

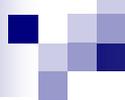


HEALTH AFFAIRS



Protected Health Information Management Tool (PHIMT)





PHIMT

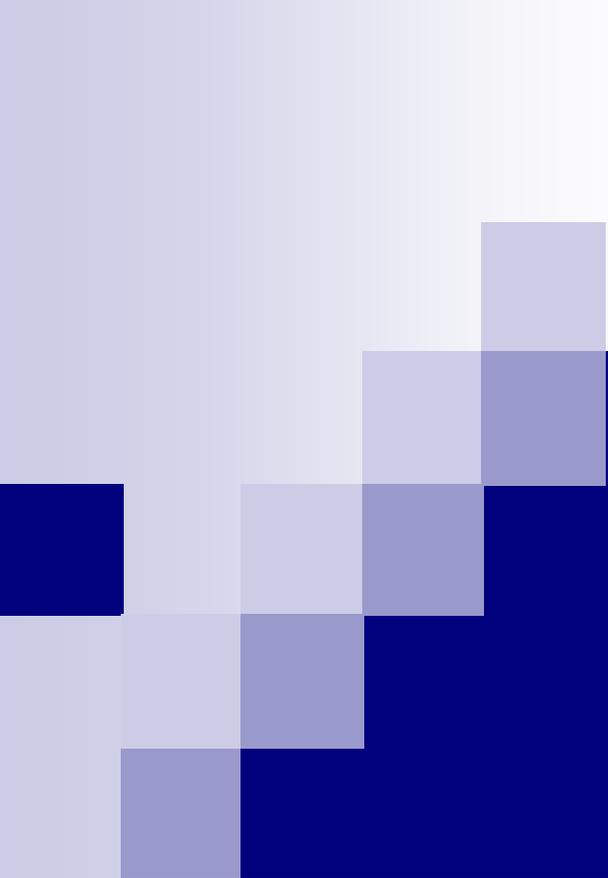
Agenda

- Introduction to the PHIMT
- User Admin Functionality
- Regular User Functionality
- Privacy Specialist Functionality
- Administrative Summary Reports
- Implementation of the PHIMT
- Tool Enhancements

PHIMT

Training Objectives

- Upon completion of this training, you will be able to:
 - Identify the use of the PHIMT in meeting the Accounting of Disclosures requirement of the HIPAA Privacy Rule
 - Describe the necessary policies and procedures
 - Describe the user roles and responsibilities within the PHIMT
 - Describe and interpret the data that the PHIMT can provide for compliance measurement
 - Implement PHIMT at your facility
 - Identify the latest tool enhancements



Introduction to PHIMT

Introduction to PHIMT

Objectives

- Upon completion of this lesson, you will be able to:
 - Explain what the PHIMT is and why it exists
 - Describe the capabilities of the PHIMT
 - Identify the advantages of using the tool
 - Explain the Authority for Multiple Disclosure Accounting
 - Identify the 14 Permitted Uses and Disclosures
 - Locate and describe the Disclosure Notification Letter
 - Describe the PHIMT terminology, user roles, and permissions
 - Explain the PHIMT Hierarchy

What is the PHIMT?

- The PHIMT is a web-based application that assists in complying with the HIPAA Privacy Disclosure Accounting Requirement
 - Commercial Off-The-Shelf (COTS) product customized for TMA
 - Deployed in October 2003 with a series of training supporting the deployment to the MTFs
 - Centrally managed application that is accessed via the Internet
 - Database is stored within TMA's Network Operations Center located in Falls Church, VA

Introduction to PHIMT

Why Does the PHIMT Exist?

- The HIPAA Privacy Rule requires a Covered Entity (CE) to maintain a history of when and to whom disclosures of Protected Health Information (PHI) are made for purposes other than treatment, payment and healthcare operations (TPO)
- Individuals have the right to receive an accounting of disclosures of PHI made by the CE
- Military Health System (MHS) must be able to provide an accounting of those disclosures to an individual upon request
 - Not required to account for disclosures that occurred prior to the April 14, 2003 compliance date
- To comply with this requirement, TMA provides an electronic disclosure-tracking tool

Tool Capabilities

- The tool enables users to:
 - Track PHI Requests or Release of Information
 - Maintain authorizations
 - Track complaints
 - Create an automated workflow process developed by the users
 - Create pre-defined requesters from organizations
 - View the details about the information disclosed
- It allows users to track disclosures, document requests for amendments and authorizations, document complaints and restrictions to PHI

Advantages of the PHIMT

- Consolidates multiple tasks into one electronic environment
- Protects the data
 - Allows for role-based access to maintaining the records and access to patient information
 - Protected Enclave
 - Defense Information Technology Security Certification and Accreditation Process (DITSCAP) certified
- Pre-populated drop-down fields
- Monthly MHS Data Repository (MDR) uploads
- Streamlined disclosure process
- Multiple Disclosure Accounting

Authority for Multiple Disclosure Accounting (1 of 2)



Multiple Disclosures

H I P A A P r i v a c y ♦ M a r c h 2 0 0 6

PURPOSE

The purpose of this paper is to provide guidance on multiple disclosures. It is intended to ensure that the Military Health Systems (MHS) apply appropriate safeguards, as set by the DoD Health Information Privacy Regulation (DoD 6025.18-R, C13.2.3) and the Health Insurance Portability and Accountability Act (HIPAA) of 1996, to prevent any use or disclosure of Protected Health Information (PHI) that would be in violation of HIPAA.

POLICY:

A Covered Entity (CE), (i.e. the Military Treatment Facility (MTF)), may account for multiple disclosures with a single entry if the MTF has made multiple disclosures of PHI to the same person or entity for a single purpose.

Authority for Multiple Disclosure Accounting (2 of 2)

- If, during the period covered by the accounting, the CE has made multiple disclosures of protected health information to the same person or entity for a single purpose...the accounting may, with respect to such multiple disclosures, provide the following:
 - Date, recipient of PHI, description, and purpose of disclosure
 - Frequency, periodicity, or number of the disclosures made during the accounting period
 - Date of the last such disclosure during the accounting period

14 Permitted Uses and Disclosures (1 of 2)

- Permitted Uses and Disclosures

- For the permitted uses and disclosures listed below, a patient's opportunity to agree or object is not required

- 1. As required by law**
- 2. Avert serious threats to health or safety**
- 3. Specialized government functions**
- 4. Judicial and administrative proceedings**
- 5. Medical facility patient directories**
- 6. Cadaver organ, eye or tissue donation purposes**
- 7. Victims of abuse, neglect or domestic violence**

14 Permitted Uses and Disclosures (2 of 2)

- Permitted Uses and Disclosures
- For the permitted uses and disclosures listed below, a patient's opportunity to agree or object is not required

- 8. Inmates in correctional institutions or in custody**
- 9. Workers' compensation**
- 10. Research purposes**
- 11. Public health activities**
- 12. Health oversight activities**
- 13. About decedents**
- 14. Law enforcement purposes**

Introduction to PHIMT

Disclosure Notification Letter (1 of 2)

HOME A to Z SEARCH HELP WHAT'S NEW SITE MAP

 TMA Privacy Office
HIPAA Compliance: Privacy



[Home](#)

[Freedom of Information Act \(FOIA\)](#)

[Records Management](#)

[HIPAA Privacy/Security](#)

[Privacy Act of 1974](#)

[System of Records](#)

[Data Use Agreements](#)

[Personnel Security \(ADP Background Checks\)](#)

POLICY MEMOS

[Expediting Veterans Benefits to Members with Serious Injuries and Illness](#)
The policy outlined in the above memorandum has been approved by the Under Secretary of Defense and is posted for your awareness and support. This policy is consistent with HIPAA and its execution is necessary to support the delivery of healthcare and other services or benefits Service Members are entitled to from the Department of Veterans Affairs (DVA).

