Defense Health Agency (DHA)

Protected Health Information Management Tool
(PHIMT)

Training Reference: User Admin Guide
Version 3.0

March 2011

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

Last Edited: 3/8/2011

TABLE OF CONTENTS

1.0 INTRODUCTION TO PHIMT 3
1.1 PHIMT USER PERMISSIONS 3
1.2 PHIMT USER ROLES 4
1.2.1 PRIVACY SPECIALIST 5
1.2.2 REGULAR USER 5
1.2.3 USER ADMIN 5
1.3 PHIMT SYSTEM REQUIREMENTS 5
1.3.1 BROWSER REQUIREMENTS 5
1.3.2 PLUG-INS 6
2.0 ACCESSING AND USING PHIMT 6
3.0 UNDERSTANDING PHIMT SCREENS 9
3.1 SCREEN FEATURES 9
3.1.1 DATE 9
3.1.2 NAVIGATIONAL OPTIONS 9
3.1.3 STATUS BOX 9
3.1.4 ACTIVITY HYPERLINKS 10
3.1.5 PHIMT SCREEN TABS 10
3.1.6 SCREEN TITLE 10
3.1.7 DISPLAY SCREEN/APPLICATION WINDOW 10
3.2 PHIMT ERROR MESSAGES 11
4.0 MHS DATA REPOSITORY 11
4.1 ACCESSING PATIENT ACCOUNTS 12
4.2 DUPLICATE ACCOUNTS 13
4.3 PATIENT PROFILE 13
5.0 USER ADMIN FUNCTIONALITY 14
5.1 ESTABLISH WORKFLOW 14
5.2 QUEUE SETUP 17
5.3 REQUESTER FAVORITES 19
6.0 GLOSSARY 25
7.0 USER ROLE PERMISSIONS 29

1.0 INTRODUCTION TO PHIMT

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

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

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

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

1.1 PHIMT User Permissions

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

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

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

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

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

1.2 PHIMT User Roles

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

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

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

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

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

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

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

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

1.2.1 Privacy Specialist

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

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

1.2.2 Regular User

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

1.2.3 User Admin

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

1.3 PHIMT SYSTEM REQUIREMENTS

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

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

1.3.1 Browser Requirements

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

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

1.3.2 Plug-Ins

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

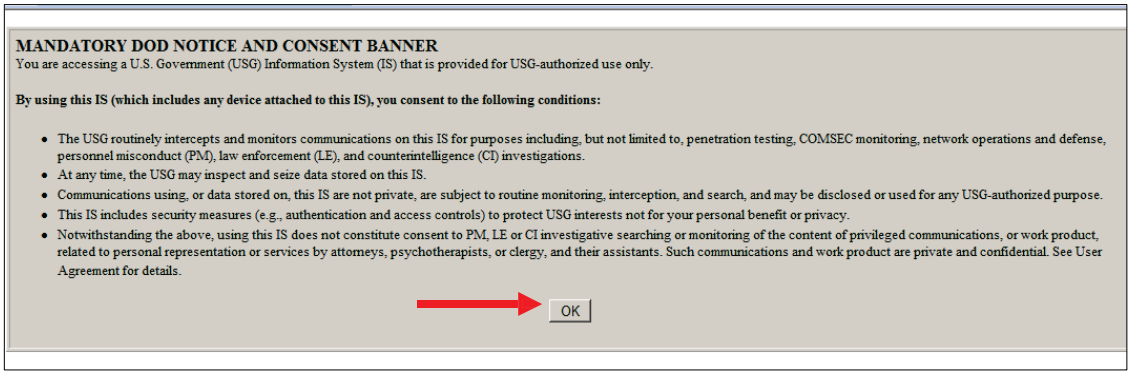
NOTE: To display the generated letters and reports in the browser, the Adobe Acrobat Plug-in is required. This is normally installed with Adobe Acrobat Reader. Download Adobe Acrobat for free at http://www.adobe.com.

2.0 ACCESSING AND USING PHIMT

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

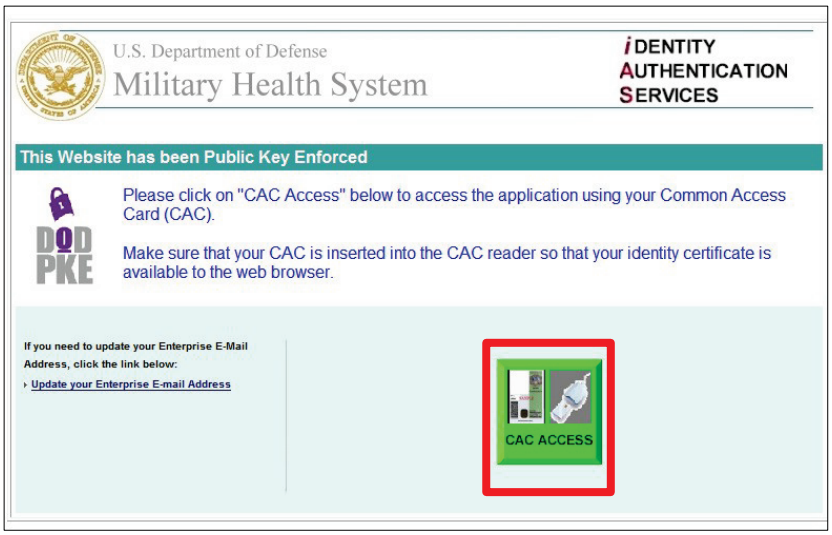
To login to the PHIMT application:

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



2. Read the DoD Notice and Consent Banner.

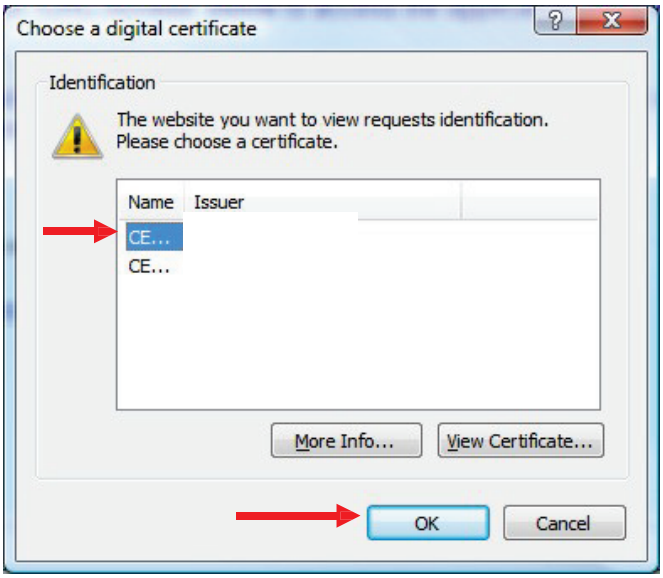
3. Click on the OK button.

