained information belonging to another beneficiary. Washington Post is also concerned that his medical information may have been misplaced in another beneficiary's record]

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

Complaint Description (the description of the complaint - limited to 1020 characters)
The medical records contained information belonging to another beneficiary. Washington Post is also concerned that his medical information may have been misplaced in another beneficiary's record.

Outcome Type (the type of outcome after complaint investigation)
Not Selected

Outcome Date (the date of the complaint outcome in MM/DD/YYYY format)
[]

Outcome Description (the description of the complaint outcome - limited to 1020 characters)
[]

Back Next

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.

Protected Health Information Management Tool User Manual

Tuesday, November 15, 2016 Patient Search Logoff

Patient User Admin Requests Authorizations Requester Reports

Current Request: Complainant Complaint Details **Documents** Request Action

1 2 3 4

Create New Request Search for a Request

Documents

You may attach any document, with file size not exceeding 5M

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

Please select a file you wish to attach
C:\Users\rsalvado\Desktop\MTF XX COMPLAINT FORM.docx 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.

Tuesday, November 15, 2016 Patient Search Logoff

Patient User Admin Requests Authorizations Requester Reports

Current Request: Complainant Complaint Details Documents **Request Action**

1 2 3 4

Create New Request Search for a Request

Request Action

Patient
Name: Washington Post
Birth Date: 01-15-1968
Address: 1600 Penn Ave, Washington, DC 20011

Details of the Request (requester's comments about the scope of this request)
The medical records contained information belonging to another beneficiary. Washington Post is also concerned that his medical information may have been misplaced in another beneficiary's record.

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

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

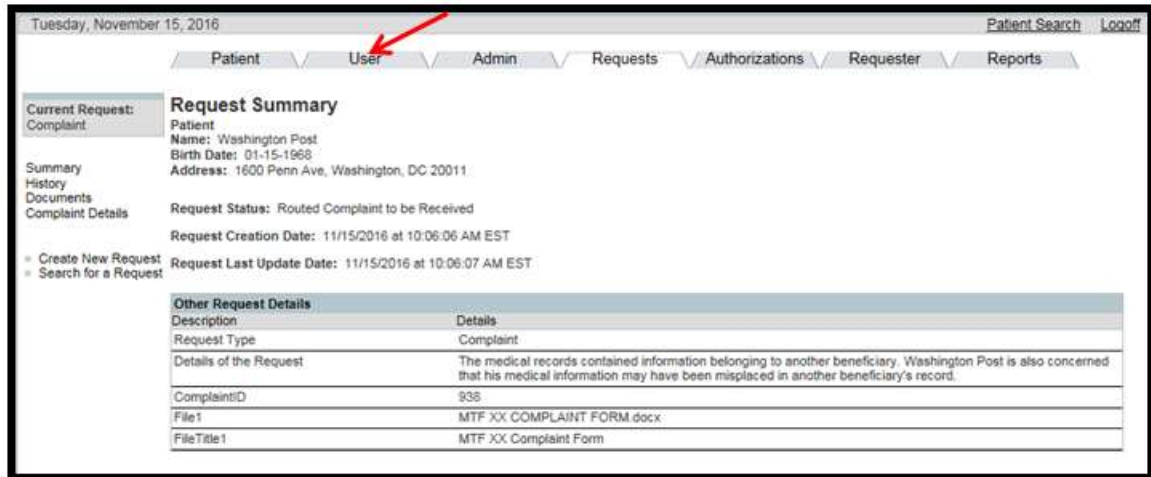
13. Click on the Save button.

- The Request Summary screen will display.

Steps to Receive a Complaint:

1. Select the User Tab.

Protected Health Information Management Tool User Manual



- 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.

Protected Health Information Management Tool User Manual

Tuesday, November 15, 2016 Patient Search Logoff

Patient User Admin Requests Authorizations Requester Reports

Current Request: Complaint
Edit Activity Details

Originator Name: John Doe
Phone:

Summary
History
Documents
Complaint Details

Patient Name: Washington Post
Birth Date: 01-15-1968
Address: 1600 Penn Ave, Washington, DC 20011

Instructions
Complaint to be Received

Request Session Details

Description	Details
Request Type	Complaint
Details of the Request	The medical records contained information belonging to another beneficiary. Washington Post is also concerned that his medical information may have been misplaced in another beneficiary's record.
ComplaintID	936
File1	MTF_XX_COMPLAINT_FORM.docx
FileTitle1	MTF_XX Complaint Form

Activity Status (new activity status code)
Received

Comments (enter details about this activity. Limit 1000 characters.)

Update

Letters and Attached Documents Attach

ID	Date	Title
2620	11/15/2016	MTF_XX Complaint Form

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.

Tuesday, November 15, 2016 Patient Search Logoff

Patient User Admin Requests Authorizations Requester Reports

Current Request: Complaint
Edit Request

Request Activity History

Activity Instance ID	Request Session ID	Activity ID	Source	Patient Id	Requester Id	User	Status	Creation Date
2229	1973	Complaint to be Received	Post, Washington	John Doe	Received	11/15/2016		
2230	1973	Complaint Investigation	Post, Washington	John Doe	Action Pending	11/15/2016		

Request Session Details Edit

Description	Details
Request Type	Complaint
Details of the Request	The medical records contained information belonging to another beneficiary. Washington Post is also concerned that his medical information may have been misplaced in another beneficiary's record.
ComplaintID	936
File1	MTF_XX_COMPLAINT_FORM.docx
FileTitle1	MTF_XX Complaint Form

Letters and Attached Documents Attach

ID	Date	Title
2621	11/15/2016	Complaint - Received Letter
2620	11/15/2016	MTF_XX Complaint Form

- The Complaint Received Letter is generated.