[Notifying Individuals When Personal Information is Lost Stolen, or Compromised](#) 

[DoDVA Sharing MOU - Business Practices](#) 

[Accounting for Disclosures Regarding Military Personnel](#)

[Applicability of HIPAA Regulations to Article 32 \(pdf\)](#)

[Armed Forces Reserve Component \(pdf\)](#)

[DoD-DVA Health Information Sharing \(pdf\)](#)

[Lead Agent Guidance Memo \(pdf\)](#)



[PRIVACY HOMEPAGE](#)

[SECURITY HOMEPAGE](#)

[TMA RESOURCES](#)

[INFO LIBRARY](#)

[HIPSCC](#)

[TRAINING AND TOOLS](#)

[HIPAA FORMS](#)

[FAQs](#)

[POSTERS/BROCHURES](#)

[LINKS](#)

[CONTACT US](#)

 Notice of Privacy

Disclosure Notification Letter (2 of 2)

- Notifying Individuals When Personal Information is Lost, Stolen, or Compromised
 - 10 day notification requirement
 - Must notify patients of the loss of their information
 - Must account for them in the PHIMT (record the complaint)
- *If a DoD component is unable to comply with the notification requirements of this policy, the DoD component shall inform the Secretary immediately of the reasons why notice was not provided to the affected individuals...*

Key PHIMT Terminology

- **User** - an individual with a unique login ID and Password assigned to an organization within the tool

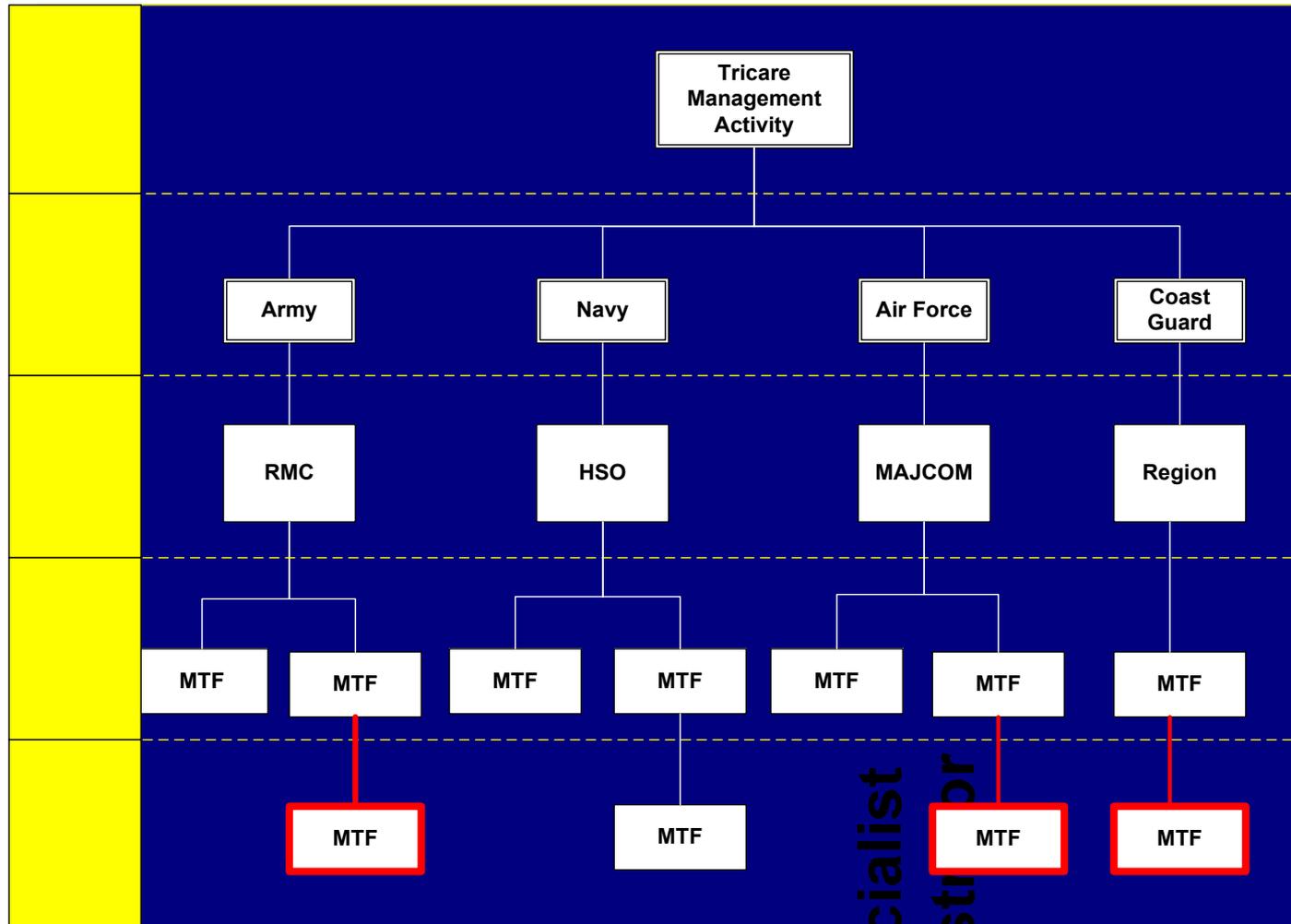
- **Organization** - a logical or physical entity such as an MTF, a Service or TMA

- **Role** - a named collection of permissions within the tool
 - A user can have the same roles in multiple organizations, or different roles in multiple organizations

User Roles and Permissions

- **User Admin** is a local admin for an MTF or a designated Service. This role allows one to add/modify users from within their Service and assign roles. This role will be handled by the email account administrators for each MTF or Service
- **Privacy Specialist** is the Privacy Officer or designee at an MTF or Service level. This role allows the user to maintain disclosure reporting, approve/deny disclosure requests, amendments to requests, restrictions to disclosures, disclosure suspensions and generate associated letters
- **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

Introduction to PHIMT Hierarchy



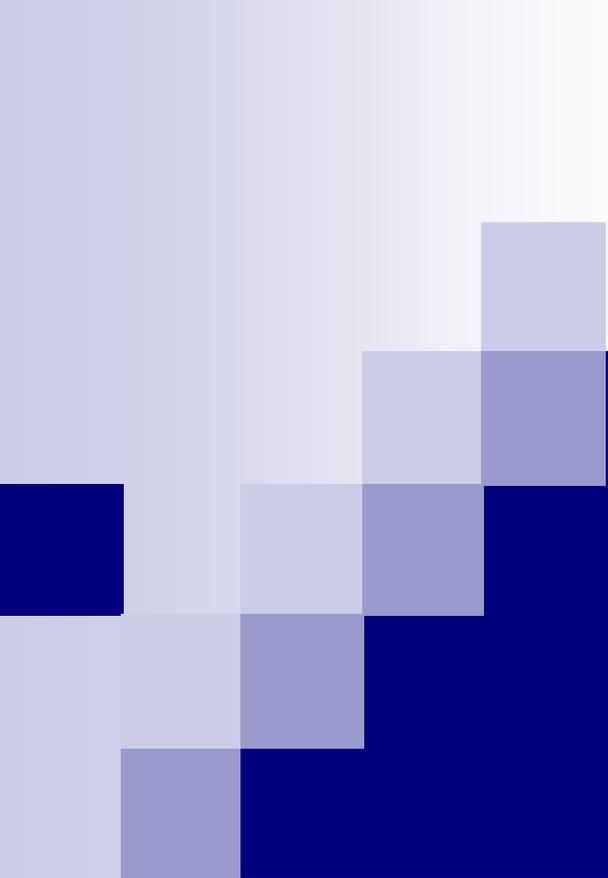
*  These do not exist at this point, but can be added to the PHIMT

Specialist
Minister

Introduction to PHIMT

Summary

- You should now be able to:
 - Explain what the PHIMT is and why it exists
 - Describe the capabilities of the PHIMT
 - Identify the advantages of using the tool
 - Explain the Authority for Multiple Disclosure Accounting
 - Identify the 14 Permitted Uses and Disclosures
 - Locate and describe the Disclosure Notification Letter
 - Describe the PHIMT terminology, user roles, and permissions
 - Explain the PHIMT Hierarchy



User Admin Functionality

User Admin Functionality

Objectives

- Upon completion of this lesson, you will be able to:
 - Obtain a User Admin account
 - Create user accounts
 - Setup a workflow
 - Setup a queue
 - Create requester favorites
 - Disable users
 - Transfer users

User Admin Functionality

Obtain a User Admin Account

- Requests for User Admins to be created must be routed to and approved by the Service Representative
- The Service Representative will route the approved request to the HIPAA Support Center
- The HIPAA Support Center will establish the User Admin account and provide the User Admin login information to the appropriate individual

User ID and Password Requirements

■ User ID:

- Assigned by the User Admin, usually first initial of the first name and complete last name (follow Service guidelines)
- Duplicate User Name not allowed by the application

■ Password:

- 8-15 characters long and must contain at least one
- Alphabetical uppercase character
- Alphabetical lower case character
- Arabic numeral (0, 1, 2, 3, 4)
- Non-alphanumeric special character (I.e. !, @, #, \$, etc.)