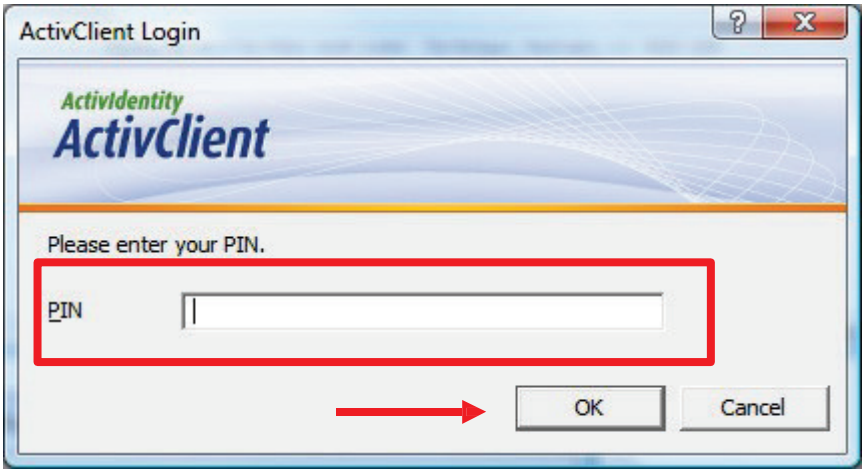


4. Click on the Green CAC Access button.

5. Select CAC Identification.

6. Click on the OK button.





7. Enter CAC PIN.

8. Click on the OK button.

9. Read the Notice and Terms of Use.

10. Click on the Accept button.

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

3.0 UNDERSTANDING PHIMT SCREENS

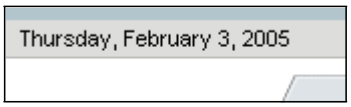
Each tab of the PHIMT screens contains some basic information that will be helpful to you when performing the various activities.

3.1 SCREEN FEATURES

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

3.1.1 Date

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

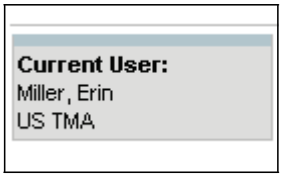


3.1.2 Navigational Options

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

3.1.3 Status Box

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



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

3.1.4 Activity Hyperlinks

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

3.1.5 PHIMT Screen Tabs

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

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

3.1.6 Screen Title

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

3.1.7 Display Screen/Application Window

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

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

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

3.2 PHIMT ERROR MESSAGES

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

4.0 MHS DATA REPOSITORY

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

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

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

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

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

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

Monday, April 19, 2010 Patient Search Logoff

Patient | User | Admin | Requests | Requester

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

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

Patient Search

Patient Search Results

Search Results - Click on the name to select a person

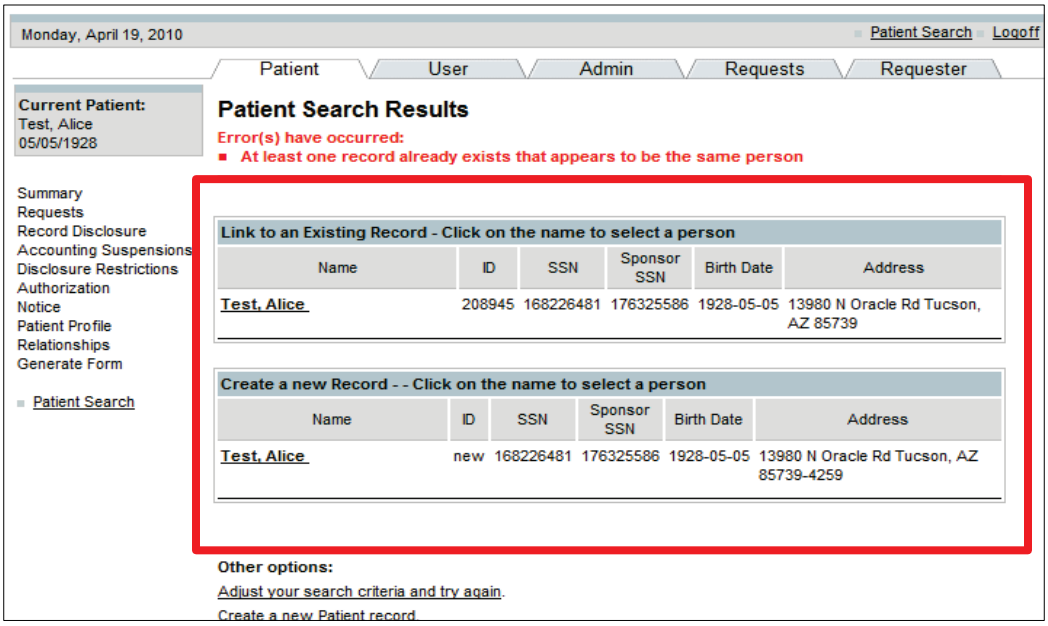
Name	ID	SSN	Sponsor SSN	Birth Date	Address
Test, Rebecca	208939	271905664	274864759	1984-03-13	1445 Beaver Creek Ln Kettering, OH 45429-3703
		EDIPN:1385132766			

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

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

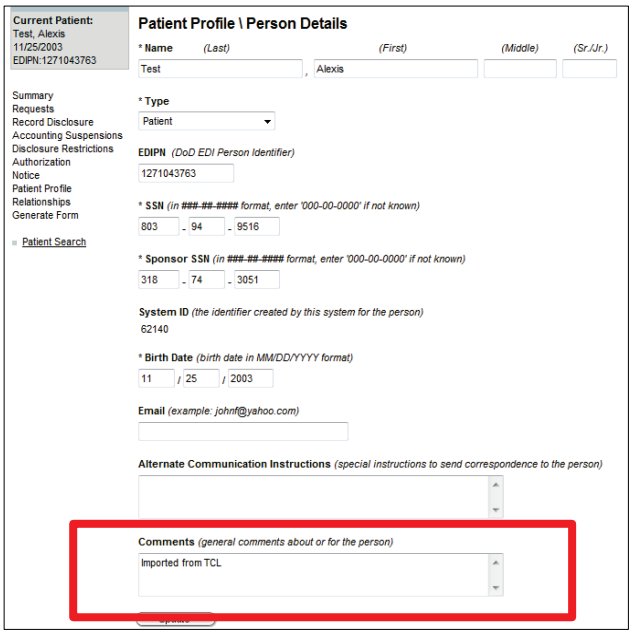
4.2 DUPLICATE ACCOUNTS

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



4.3 PATIENT PROFILE

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



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

5.0 USER ADMIN FUNCTIONALITY

The following information will provide you with step-by-step instructions for adding organizations, and establishing User-to-User Relationships (establishing office workflow).