Protected Health Information Management Tool User Manual



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.

Protected Health Information Management Tool User Manual

Monday, December 12, 2016 Patient Search [Logout](#)

Patient User Admin Requests Authorizations Requester Reports

Current Request: **Edit Activity Details**

Complaint:
Originator Name: John Doe
Phone:

Summary
History Patient Name: Washington Post
Documents Birth Date: 01-15-1968
Complaint Details Address: 1600 Penn Ave, Washington, DC 20011

▢ Create New Request
▢ Search for a Request

Instructions
Complaint investigation

Request Session Details	
Description	Details
Request Type	Complaint
Details of the Request	The medical records contained information belonging to another beneficiary. Washington Post is also concerned that his medical information may have been misplaced in another beneficiary's record.
ComplaintID	939
File1	MTF_XX_COMPLAINT_FORM.docx
FileTitle1	MTF_XX Complaint Form

Activity Status (new activity status code)
Completed

Comments (enter details about this activity. Limit 1000 characters.)

Update

Letters and Attached Documents		
ID	Date	Title
2644	12/12/2016	Complaint - Received Letter
2643	12/12/2016	MTF_XX_Complaint_Form

4. Click on the Update button.
 - The Complaint Details Screen will appear.
5. Complete the Complaint Details: outcome type, outcome date and outcome description.

Complaint Description (the description of the complaint - limited to 1020 characters)
The medical records contained information belonging to another beneficiary. Washington Post is also concerned that his medical information may have been misplaced in another beneficiary's record.

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

Outcome Date (the date of the complaint outcome in MM/DD/YYYY format)
12/12/2016

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

Update

6. Click on the Update button.
7. Select Completed from the Activity Status drop-down box.

Protected Health Information Management Tool User Manual

Monday, December 12, 2016 Patient Search [Logout](#)

Patient User Admin Requests Authorizations Requester Reports

Current Request: Complaint

Edit Activity Details

Originator Name: John Doe
Phone:

Patient Name: Washington Post
Birth Date: 01-15-1968
Address: 1600 Penn Ave, Washington, DC 20011

Instructions
Complaint Investigation

Request Session Details

Description	Details
Request Type	Complaint
Details of the Request	The medical records contained information belonging to another beneficiary. Washington Post is also concerned that his medical information may have been misplaced in another beneficiary's record.
ComplaintID	939
File1	MTF XX COMPLAINT FORM.docx
FileTitle1	MTF XX Complaint Form

Activity Status (new activity status code)
Completed

Update

Letters and Attached Documents [Attach](#)

ID	Date	Title
2644	12/12/2016	Complaint - Received Letter
2643	12/12/2016	MTF XX Complaint Form

8. Click on the Update button.
 - The Edit Request Screen will appear.
9. Select the Substantiated Complaint Letter hyperlink.

Monday, December 12, 2016 Patient Search [Logout](#)

Patient User Admin Requests Authorizations Requester Reports

Current Request: Complaint

Edit Request

Request Activity History

Activity Instance ID	Request Session ID	Activity ID	Source	Patient Id	Requester Id	User	Status	Creation Date
2231	1974	Complaint to be Received	Post, Washington			John Doe	Received	12/12/2016
2232	1974	Complaint Investigation	Post, Washington			John Doe	Completed	12/12/2016

Request Session Details [Edit](#)

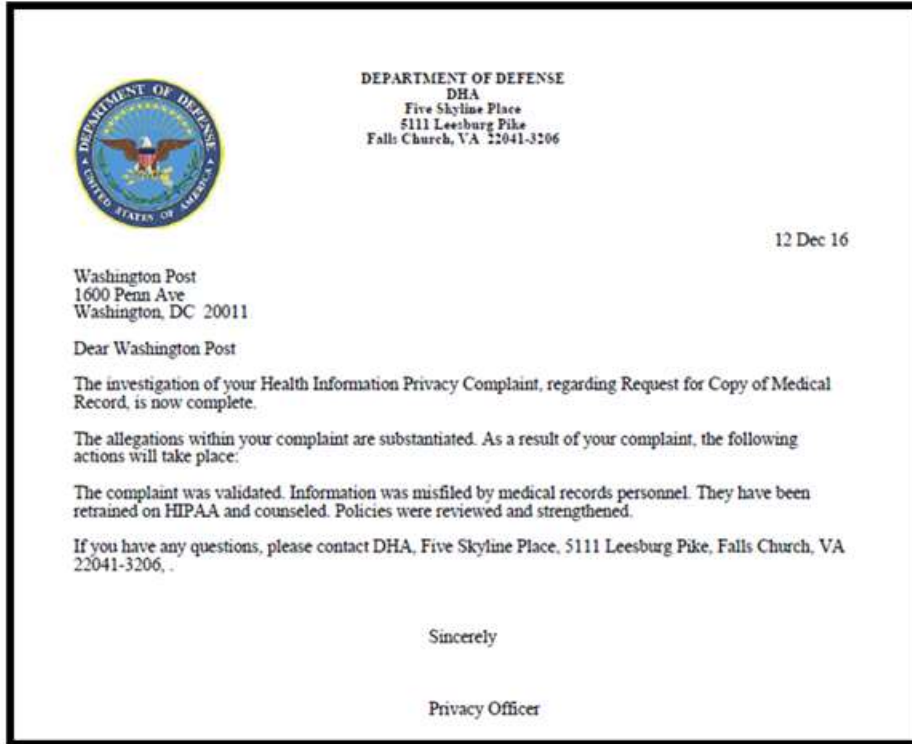
Description	Details
Request Type	Complaint
Details of the Request	The medical records contained information belonging to another beneficiary. Washington Post is also concerned that his medical information may have been misplaced in another beneficiary's record.
ComplaintID	939
File1	MTF XX COMPLAINT FORM.docx
FileTitle1	MTF XX Complaint Form