User Admin Functionality

Login Screen (1 of 3)



User Admin Functionality

Login Screen (2 of 3)

MHS PHIMT

THIS IS A DOD COMPUTER SYSTEM. THIS COMPUTER SYSTEM, WHICH INCLUDES ALL RELATED EQUIPMENT, NETWORKS, AND NETWORK DEVICES (SPECIFICALLY INCLUDING ACCESS TO THE INTERNET), ARE PROVIDED ONLY FOR OFFICIAL U.S. GOVERNMENT BUSINESS. DOD COMPUTER SYSTEMS MAY BE MONITORED BY AUTHORIZED PERSONNEL TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES. MONITORING INCLUDES "HACKER" ATTACKS TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM AGAINST USE BY UNAUTHORIZED PERSONS. DURING THESE ACTIVITIES, INFORMATION STORED ON THIS SYSTEM MAY BE EXAMINED, COPIED AND USED FOR AUTHORIZED PURPOSES AND DATA OR PROGRAMS MAY BE PLACED INTO THIS SYSTEM. THEREFORE, INFORMATION YOU PLACE ON THIS SYSTEM IS NOT PRIVATE. USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO OFFICIAL MONITORING OF THIS SYSTEM. UNAUTHORIZED USE OF A DOD COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE PROVIDED TO APPROPRIATE PERSONNEL FOR ADMINISTRATIVE, CRIMINAL, OR OTHER ACTION.

PRIVACY ACT WARNING

INFORMATION CONTAINED IN THIS SYSTEM IS SUBJECT TO THE PRIVACY ACT OF 1974 (5 U.S.C. 552A, AS AMENDED). PERSONAL INFORMATION CONTAINED IN THIS SYSTEM MAY BE USED ONLY BY AUTHORIZED PERSONS IN THE CONDUCT OF OFFICIAL BUSINESS. ANY INDIVIDUAL RESPONSIBLE FOR UNAUTHORIZED DISCLOSURE OR MISUSE OF PERSONAL INFORMATION MAY BE SUBJECT TO FINE OF UP TO \$5,000.



User Admin Functionality

Login Screen (3 of 3)



The login screen features the TRICARE logo on the left, which consists of three red wavy lines and a blue star. To the right is the official seal of the Department of Defense, United States of America, featuring an eagle with wings spread, holding an olive branch and arrows, with a shield on its chest. Below the logos, the text "MHS PHIMT" is displayed in blue. A red-bordered box contains the text: "You are logging into the production server. Information in this version will be retained." Below this, there are two input fields: "User Name:" and "Password:". A red arrow points to a "Login" button located below the password field. At the bottom, a red arrow points to the "Login" button with the text: "Enter your User Name and Password to logon."

T R I C A R E

MHS PHIMT

You are logging into the production server.
Information in this version will be retained.

User Name:

Password:

Login

Enter your User Name and Password to logon.

User Admin Functionality

Main Screen

Tuesday, June 28, 2005 [Logoff](#)

User Admin

Current User:
Scovel, Natalie
US TMA

My Profile
My Requests
My Worklist

■ [Switch organizations](#)

User Worklist

User Worklist

Activity Instance ID	Request Session ID	Activity ID	Source	Patient	Requester	Status	Creation Date
<i>There are no activities on your worklist</i>							

Naval Hospital Worklist

Activity Instance ID	Request Session ID	Activity ID	Source	Patient	Requester	Status	Creation Date
<i>There are no activities for this queue</i>							

Copyright © New Governance, Inc. 2000-2004, ALL RIGHTS RESERVED
Version: 2.27 build [0916]

User Admin Functionality

Create User Accounts

- The User Admin is responsible for adding users and assigning roles to the users within their organization
- The User Admin provides the user with their login information
- Determined by Service specific requirements or MTF requirements

User Admin Functionality

Workflow Setup

- Once a user has been added and their organization and user role is established, the User Admin can establish the workflow for that user's disclosures
- The workflow delineates the process by which requests are routed within the system
- Workflows should be set up so that a Regular Users work will be routed to a Privacy Specialist for approval or denial

User Admin Functionality

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 sets up queues
- 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

User Admin Functionality

Requester Favorites

- An organization can create a list of requester "favorites" that show up in the requester drop-down list box
- 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

User Admin Functionality

Disabling Users

- If a user transfers to another facility or separates from the Service, the User Admin needs to disable that individual's ability to access the tool
- You cannot delete users from the system
 - Future auditing
 - Disclosures tracking
 - Users are attached to records they created

User Admin Functionality

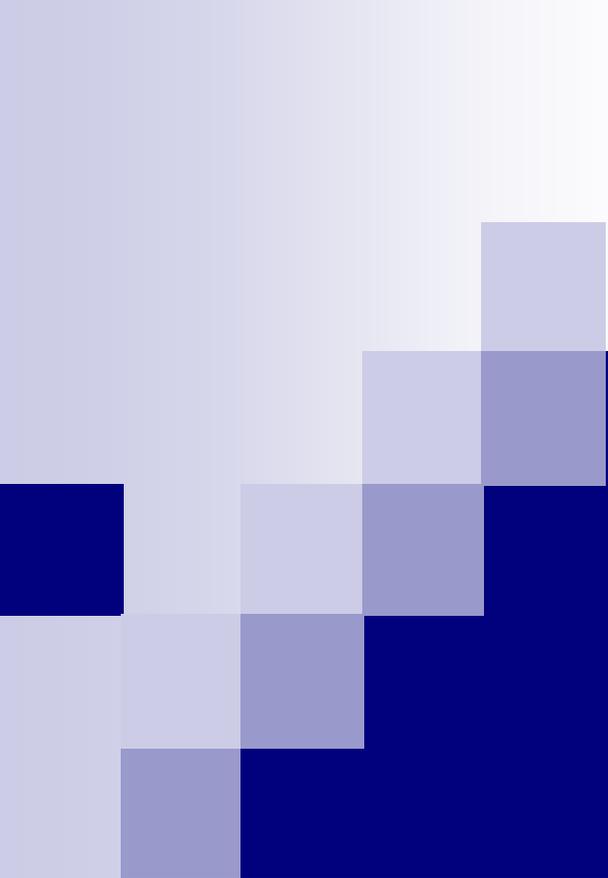
Transferring Users

- A transfer from one MTF to another can only be executed by the User Admin at the Service level
- If a user transfers to a new organization, the User Admin at the receiving location would initiate an action for the transfer according to Service requirements
- If a User transfers from one Service to another, please contact the HIPAA Support Center at
 - <https://hipaasupport.tricare.osd.mil>
- The User Admin can only search for users within their level of the hierarchy

User Admin Functionality

Summary

- You should now be able to:
 - Describe the process of obtaining a User Admin account
 - Create user accounts
 - Setup a workflow
 - Setup a queue
 - Create requester favorites
 - Disable users
 - Transfer users



Regular User Functionality

Regular User Functionality

Objectives

- Upon completion of this lesson, you will be able to:
 - Search for a patient
 - Explain the monthly MDR upload
 - Record a Request for Disclosure/Accounting of Disclosures
 - Identify the streamlined process for recording a disclosure

Regular User Functionality

Patient Search

- The user must search for a patient record in order to:
 - Track a disclosure
 - Identify an authorization or restriction
 - Track a complaint
- The user can search for a patient record using the Family Member Prefix Sponsor's SSN (FMP-SSSN) or the patient's name

Regular User Functionality

Patient Search- MDR Upload

- An upload of MDR demographic information is loaded into the PHIMT
 - There are monthly updates to the MDR data
 - Last Wednesday of every month
 - MDR data will be unavailable for 2 hours
 - 7:00 am- 9:00 am EST
 - PHIMT will still be available
- Due to the implementation of the MDR Data:
 - Search results are limited to 50 records
 - If more results are found, the user must narrow down their search by selecting additional search criteria
 - Example: The user can utilize the State search field to limit the search results

Regular User Functionality

Patient Search- MDR Upload (1 of 5)

- When searching for a patient's account, an error message will display if your search results in more than 50 matches

Friday, September 9, 2005 Patient Search Logoff

Patient User Admin Requests Requester

Current Patient:
Test, Osxehp
07/22/1934
FMP-SSSN:05-485268813

Patient Search
Error(s) have occurred: Too many results (over 50) match your criteria, please change your criteria and resubmit ...

Use the current person:

Name: Osxehp Test
SSN #: 934721013
Birth Date: 07-22-1934
Address: 123 Jon St., San Antonio, TX 76119-4505

- OR -

Search for another person:

FMP-SSSN (Family Member Prefix and Sponsor SSN (in xx-xxx-xx-xxxx format))

- - -

- OR -

by Name/State (Last) (First) (State)

, / -

- OR -

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

Regular User Functionality

Patient Search- MDR Upload (2 of 5)

- To narrow down the search results, the user can utilize the State search field

Friday, September 9, 2005 Patient Search [Logout](#)

Patient | User | Admin | Requests | Requester

Current Patient:
Test, Osxehp
07/22/1934
FMP-SSSN:05-485268813

Patient Search
Error(s) have occurred: Too many results (over 50) match your criteria, please change your criteria and resubmit ...