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

- Establish workflow
- Setup a queue
- Create a requester favorites

5.1 ESTABLISH WORKFLOW

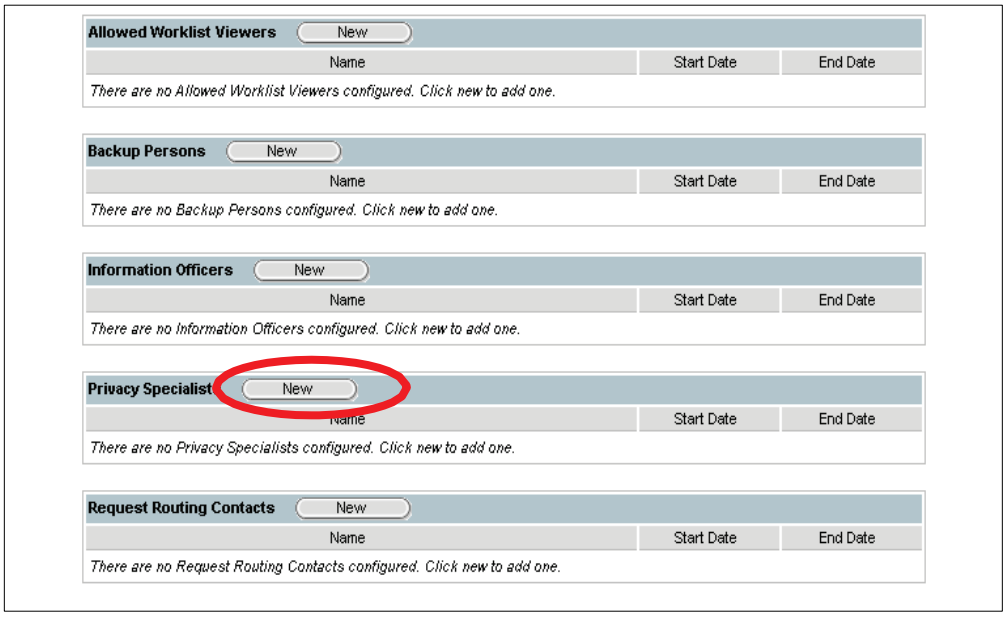
User-to-User relationships affect how requests are routed within PHIMT. These relationships need to be constructed in a manner that allows them the most use of all available Action Types shown on Request Action and Edit Activity screens. A typical request may be routed to a User Worklist, Privacy Specialist, or Other User. The User-to-User Relationships screen defines specific users who would be fulfilling these roles. This table shows the definitions of available user relationships.

User Relationship Definitions	
User Role	Description
Privacy Specialist	• Privacy Specialist is a user who is responsible for accepting and approving disclosure and disclosure accounting requests. • A Privacy Specialist for a Regular User is usually someone from the same organization who is working in the Privacy Office. • A Privacy Specialist for a Privacy Specialist is a person at the high level who is working in the Central Privacy Office. NOTE: The person selected as a Privacy Specialist should also have Privacy Specialist permission assigned to them by the User Admin.
Backup Person	• Backup Person is a user who acts in your place whenever you are not able to attend to your requests due to being out of the office for business or pleasure, changing work priorities, or other reasons. • All outstanding requests assigned to you will be reassigned to your Backup Person at the time when the Backup Person relationship is assigned. • Any new requests will be routed to your Backup Person instead of you. You can assign a date when the Backup Person relationship should end or leave it open ended. NOTE: End the Backup Person relationship as soon as you can resume working on your own requests.

To set up a Workflow:

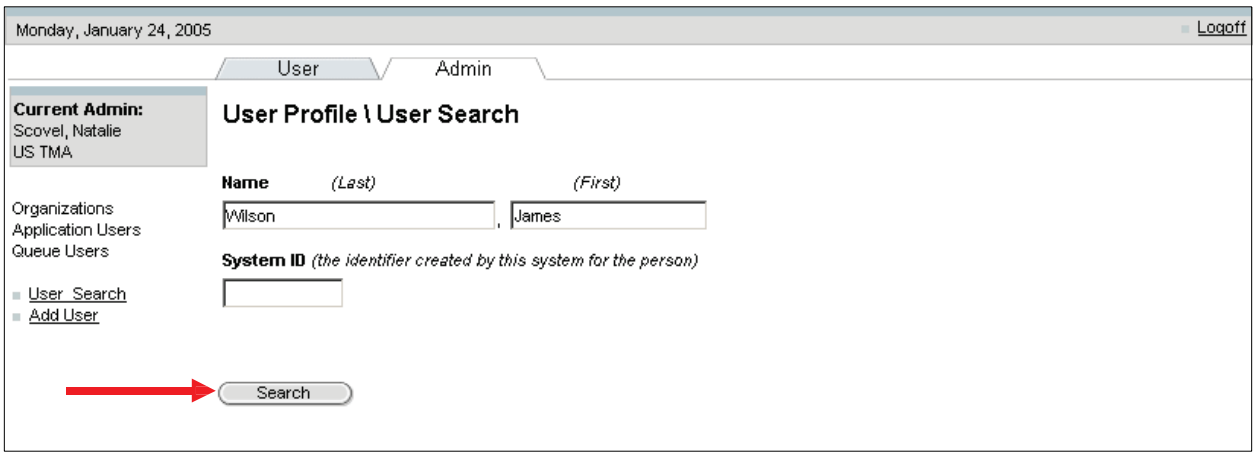
1. Scroll to the bottom of the User Profile screen (Regular User).