Letters and Attached Documents [Attach](#)

ID	Date	Title
2645	12/12/2016	Substantiated Complaint Letter
2644	12/12/2016	Complaint - Received Letter
2643	12/12/2016	MTF XX Complaint Form

- The Substantiated Complaint Letter is generated.

Protected Health Information Management Tool User Manual



- 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:

Protected Health Information Management Tool User Manual

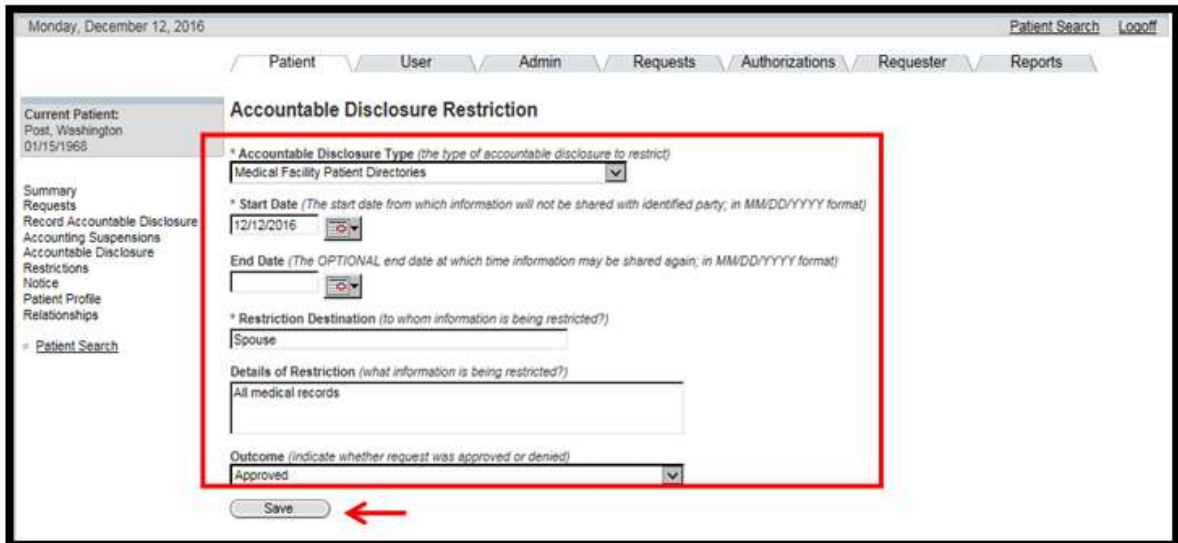
1. From the Patient tab, search for and select a patient record.
2. Select the Accountable Disclosure Restrictions hyperlink.



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.

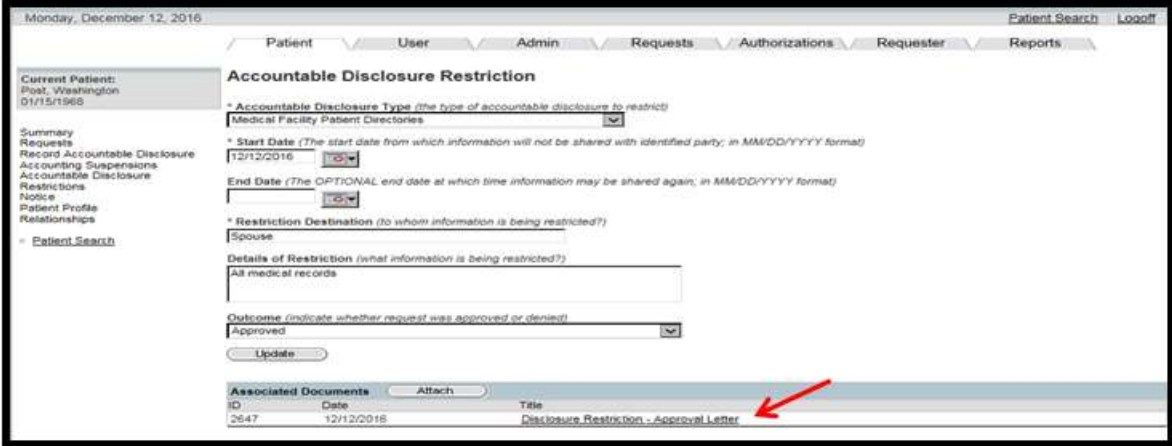
Protected Health Information Management Tool User Manual

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.