Use the current person:

Name: Osxehp Test
SSN #: 934721013
Birth Date: 07-22-1934
Address: 123 Jon St., San Antonio, TX 76119-4505

- OR -

Search for another person:

FMP-SSSN (Family Member Prefix and Sponsor SSN (in xx-xxx-xx-xxxx format))
[] - [] - [] - []

- OR -

by Name/State (Last) (First) (State)
Test [] / [] / TX

- OR -

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

Search

OK

Summary
Requests
Record Disclosure
Accounting Suspensions
Disclosure Restrictions
Authorization
Patient Profile

■ Patient Search

Regular User Functionality

Patient Search- MDR Upload (3 of 5)

- When accessing a patient account that has been imported from the MDR data, the record will be labeled as “New”

<input type="radio"/>	62137 03	Test, Dylan	652287824	2003-08-25	2510 Trinity Cir Apt A Colorado Springs, CO 80918-6939
<i>FMP-SSSN 03-553890603</i>					
<input type="radio"/>	62140 02	Test, Alexis	803949516	2003-11-25	4212 S Dowfield Dr Fayetteville, NC 28311-3742
<i>FMP-SSSN 02-318743051</i>					
<input type="radio"/>	6690 30	Test, Public Health	000000000	2004-03-16	123 Test Stree Arlington, CA 22222-2222 Undefined
<i>FMP-SSSN 30-000660000 (2004-03-16 to 2004-03-16)</i>					
<input type="radio"/>	62136 02	Test, David	804009456	2004-04-04	Cmr 464 Box 714 1/4 Cav A Trp Cmr 464 Box 714 1 4 Cav A Trp APO, AE 09226
<i>FMP-SSSN 02-493948027</i>					
<input type="radio"/>	38500 12	Test, Natalie	122444556	2005-01-25	5678 Yahoo St. Washington, DC 20123-4444
<i>FMP-SSSN 12-334558989 (2005-01-25 to 2005-01-25)</i>					
<input type="radio"/>	4942 20	Test, Test II	111990000		1411 Jeffrson David Arlington, VI 25896
<i>FMP-SSSN 20-111990000 (2004-02-24 to 2004-02-24)</i>					
<input type="radio"/>	4944 20	Test, Test III	999001111		111 New St. Colorado Springs, CO 80840 Undefined
<i>FMP-SSSN 20-999001111 (2004-02-24 to 2004-02-24)</i>					
<input checked="" type="radio"/>	new 65	Test, Daffy	876434985	1911-01-01	456 My St. Nowhere, MD 87654-9999
<i>FMP-SSSN 65-888887777</i>					

Select

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

Regular User Functionality

Patient Search- MDR Upload (4 of 5)

- All records that have been imported from the MDR data will be labeled with “Imported from TCL”

01/01/1911 FMP-SSSN:65- 888887777	* Name (Last) (First) (Middle) (Sr./Jr.) Test , Daffy
Summary Requests Record Disclosure Accounting Suspensions Disclosure Restrictions Authorization Notice Patient Profile Relationships Generate Form	* Type Patient
Patient Search	* SSN (in ###-##-#### format, enter '000-00-0000' if not known) 876 - 43 - 4985
	System ID (the identifier created by this system for the person) 67473
	* Birth Date (birth date in MM/DD/YYYY format) 01 / 01 / 1911
	Email (example: johnf@yahoo.com) <input type="text"/>
	* FMP-SSSN (Family Member Prefix and Sponsor SSN (in xx-xxxxxxxx format)) 65 - 888 - 88 - 7777
	Alternate Communication Instructions (special instructions to send correspondence to the person) <input type="text"/>
	Comments (general comments about or for the person) Imported from TCL
	<input type="button" value="Update"/>

Regular User Functionality

Patient Search- MDR Upload (5 of 5)

- Selecting the “New” patients account will import all data from the MDR
- The word “New” is replaced with the patient’s PHIMT ID

Friday, October 14, 2005 Patient Search Logoff

Patient User Admin Requests Requester

Current Patient:
Test, Daffy
01/01/1911
FMP-SSSN:65-88887777

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

■ Patient Search

Patient Search Results

Search Results for FMP-SSSN = [*65-77778888] (sorted by birth date)

ID	FMP	Name	SSN	Birth Date	Address
<input checked="" type="radio"/>	62503 65	Test, Goofy	217468400	1901-01-01	123 Your St. Anywhere, MD 87654-9999
<input type="radio"/>	67473 65	Test, Daffy	876434985	1911-01-01	456 My St. Nowhere, MD 87654-9999
<input type="radio"/>	62141 02	Test, Virginia	177308169	1939-12-27	12475 Highgate Ln Gloucester, VA 23061-2649
<input type="radio"/>	62138 00	Test, Test	323212312	1945-08-31	Undefined
<input type="radio"/>	17197 20	Test, Test	986899999	1950-02-03	Dsgfdsg Dfsgdfg, AL 20194
<input type="radio"/>	62135 00	Test, Test	217396639	1958-06-15	1234 Abckkk Fsgfgfg Test Ln., DC 20010
<input type="radio"/>	11870 20	Test, Bob	000000003	1962-12-22	200 Hospital Dr Augusta, GA 30905 Undefined
<input type="radio"/>	62139 00	Test, Weekend	266090002	1965-10-01	Undefined
<input type="radio"/>	59878 30	Test, Cam L	999887777	1966-05-28	44 Hockey St. Nowhere, MT 59401

Note: If there is no address in the PHIMT, the address from the MDR Data will be used. If the address in the MDR does not match the address in the PHIMT, the address in the PHIMT will be the default address, to ensure that Alternative Addresses are kept valid.

Regular User Functionality

Recording a Request

- An individual has a right to receive an accounting of disclosures of PHI made by a CE in the 6 years prior to the date that the accounting is requested
 - DoD 6025.18-R Chapter 13
- Regular Users can record a request for:
 - A disclosure
 - An accounting of disclosures
- Only Privacy Specialists can approve or deny the request

Recording a Request- Streamlined Process

- The Streamlined Disclosure process was requested by the field to:
 - Decrease the number of steps for recording a disclosure request
 - Eliminate optional fields that were not required
- Users can still record a disclosure request using the Wizard
- Disclosure descriptions were added to the PHIMT to make it easier for the user to select the appropriate Disclosure Type

Recording a Request- Simple Disclosure vs. Disclosure Wizard

- The Simple Disclosure radio button includes two screens:
 - Select Patient
 - Disclosure Details

- The Disclosure radio button (Wizard) includes 5 screens:
 - Select Patient
 - Select Requester
 - Request Details
 - Disclosure Details
 - Request Action

Regular User Functionality

Recording a Request- Simple Disclosure

■ The Simple Disclosure

Thursday, February 16, 2006 [Patient Search](#) [Logoff](#)

Patient User Requests Requester

Current Request:
None

Create New Request

Select Request Type

- Disclosure
- Disclosure Accounting
- Simple Disclosure Request

Next

■ Create New Request
■ Search for a Request

Regular User Functionality

Recording a Request

- Required fields are marked with an asterisk

*** Patient** *(the Patient to whom the disclosure applies)*
Name: Samuel Kirby
SSN #: 234453456
Birth Date: 10/12/1978
Address: 15 King St. Alexandria, VA 22301

*** Requester** *(the organization or person requesting the disclosure)*
Name: Kirby, Samuel
Address: 15 King St., Alexandria, VA 22301
Phone:
Contact Person:

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

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

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

*** Recipient** *(the organization or person where the disclosure went)*
Name: Kirby, Samuel
Address: 15 King St., Alexandria, VA 22301
Phone:
Contact Person:

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

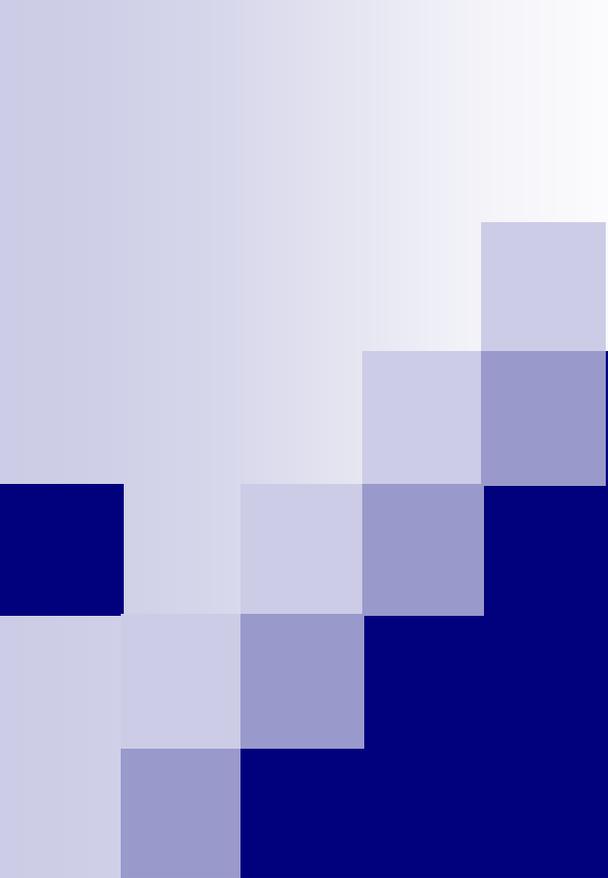
Disclosure Description *(a read-only description and example of the disclosure type selected above)*