2. Click on the New button next to Privacy Specialists.



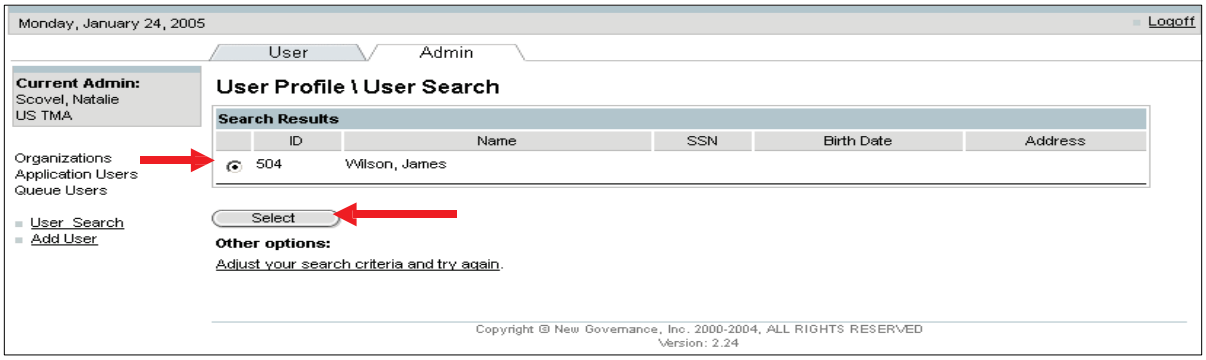
3. Enter Search Criteria for the Privacy Specialist that you want to add.

4. Click on the Search button.



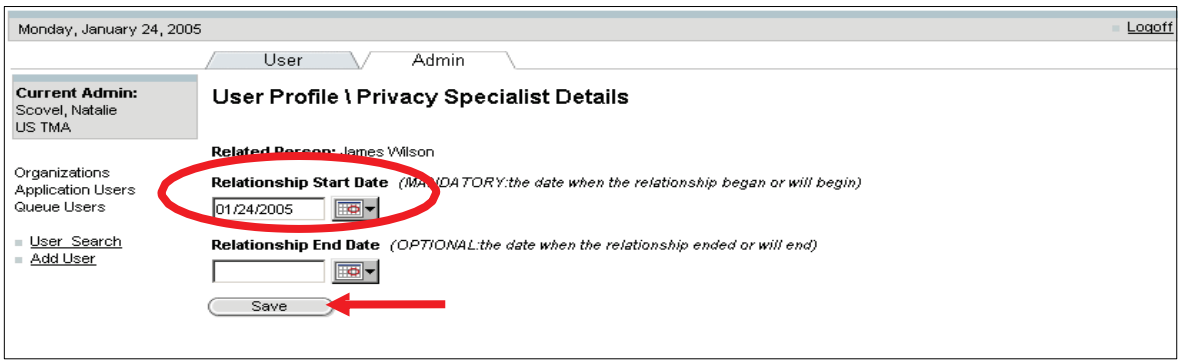
5. Select the appropriate Privacy Specialist from the search results and click on the Select button.

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

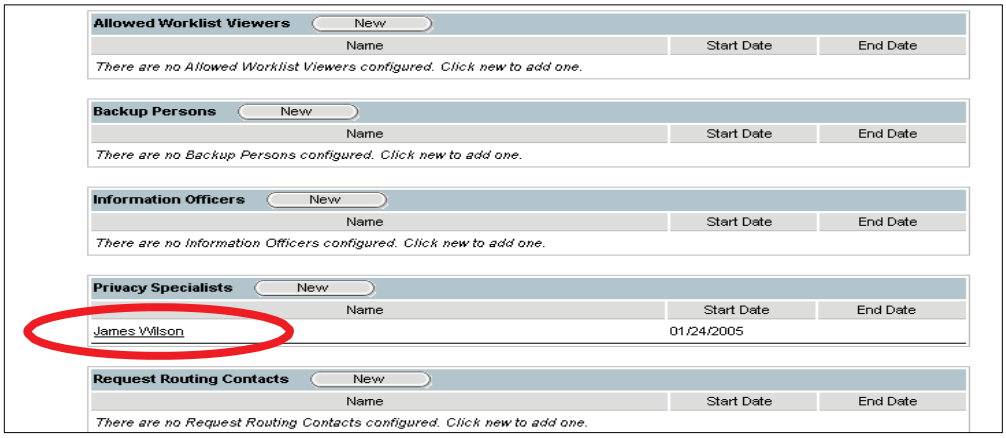


6. Set the Relationship Start Date/End Date. (The end date is optional).

7. Click on the Save button.



- The Privacy Specialist is added to the User Profile screen.



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

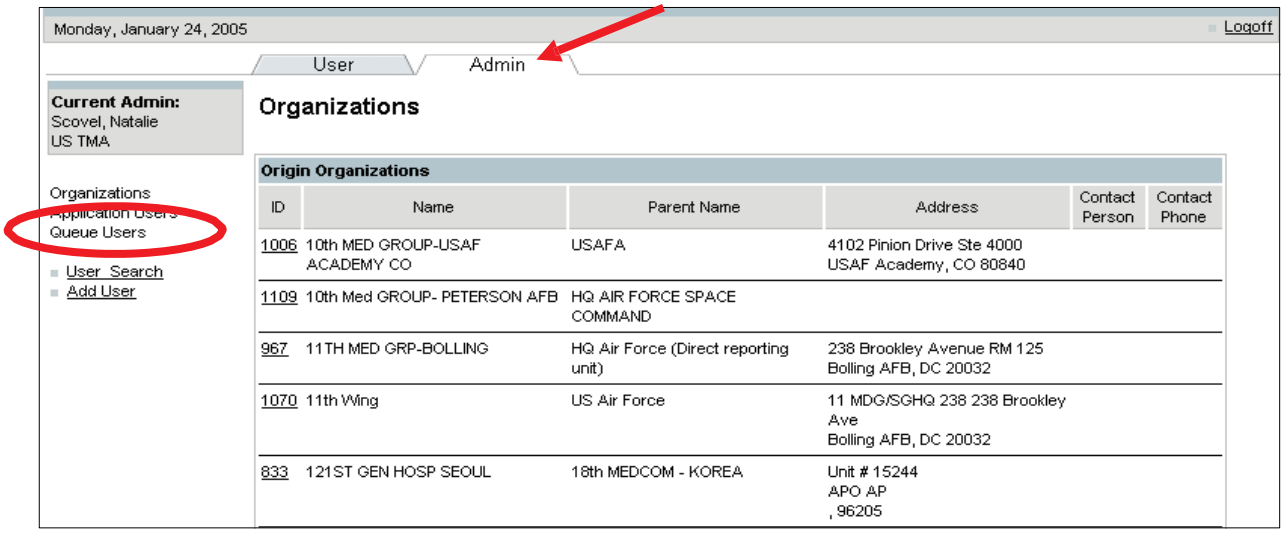
5.2 QUEUE SETUP

A queue is a distribution list for a specific organization that is comprised of two or more Privacy Specialists. The User Admin at the local command is responsible for setting up a queue. Queues are created to expedite the process of approving/denying a disclosure. Only users affiliated with a given organization will see that organization's routing options.