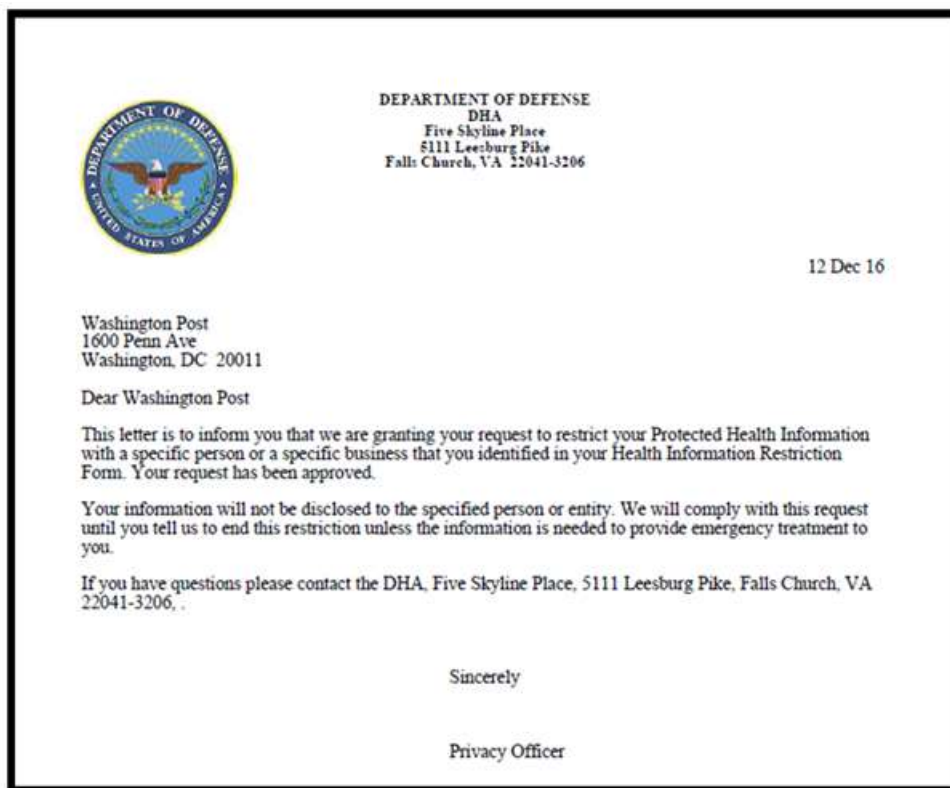


The screenshot shows the 'Accountable Disclosure Restriction' form. The 'Outcome' is set to 'Approved'. Below the form is an 'Associated Documents' table with one entry: ID 2647, Date 12/12/2016, and Title 'Disclosure Restriction - Approval Letter'. A red arrow points to this entry.

ID	Date	Title
2647	12/12/2016	Disclosure Restriction - Approval Letter

- The Approval/Denial letter is generated.

Protected Health Information Management Tool User Manual



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.

Protected Health Information Management Tool User Manual

Monday, December 12, 2016 Patient Search Logout

Patient User Admin Requests Authorizations Requester Reports

Current Patient: Post, Washington 01/15/1968

Authorization

Type (the type of authorization to create)
Standard Authorization

Protected Health Information to be Released (the part of the medical record to be released, such as "complete medical record", "pathology report", etc.)
Entire medical record

Reason for Release of Medical Information (a reason for creating an authorization)
Personal Use

Accountable Disclosures to the patient or personal representative under the Right to Access their PHI, no reason is required.

Releasing Organization (Organization that released the authorization)
DHA

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.

Authorization Start Date (the effective date of the authorization in MM/DD/YYYY format)
12/12/2016

Authorization Expiration (the expiration date of the authorization in MM/DD/YYYY format, an Action Completed may be used instead of a date)
12/11/2017

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)
[Text Field]

Treatment Type (the type of Treatment)
Outpatient and Inpatient

Signed (checked if the authorization is signed)
 by Washington Post on 12/12/2016

Revoked (checked if the authorization is revoked)
 by Washington Post on 12/12/2016

Comments (the comments related to the Authorization)
[Text Field]

Generate Authorization Document (generate authorization document for printing purposes)

Save

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

Protected Health Information Management Tool
User Manual

Treatment Type (the type of Treatment)
Outpatient and inpatient

Signed (checked if the authorization is signed)
by Washington Post on 12/12/2016

Revoked (checked if the authorization is revoked)
by Washington Post on 12/12/2016

Invalid (Invalidates the Authorization but does NOT remove any previous Authorized Releases)

Comments (the comments related to the Authorization)

Created: 12/12/2016 10:07 Updated: 12/12/2016 10:07

Update

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

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.

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

Monday, December 12, 2016 Patient Search Logoff

Patient User Admin Requests Authorizations Requester Reports

Current Patient: Post, Washington 01/15/1966

Summary
A restriction of disclosures exists for this patient.
An alternate address exists for this patient.

Summary Item Filters Display Show All

Accountable Disclosures Suspensions Restrictions Reports Letters Authorizations Authorized Releases NPPs Complaints

10. Place a check in the Authorizations checkbox.

11. Click on the Display button.

Monday, December 12, 2016 Patient Search Logoff

Patient User Admin Requests Authorizations Requester Reports

Current Patient: Post, Washington 01/15/1966

Summary
A restriction of disclosures exists for this patient.
An alternate address exists for this patient.