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

Regular User Functionality

Summary

- You should now be able to:
 - Search for a patient
 - Explain the monthly MDR upload
 - Record a Request for Disclosure/Accounting of Disclosures
 - Identify the streamlined process for recording a disclosure



Privacy Specialist Functionality

Privacy Specialist Functionality

Objectives

- Upon completion of this lesson, you will be able to:
 - Approve/Deny a Request for Disclosure/Accounting of Disclosures
 - Record a Disclosure/Accounting of disclosures
 - Create Alternative Communication
 - Amend a disclosure
 - Create a suspension
 - Record a restriction
 - Generate correspondence
 - Create/sign/revoke an authorization
 - Record a complaint

Approving/Denying a Request

- Once a request for an accounting of disclosures has been recorded, a Privacy Specialist must approve or deny the request
- Once routed, the request will display in the Privacy Specialist's worklist
- Once a Regular User routes a request for disclosure to the Privacy Specialist, the request will display in the Privacy Specialist's worklist
- The Privacy Specialist will then approve or deny the request

Privacy Specialist Functionality

Recording a Disclosure

- The Privacy Specialist will record the disclosure using the same steps that the Regular User would use
 - Privacy Specialists have the ability to record and approve disclosures in one step
- This eliminates the two step process of recording the request, routing it to their work list, and then approving it

Creating Alternative Communication

- A CE shall permit individuals to request and shall accommodate reasonable requests by individuals to receive communications of PHI from the covered health care provider by alternative means or at alternative locations
 - -DoD 6025.18-R C10.2.2
 - -164.522
- An alternative address can only be created by a Privacy Specialist
- 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
- Should be P&P to support this functionality

Amending Disclosures

- 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
 - The disclosure was made incorrectly

Creating a Suspension

- The CE shall temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official...DoD 6025.18-R
C13.1.2.1
- Two types of disclosures can be suspended:
 - Law enforcement purposes
 - Health oversight activities
- Privacy Specialists have the ability to enter an accounting suspension in two ways
 - Specific disclosure (Recommended)
 - Type of disclosure
- Once entered, the suspension can be viewed by all users

Privacy Specialist Functionality

Recording a Restriction

- DoD 6025.18-R Chapter 10 describes the rights to request privacy protection for protected health information
 - CE is not required to agree to such requests
 - Requests may be made orally or in writing, but must be documented
 - CE must provide a response to the individual
- Privacy Specialists can record and approve or deny requests for disclosure restrictions
 - Once approved or denied, a letter with an explanation can be generated

Privacy Specialist Functionality

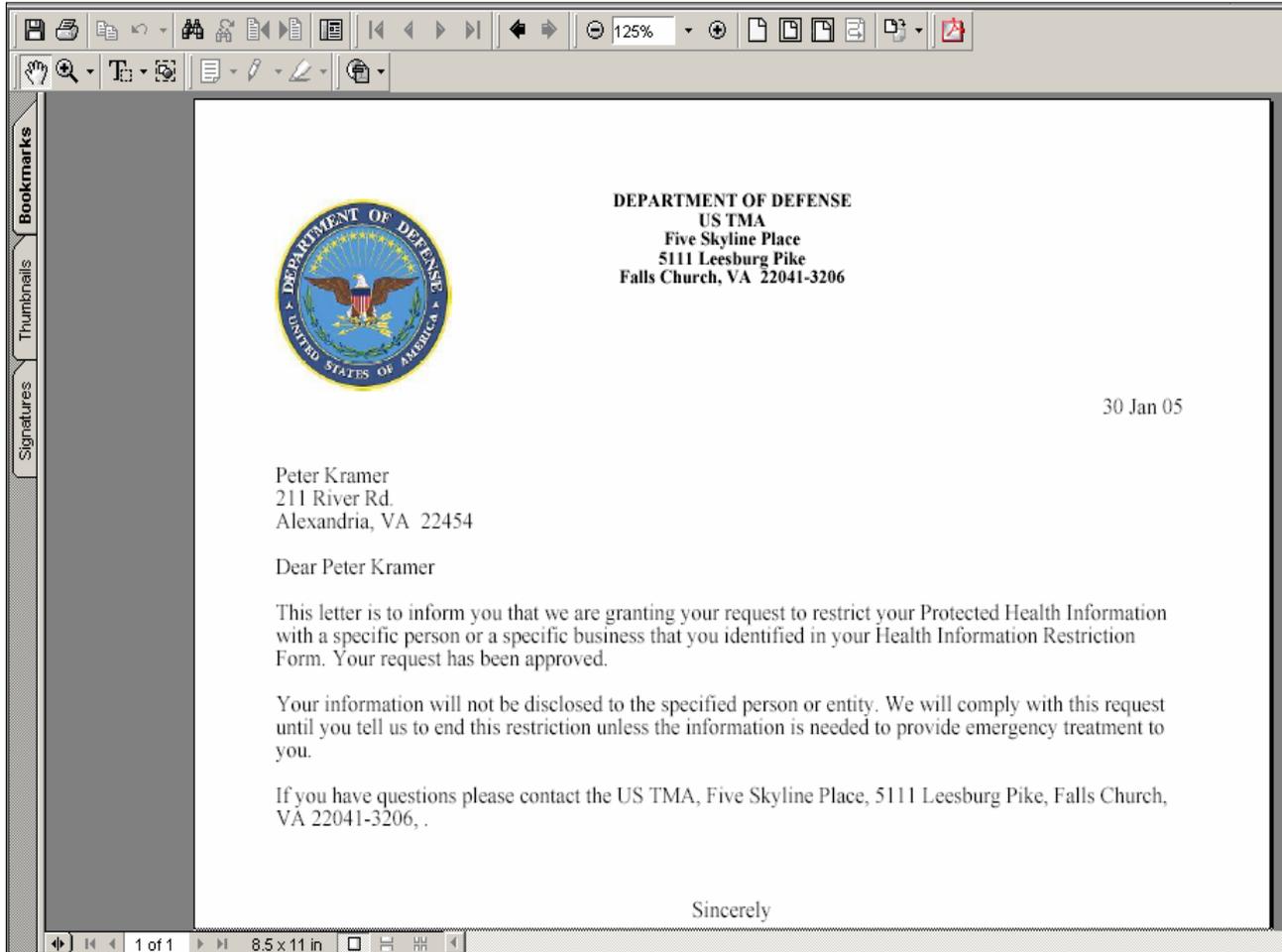
Generating Correspondence (1 of 2)

- 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

Privacy Specialist Functionality

Generating Correspondence (2 of 2)

■ The Approval letter



The screenshot shows a PDF viewer window with a toolbar at the top and a sidebar on the left containing 'Bookmarks', 'Thumbnails', and 'Signatures'. The main content area displays a letter from the Department of Defense. The letterhead includes the Department of Defense seal and the following text: 'DEPARTMENT OF DEFENSE', 'US TMA', 'Five Skyline Place', '5111 Leesburg Pike', and 'Falls Church, VA 22041-3206'. The date '30 Jan 05' is printed on the right. The recipient's address is 'Peter Kramer, 211 River Rd., Alexandria, VA 22454'. The letter body begins with 'Dear Peter Kramer' and contains three paragraphs of text regarding a request to restrict Protected Health Information. The letter concludes with 'Sincerely'.

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

30 Jan 05

Peter Kramer
211 River Rd.
Alexandria, VA 22454

Dear Peter Kramer

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

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

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

Sincerely

Creating an Authorization (1 of 2)

- The MHS uses the DD Form 2870 (Authorization for Disclosure of Medical or Dental Information)
- Authorizes an individual or organization to disclose a patient's medical or dental information
- Once an authorization has been created, the DD Form 2870 can be downloaded from the Privacy Office website, or from the DoD Forms website
- Can be generated using PHIMT

Privacy Specialist Functionality

Creating an Authorization (2 of 2)

- DD Form 2870 in Adobe Acrobat format

The image shows a screenshot of an Adobe Acrobat window displaying a form titled "AUTHORIZATION FOR DISCLOSURE OF MEDICAL OR DENTAL INFORMATION". The form is filled out with patient information and treatment details. The Acrobat interface includes a toolbar at the top with various navigation and editing tools, and a sidebar on the left with "Bookmarks", "Thumbnails", and "Signatures" sections.