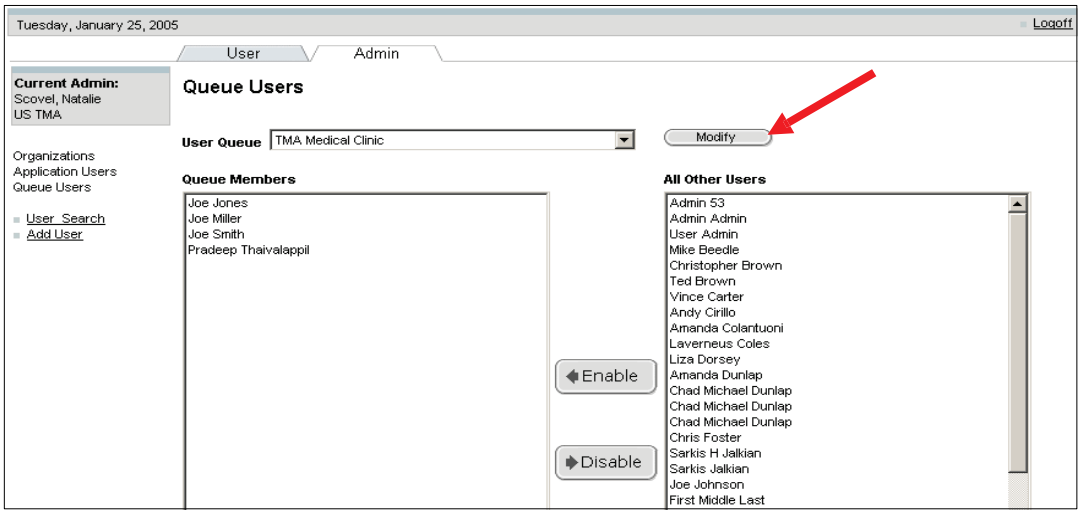
To setup a queue:

1. Select the Admin Tab.

2. Select the Queue Users hyperlink.



3. Click on the Modify button to add a new queue.



4. Click on the New button.

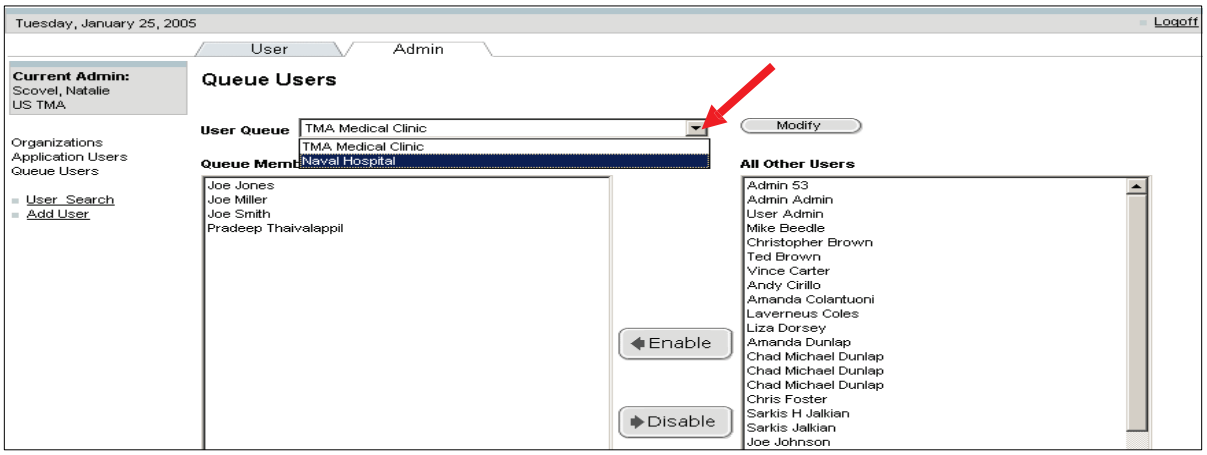
Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.

5. Enter the description of the Queue in the text box.

6. Click on the Save button.

7. Once saved, select the Queue Users hyperlink.

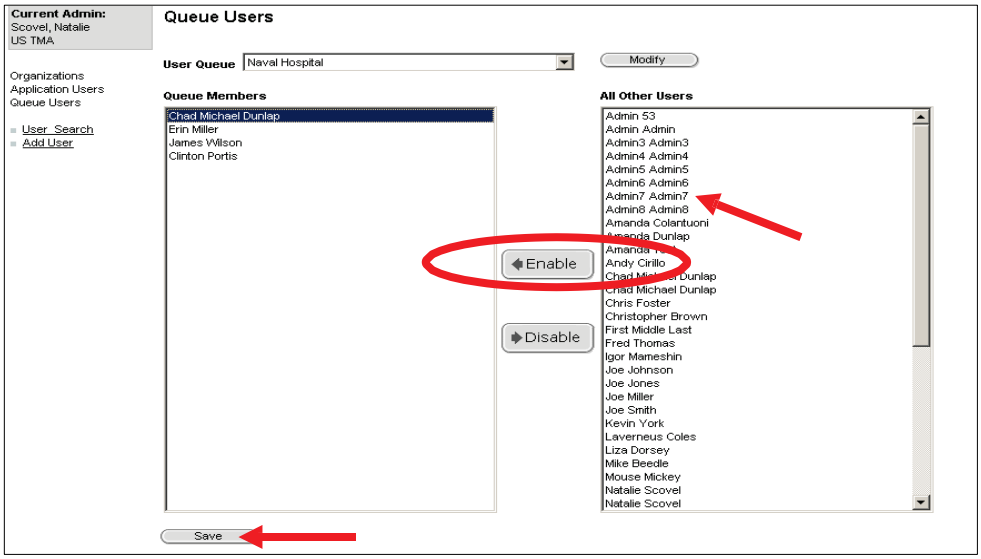
8. Select the Queue you created from the drop-down box.