Summary Item Filters Display Show All

Accountable Disclosures Suspensions Restrictions Reports Letters Authorizations Authorized Releases NPPs Complaints

Authorizations (Invalid authorizations are highlighted in red)

ID	Type	Reason	Description	Signed	Expiration	Revoked
2572	Standard Authorization	Personal Use	For releases of 'Entire medical record' to 'New York Post, 123 Manhattan St, New York NY 54321, ph:123-123-1234, fc:123-123-4567'		12/11/2017	
2552	Standard Authorization	Personal Use	For releases of 'Complete medical record' to 'Washington Post Jr., 2000 Pennsylvania Ave., Washington DC, ph:111-222-3333, fc:111-222-4444'	11/17/2016	12/25/2016	

Protected Health Information Management Tool User Manual

- 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.

The screenshot displays the 'Standard Authorization' form. At the top, there is a dropdown menu for 'Treatment Type (the type of Treatment)' set to 'Outpatient and Inpatient'. Below this are sections for 'Signed (checked if the authorization is signed)', 'Revoked (checked if the authorization is revoked)', and 'Invalid (invalidates the Authorization but does NOT remove any previous Authorized Releases)'. Each section has a checkbox and a 'by' field with a dropdown menu, and an 'on' field with a date picker. The 'Signed' and 'Revoked' sections are currently unchecked. Below these is a 'Comments (the comments related to the Authorization)' text area. The form is dated 'Created: 12/12/2016 10:07 Updated: 12/12/2016 10:07' and has an 'Update' button. At the bottom, there are two tables. The first is 'Authorized Releases (Invalid authorized releases are highlighted in red)' with columns for ID, Date, Origin Organization, and Comments, and a 'Create' button. The second is 'Associated Documents' with columns for ID, Date, and File, and an 'Attach' button. The 'Associated Documents' table has one entry with ID 2648, Date 12/12/2016, and File 'Standard Authorization', which is highlighted with a red box.

ID	Date	Origin Organization	Comments
----	------	---------------------	----------

ID	Date	File
2648	12/12/2016	Standard Authorization

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

Protected Health Information Management Tool User Manual

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) Post, Washington	2. DATE OF BIRTH (YYYYMMDD) 19680115	3. SOCIAL SECURITY NUMBER 000-00-0000
4. PERIOD OF TREATMENT: FROM - TO (YYYYMMDD) 20161212	5. TYPE OF TREATMENT (X one) <input type="checkbox"/> OUTPATIENT <input type="checkbox"/> INPATIENT <input checked="" type="checkbox"/> BOTH	
SECTION II - DISCLOSURE		
6. I AUTHORIZE <u>DHA</u> TO RELEASE MY PATIENT INFORMATION TO: <i>(Name of Facility/TRICARE Health Plan)</i>		
a. NAME OF PHYSICIAN, FACILITY, OR TRICARE HEALTH PLAN New York Post		b. ADDRESS (Street, City, State and ZIP Code) 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) <input checked="" type="checkbox"/> PERSONAL USE <input type="checkbox"/> CONTINUED MEDICAL CARE <input type="checkbox"/> SCHOOL <input type="checkbox"/> OTHER (Specify) <input type="checkbox"/> INSURANCE <input type="checkbox"/> RETIREMENT/SEPARATION <input type="checkbox"/> LEGAL		
8. INFORMATION TO BE RELEASED Entire medical record		
9. AUTHORIZATION START DATE (YYYYMMDD) 20161212	10. AUTHORIZATION EXPIRATION <input checked="" type="checkbox"/> DATE (YYYYMMDD) 20171211 <input type="checkbox"/> 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 where my medical records are held or to the TMA Service Officer if this is an authorization for information maintained by the		

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.

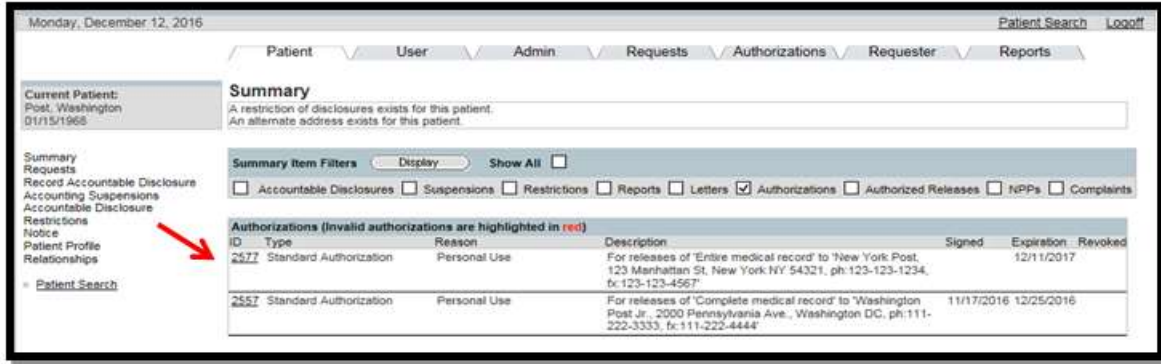
Steps to document signature for an authorization has been obtained:

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

The screenshot shows the PHIMT interface. At the top, the date is Monday, December 12, 2016. The navigation tabs are Patient, User, Admin, Requests, Authorizations, Requester, and Reports. The Patient tab is selected. Below the tabs, the current patient information is displayed: Post, Washington, 01/15/1968. The Summary section shows a restriction of disclosures and an alternate address. The Summary Item Filters section has a 'Display' button and a 'Show All' button. The 'Authorizations' checkbox is checked and highlighted with a red box. Other checkboxes include Accountable Disclosures, Suspensions, Restrictions, Reports, Letters, Authorized Releases, NPPs, and Complaints.