AUTHORIZATION FOR DISCLOSURE OF MEDICAL OR DENTAL INFORMATION		
The purpose of this form is to provide the MTF/DTF/TRICARE Health Plan with a means to request the use and/or disclosure of an individual's protected health information. Guidelines regarding use of this form are contained in DOD Regulation 6025.18-R.		
This form will not be used for authorization to disclose alcohol or drug abuse patient information from medical records or for authorization to disclose information from records of an alcohol or drug abuse treatment program. In addition, any use as an authorization to use or disclose psychotherapy notes may not be combined with another authorization except one to use or disclose psychotherapy notes. Privacy Act of 1974 applies		
PATIENT DATA		
Name (Last, First, MI) Smith, Joe, J	Date of Birth 07-05-1968	Patient SSN 121131414
Period of Treatment 01-11-2005- 01-11-2005	Type of Treatment: Outpatient	
DISCLOSURE		
I authorize <u>USADC-Hospital</u> (Name of MTF/DTF) to release my patient information to recipient: <u>1100 Main Street</u> <u>Woodbridge, VA 22321</u>	Reason for Request/Use of Medical Information: Personal Use, patient authorizes his brother to have a copy of entire medical record.	
Information to be Released: entire medical record		

Signing/Revoking an Authorization

Signing an Authorization:

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

Revoking an Authorization:

- DoD 6025.18-R, Section C5.2.5
- Privacy Specialists can revoke an authorization when instructed by a patient in writing
 - Except if:
 - The CE has taken action in reliance thereon
 - Insurance coverage

Recording a Complaint (1 of 4)

- Individuals have the right to make a complaint concerning TMA's implementation and compliance with the rule
- You must provide that process and make it available
- You must document all complaints and their disposition
- You must not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for exercising their rights or obligations

Recording a Complaint (2 of 4)

- Privacy/Security Officers (PO/SO) are able to track complaints using the PHIMT
- Allows for easy tracking and documentation of complaints in one centrally managed application
- PO/SO can quickly create complaint reports
- Complaint documentation is stored and maintained in a centrally managed database

Privacy Specialist Functionality

Recording a Complaint (3 of 4)

Monday, June 6, 2005 Patient Search | Logoff

Patient | User | Admin | Requests | Requester

Current Request: Complaint

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

Create New Request
Search for a Request

Complaint Details

Complainant *(the person who is making the complaint)*
Name: Patty Smith

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)*
05/23/2005

Subject *(the subject of the complaint)*
Request for copy of medical record

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

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

Privacy Specialist Functionality

Recording a Complaint (4 of 4)

Complaint Description *(the description of the complaint)*

The medical record contained information belonging to another beneficiary. Priscilla Smith's information was in Patty Smith's record. Patty Smith is concerned that her information could also be misplaced.

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)*

Back

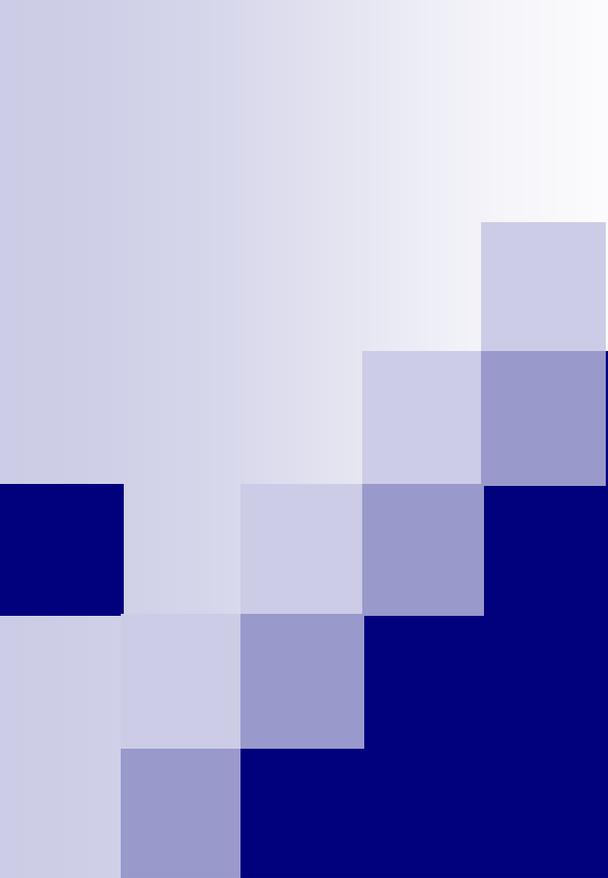
Next



Privacy Specialist Functionality

Summary

- You should now be able to:
 - Approve/Deny a Request for Disclosure/Accounting of Disclosures
 - Record a Disclosure/Accounting of Disclosures
 - Create Alternative Communication
 - Amend a disclosure
 - Create a suspension
 - Record a restriction
 - Generate correspondence
 - Create/sign/revoke an authorization
 - Record a complaint



Administrative Summary Reports

Administrative Summary Reports

Objectives

- Upon completion of this lesson, you will be able to:
 - View Administrative Summary Reports
 - Interpret the report data

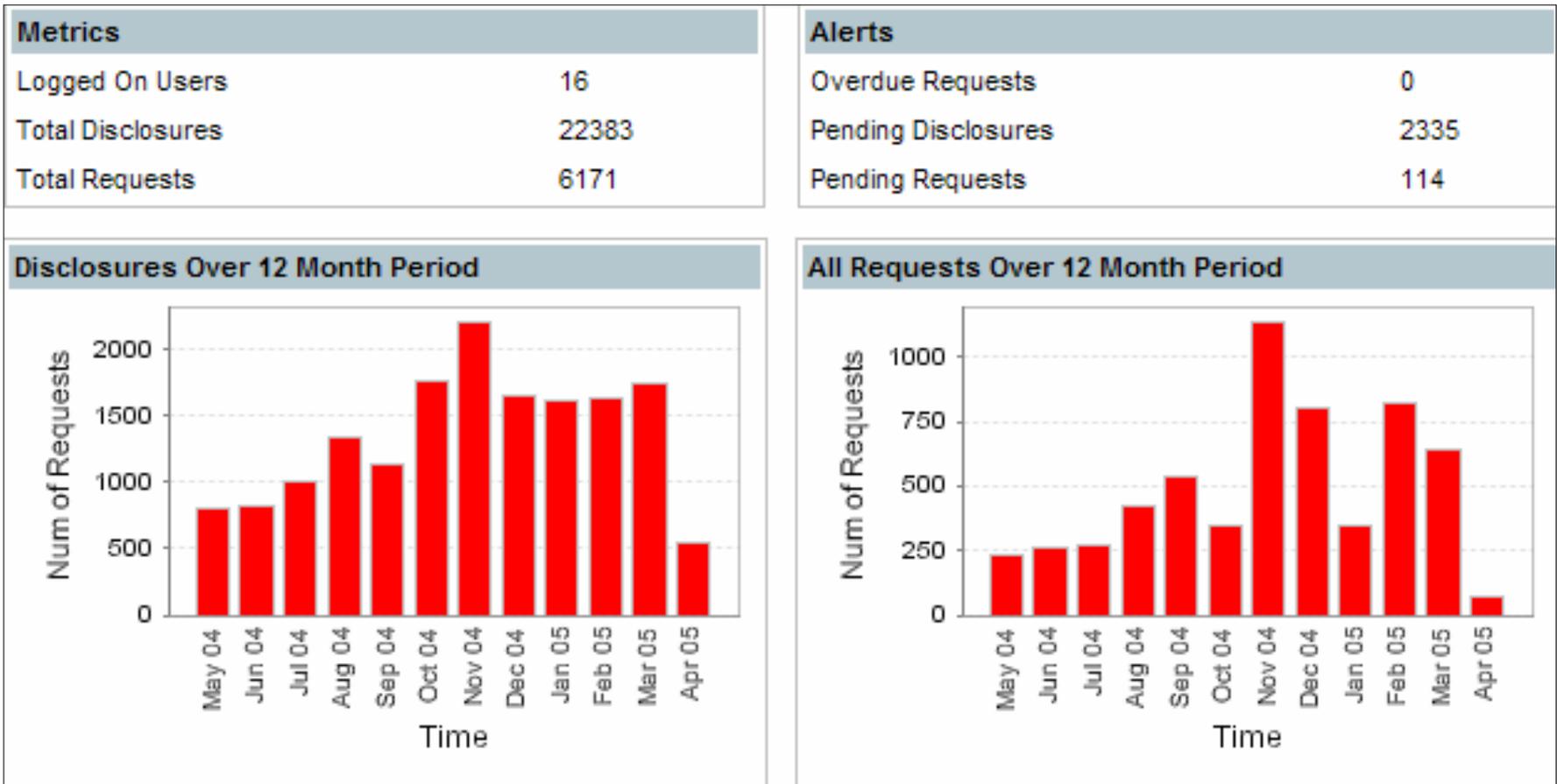
Administrative Summary Reports

Report Capabilities

- 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
- Performed by User Admins and Privacy Specialists
- PHIMT can run several types of reports:
 - Disclosures over a 12 month period
 - All requests by type
 - All requests over a 12 month period
 - Top recipients of disclosures
 - Top requesters for all requests
 - Number of recorded complaints