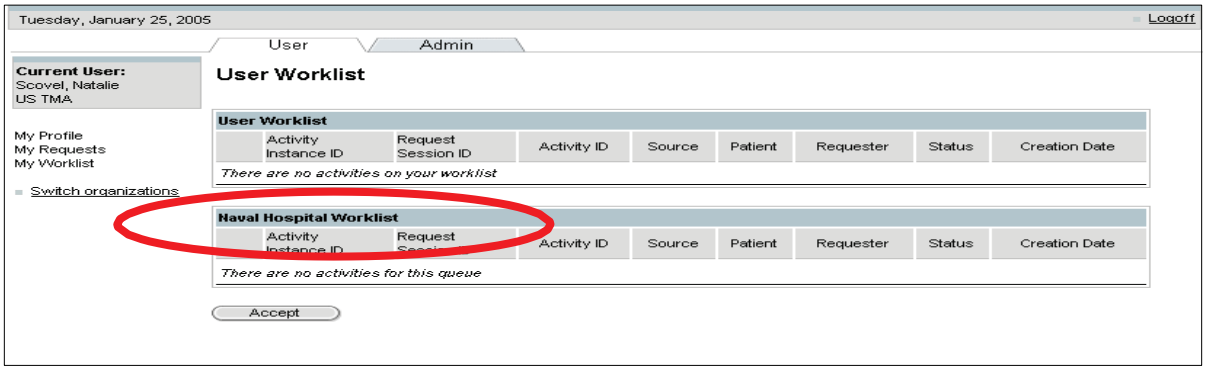
9. Select the users that you want to add to the queue and click on Enable.

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

10. Click on the Save button.



- The queue that you added will show up in the user's worklist.



5.3 REQUESTER FAVORITES

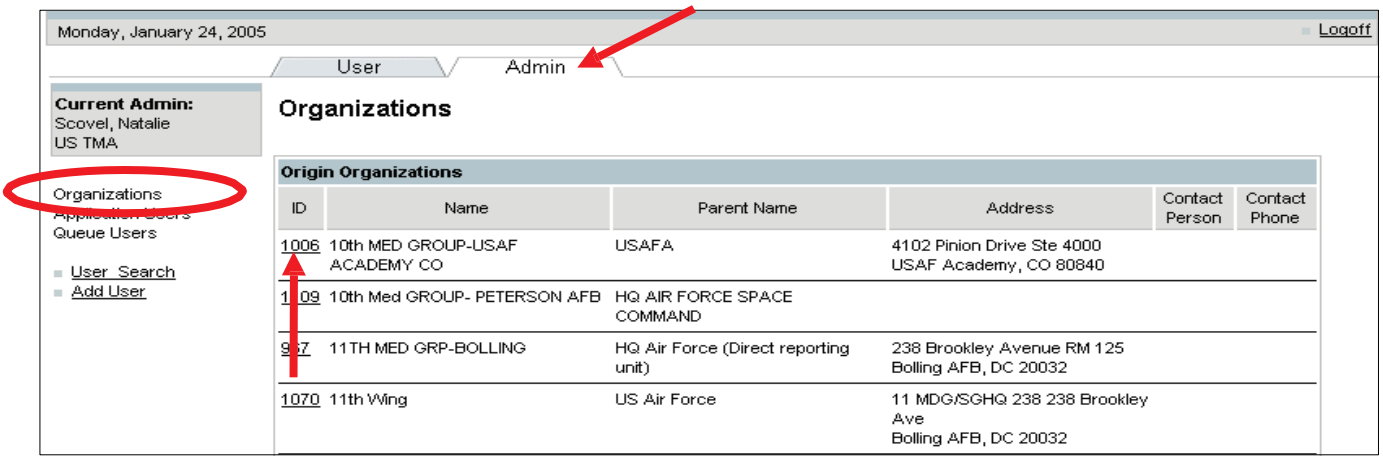
An organization can create a list of requester favorites that show up in the requester drop-down list. User Admins can set up the list of favorites per organization. If an organization name is not in the favorites list, the user will be allowed to search for it manually. A given "requester" can appear in multiple "favorites" lists.

To set up an organization's requester favorites:

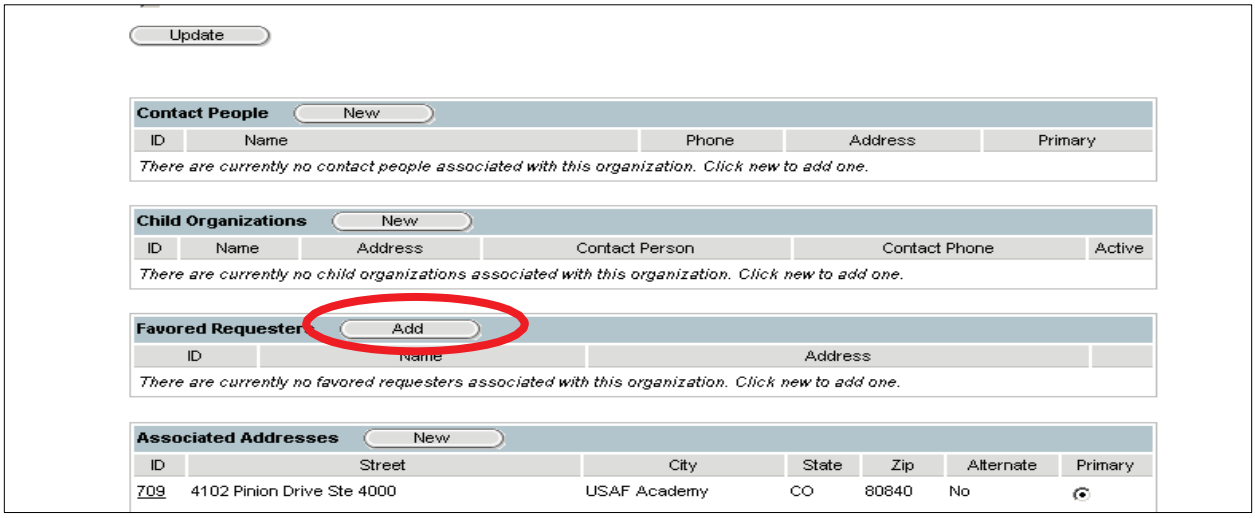
1. Select the Admin Tab.