2. Click on the numerical ID hyperlink.

Protected Health Information Management Tool User Manual



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.

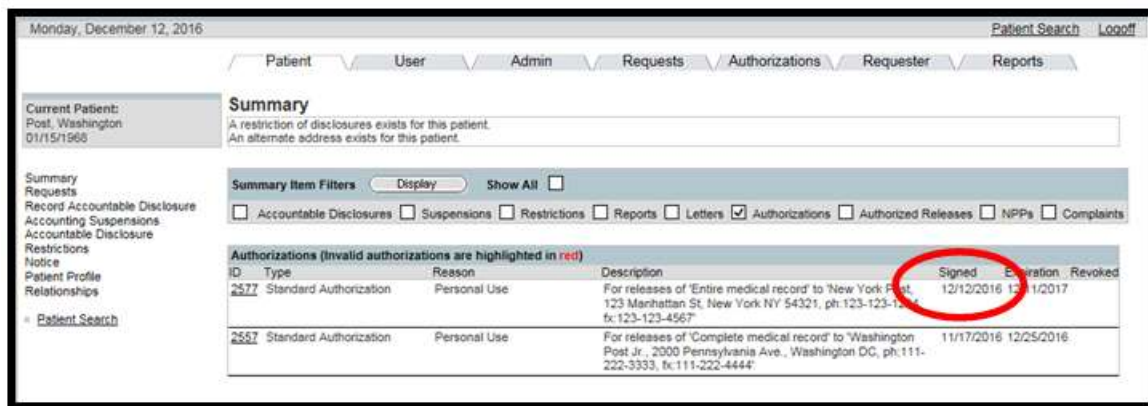


7. Select the Patient tab.
8. Place a check in the Authorizations checkbox.
9. Click on the Display button.



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

Protected Health Information Management Tool User Manual

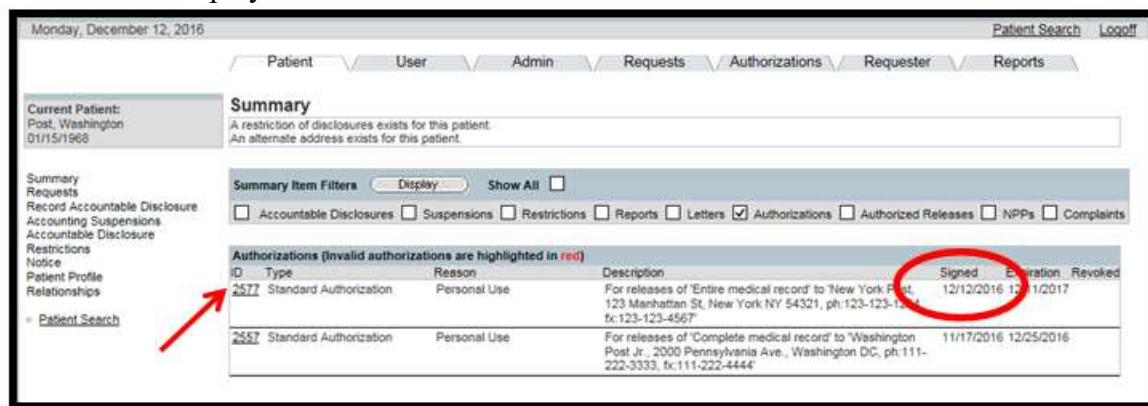


5.3.13 Revoke an Authorization

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.

Protected Health Information Management Tool User Manual

Signed (checked if the authorization is signed)
 by Washington Post on 12/12/2016

Revoked (checked if the authorization is revoked)
 by Washington Post on 12/12/2016

Invalid (invalidates the Authorization but does NOT remove any previous Authorized Releases)

Comments (the comments related to the Authorization)

Created: 12/12/2016 10:07 Updated: 12/12/2016 10:26

7. Click on the Patient tab to view the authorization.
8. Place a check in the Authorizations checkbox.
9. Click on the Display button.

Monday, December 12, 2016 Patient Search Logoff

Patient User Admin Requests Authorizations Requester Reports

Current Patient: Post, Washington 01/15/1968

Summary
A restriction of disclosures exists for this patient.
An alternate address exists for this patient.

Summary Item Filters: Display Show All

Accountable Disclosures Suspensions Restrictions Reports Letters Authorizations Authorized Releases NPPs Complaints

- The revoked authorization is highlighted in red.

Monday, December 12, 2016 Patient Search Logoff

Patient User Admin Requests Authorizations Requester Reports

Current Patient: Post, Washington 01/15/1968

Summary
A restriction of disclosures exists for this patient.
An alternate address exists for this patient.