2. Select the Organization's hyperlink.

3. Select the ID hyperlink for your Origin Organization.

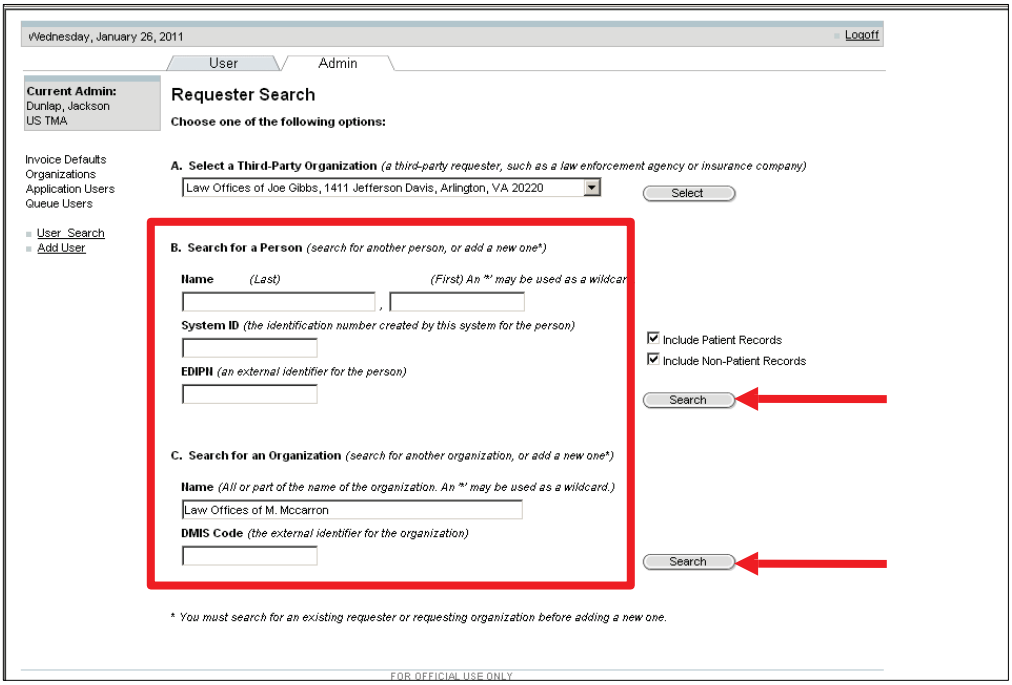


4. Scroll down to Favored Requesters and click on the Add button.

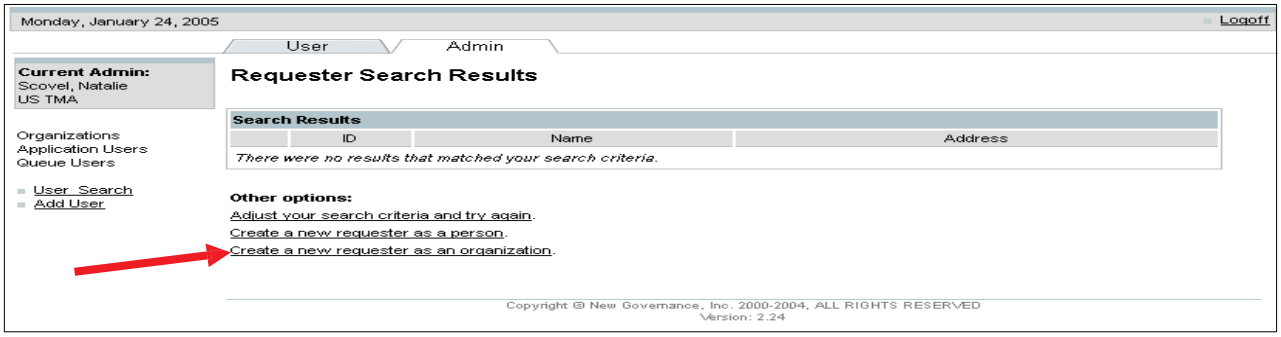


5. Enter organization search criteria.

6. Click on the Search button.

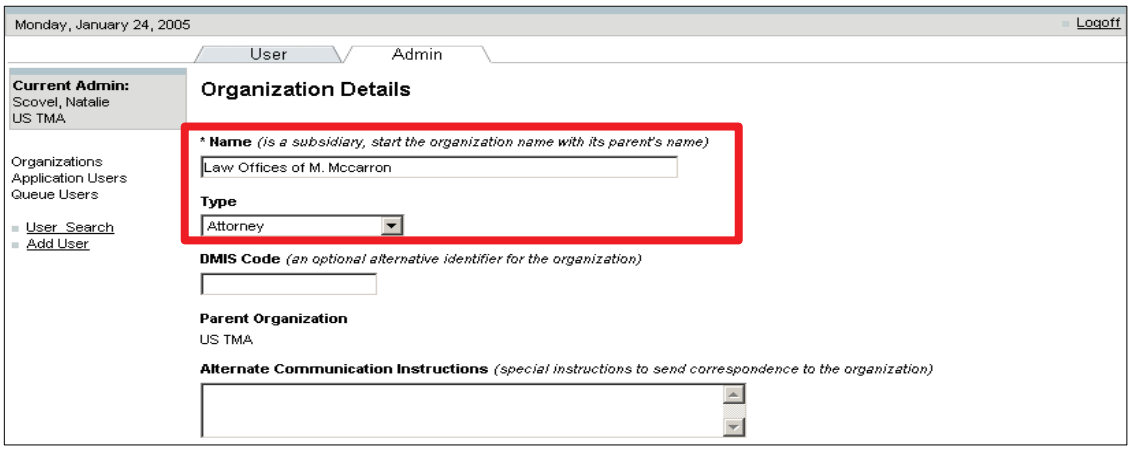


7. If the requester is not found, click on the "Create a new requester as an Organization" hyperlink.

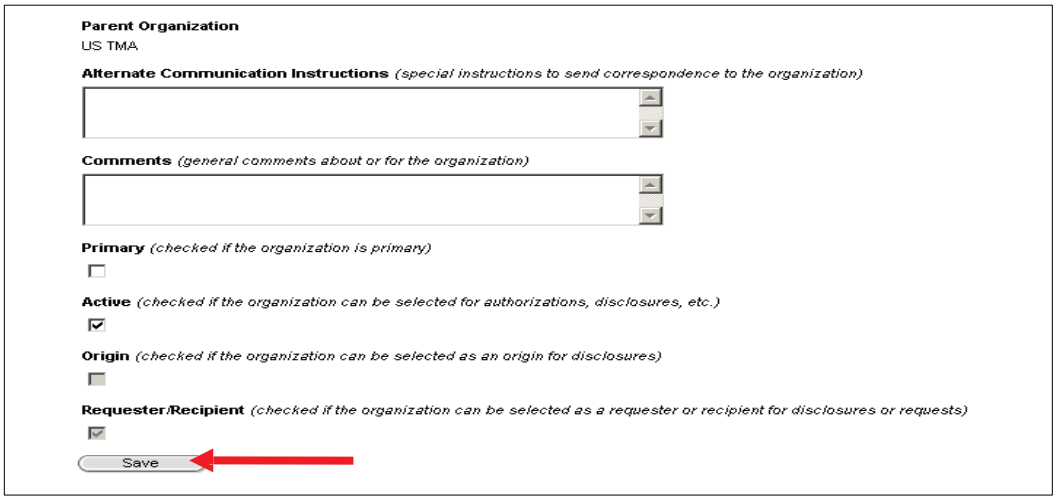


8. Enter the name of the Organization.

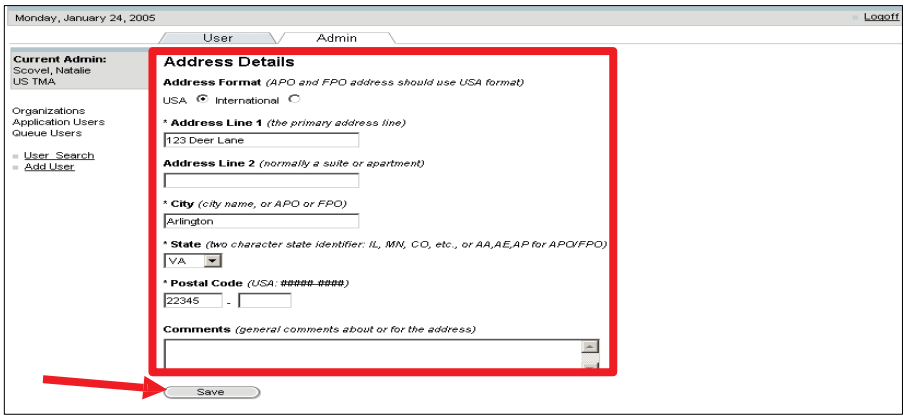
9. Select the organization type from the drop-down box.



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



11. Enter the Organization Address Details and click on the Save button.



- If you are entering an International Address, click on the International radio button.

onday, January 24, 2005 Logoff

User Admin

urrent Admin:
covel, Natalie
S TMA

ganizations
pplication Users
eue Users

User Search
Add User

Address Details

Address Format *(APO and FPO address should use USA format)*

USA International

Country *(country name)*

Antigua

International Address Line 1

International Address Line 2

International Address Line 3

Comments *(general comments about or for the address)*

Save

- The organization that you added now appears in your requester favorites.

Update

Contact People New

ID	Name	Phone	Address	Primary

There are currently no contact people associated with this organization. Click new to add one.

Child Organizations New

ID	Name	Address	Contact Person	Contact Phone	Active

There are currently no child organizations associated with this organization. Click new to add one.

Favored Requesters Add

ID	Name	Address	
1220	Law Offices of M. Mccarron	123 Deer Ln., Arlington, VA 22345	remove

Associated Addresses New

ID	Street	City	State	Zip	Alternate	Primary
709	4102 Pinion Drive Ste 4000	USAF Academy	CO	80840	No	

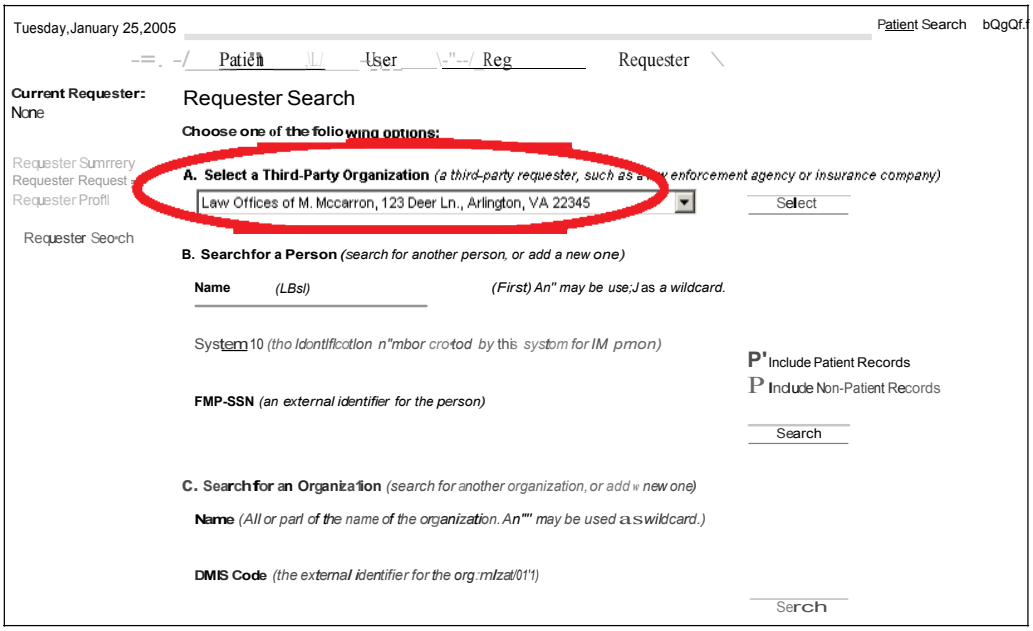
Phone Numbers New

ID	Phone	Comment	Active	Primary

There are currently no phone numbers on record for this organization. Click new to add one.

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

- When logging in as a Regular User, the organization that you added will appear in the requester favorites drop-down box for your organization



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

6.0 GLOSSARY

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

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

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

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

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

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

7.0 USER ROLE PERMISSIONS

PHIMT USER ADMIN PERMISSIONS	
PHIMT User Admin Tab	Enabled Permissions
Logon/Logoff	Both
User Tab	Switch to other organizations Update address User profile User workflow User worklist Workflow request
Admin Tab	All users list Attach file Organization management User management
Patient Tab	None (can perform patient profile and patient relationship activities.)
Requests Tab	None (perform new request: route to my worklist activity.)
Requester Tab	None