Summary Item Filters: Display Show All

Accountable Disclosures Suspensions Restrictions Reports Letters Authorizations Authorized Releases NPPs Complaints

Authorizations (invalid authorizations are highlighted in red)

ID	Type	Reason	Description	Signed	Expiration	Revoked
2577	Standard Authorization	Personal Use	For releases of 'Entire medical record' to New York Post, 123 Manhattan St, New York NY 54321, ph:123-123-1234, fx:123-123-4567	12/12/2016	12/11/2017	12/12/2016
2552	Standard Authorization	Personal Use	For releases of 'Complete medical record' to Washington Post Jr., 2000 Pennsylvania Ave., Washington DC, ph:111-222-3333, fx:111-222-4444	11/12/2015	12/04/2016	

5.3.14 Administrative Summary Reports

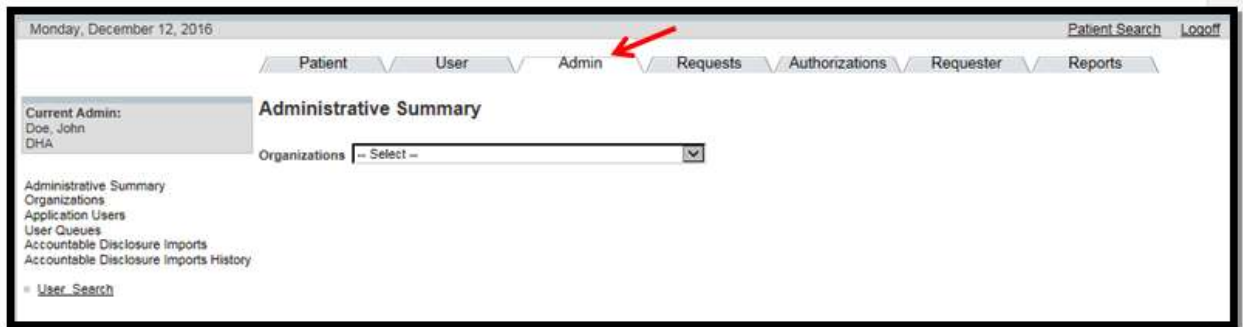
Protected Health Information Management Tool User Manual

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.

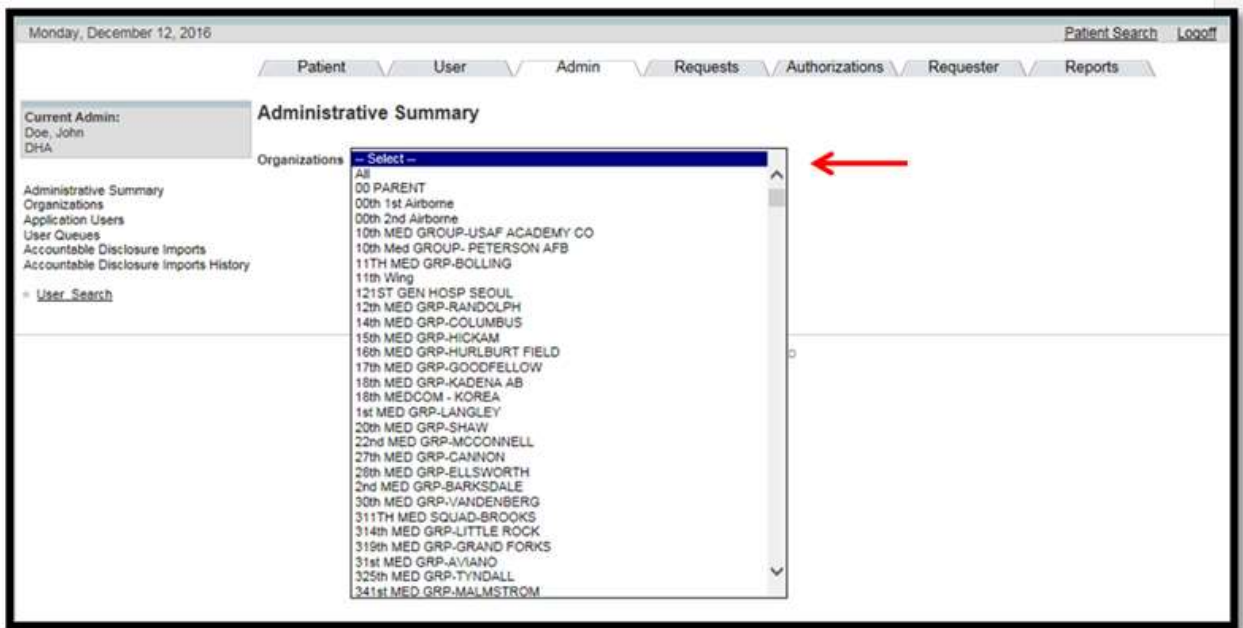
The Administrative Summary Reports are performed by Privacy Specialists.

Steps to create an Administrative Summary Report:

1. Select the Admin Tab.

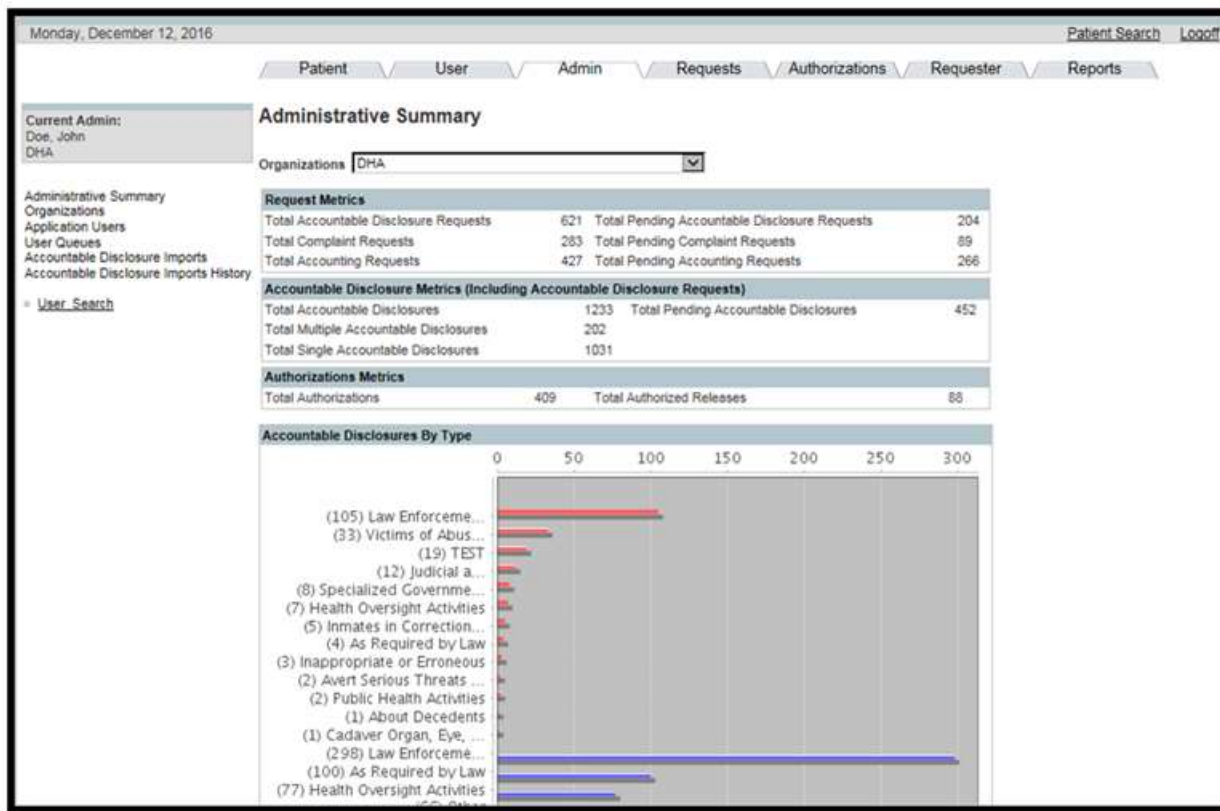


2. Select your Organization from the drop-down box.



- The Administrative Summary reports will display.

Protected Health Information Management Tool User Manual



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.

Protected Health Information Management Tool User Manual

2. Click on the Simple Disclosure radio button.
3. Click on the Next button.

Monday, November 14, 2016 Patient Search Logoff

Patient User Admin **Requests** Authorizations Requester Reports

Current Request: None

Create New Request

Select Request Type

- Accountable Disclosure
- Accountable Disclosure Accounting
- Complaint
- Simple Accountable Disclosure Request

4. Search for the Patient.

Monday, November 14, 2016 Patient Search Logoff

Patient User Admin Requests **Authorizations** Requester Reports

Current Request: Accountable Simple Disclosure Request

Select Patient Accountable Disclosure Details

1 2

Patient Search

by Name/State (Last) (First)

(State) (Birth Date in MMDD/YYYY format)

-OR-

SSN (in ###-##-#### format, enter '000-00-0000' if not known)

-OR-

EDIPN (DoD EDI Person Identifier)

-OR-

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

5. Select patient from the Search Results screen.

Monday, November 14, 2016 Patient Search Logoff

Patient User Admin Requests Authorizations Requester Reports

Current Request: Accountable Simple Disclosure Request

Select Patient Accountable Disclosure Details

1 2

Patient Search Results

Search Results - Click on the name to select a person

Name	ID	EDIPN	Birth Date	Address
Post, Washington	1163		01/15/1968	1600 Penn Ave Washington, DC 20011

Other options:
[Adjust your search criteria and try again](#)
[Create a new Patient record](#)

Protected Health Information Management Tool
User Manual

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.

The screenshot shows a form with three sections for adding files. Each section has a text input for the document title, a 'Browse...' button, and a 'Please select a file you wish to attach' label. Below these is an 'Action (action for this request)' dropdown menu with 'Route to My Worklist' selected. At the bottom are 'Back' and 'Save' buttons. Red arrows point to the 'FILE 1: Document Title' field, the first 'Browse...' button, the 'Action' dropdown, and the 'Save' button.

8. Click on the Save button.

- The Request Summary screen will display.

The screenshot shows the 'Request Summary' screen. It includes a navigation bar with 'Patient Search' and 'Logout'. The main content area is divided into sections: 'Current Request: Simple Accountable Disclosure Request', 'Summary', 'History', 'Documents', and 'Accountable Disclosure Details'. The 'Request Summary' section displays patient information (Washington Post, 1600 Penn Ave, DC 20011), requester information (John Smith, 13450 Bob Wilson, San Diego, CA 92134), request status (Routed for Approval), and creation/last update dates (11/14/2016 at 03:43:00 PM EST). An 'Other Request Details' table is also present.

Other Request Details	
Description	Details
Request Type	Simple Accountable Disclosure Request
Accountable Disclosure Type	Type: Health Oversight Activities, ID: 1861, Date: 10/31/2017
Identity Verified Text	Social Security Number

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.

Protected Health Information Management Tool
User Manual

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.

Protected Health Information Management Tool
User Manual

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.

Protected Health Information Management Tool
User Manual

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.

Protected Health Information Management Tool
User Manual

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

Protected Health Information Management Tool
User Manual

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

Protected Health Information Management Tool
User Manual

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)