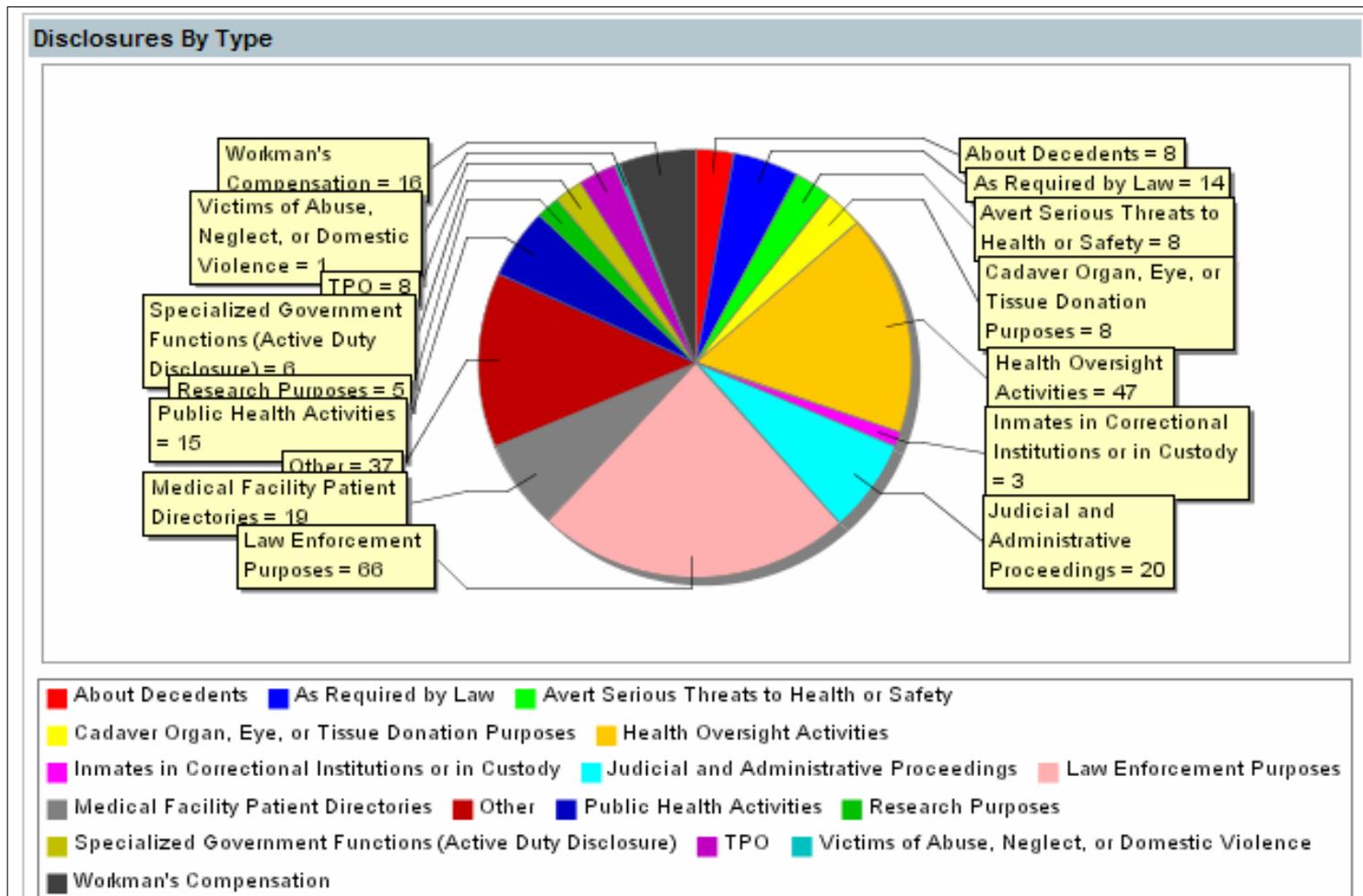
Administrative Summary Reports

Total Number of Disclosures and Requests



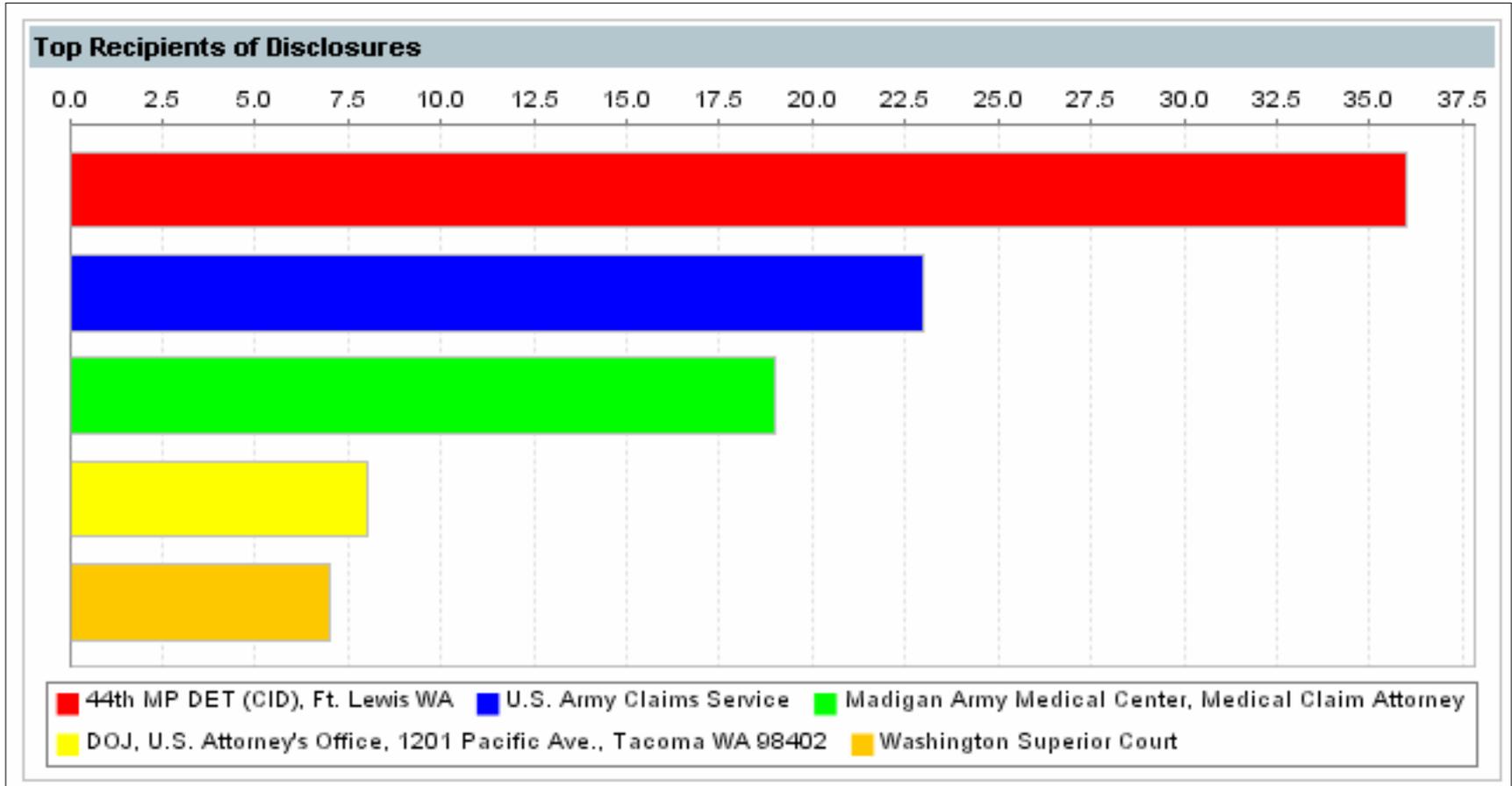
Administrative Summary Reports

Disclosures by Type



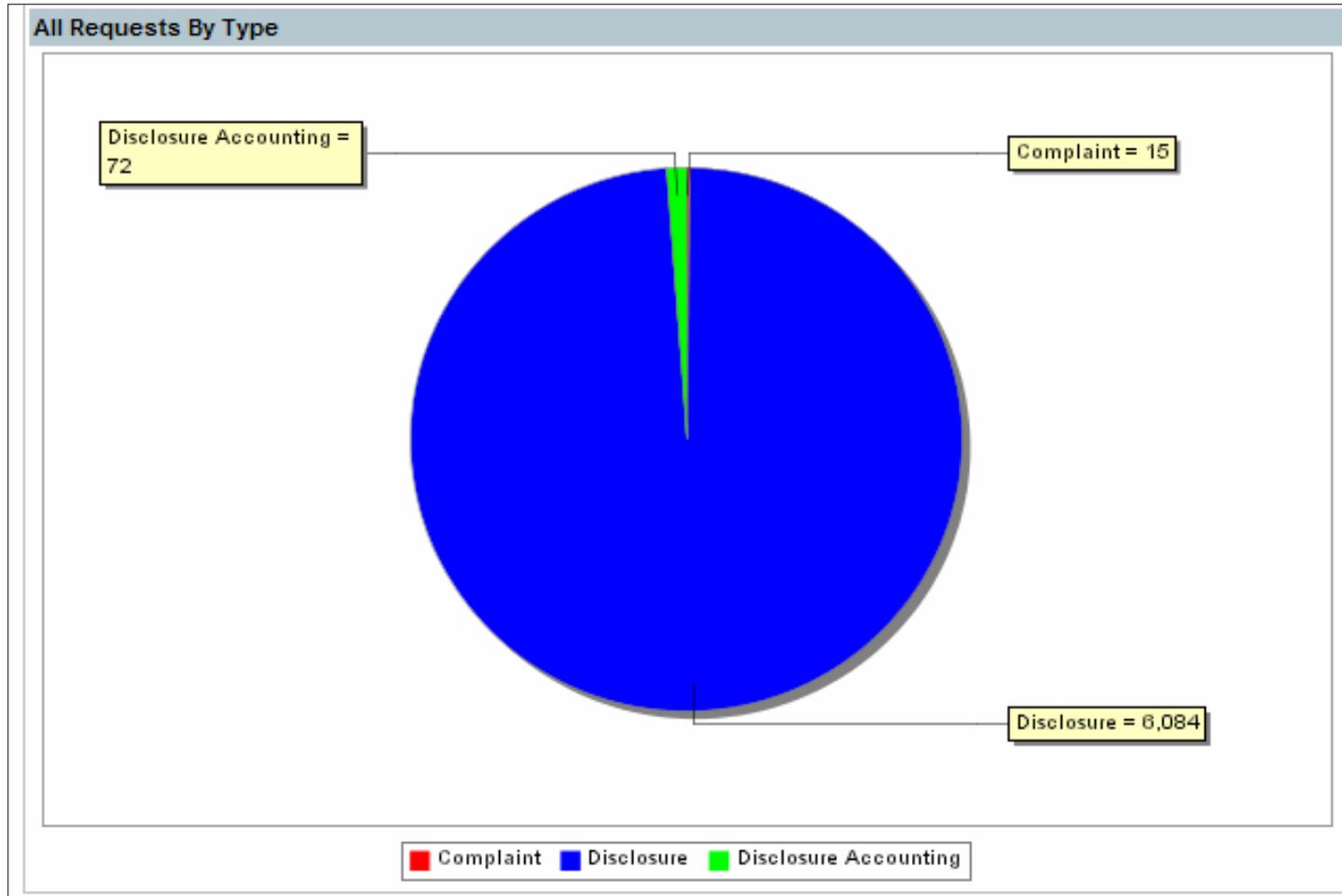
Administrative Summary Reports

Top Recipients of Disclosures



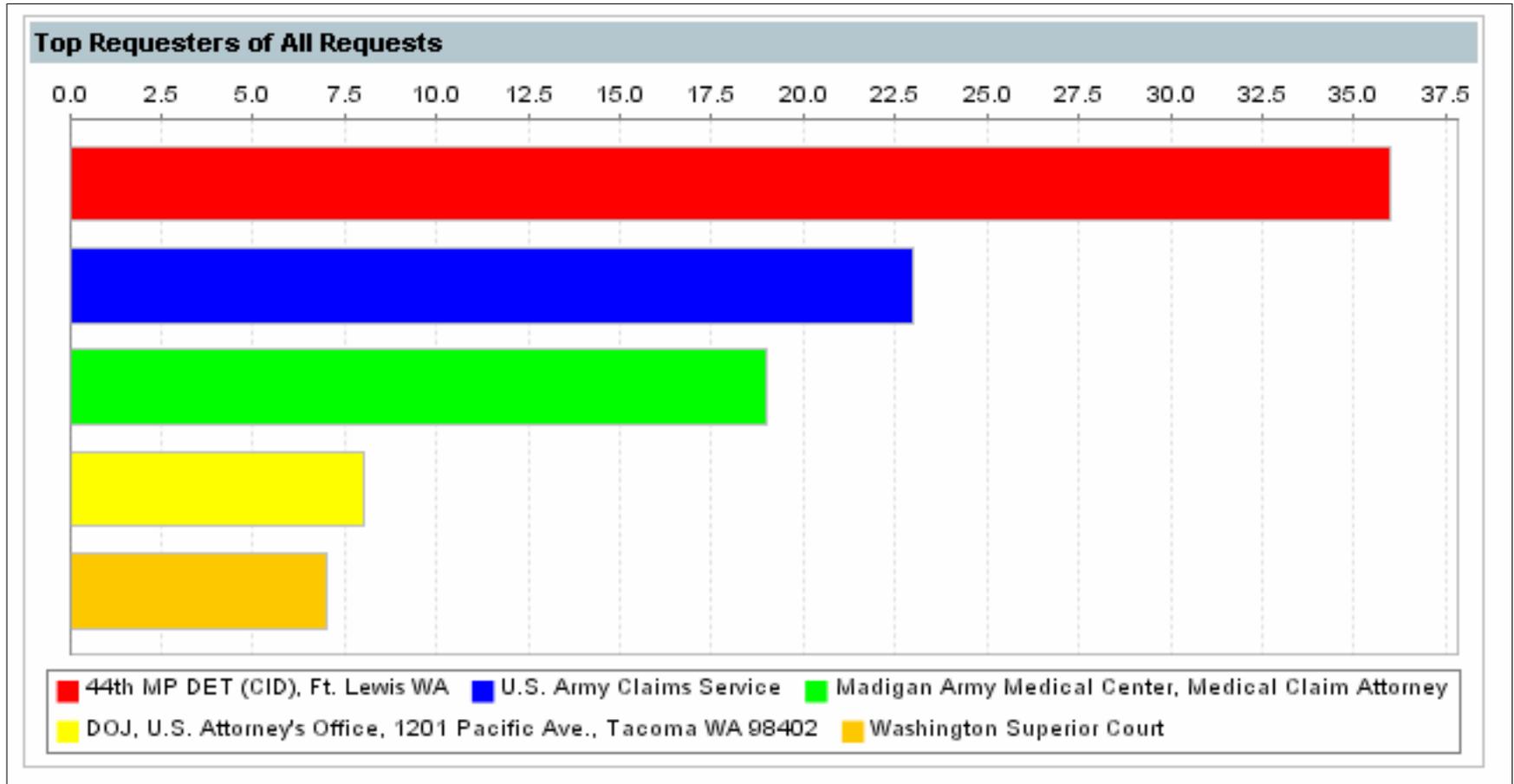
Administrative Summary Reports

All Requests by Type



Administrative Summary Reports

Top Requesters of All Requests



Administrative Summary Reports

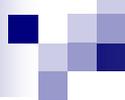
Summary

- You should now be able to:
 - View Administrative Summary Reports
 - Interpret the report data

PHIMT

Implementing PHIMT At Your Facility

- Ensure you have local policies and procedures in place for accounting of disclosures in the PHIMT
- Make sure your team is trained on how to use the PHIMT
 - Review presentations and manuals (TMA HIPAA Website)
 - Attend WebEx sessions
 - Utilize the PHIMT Training Server
 - Obtain a training account from the HIPAA Support Center
 - <https://trainingphimt.tricare.osd.mil/hipaax/>
- Ensure effective turnover of Regular Users



PHIMT

Tool Enhancements

- Multiple Disclosure Feature
- Uploading documents to disclosures
- Summary Reports

Tool Enhancements- Multiple Disclosure (1 of 3)

Monday, April 9, 2007 Patient Search Logoff

Patient User Admin Requests Requester

Current Request:
Simple Disclosure Request

■ Create New Request
■ Search for a Request

Select Patient (1) Disclosure Details (2)

Disclosure Details

Fields marked with an asterisk (*) are required.

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

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

* Requester (the organization or person requesting the disclosure)

Name:
Address:
Phone:
Contact Person:

Tool Enhancements- Multiple Disclosure (2 of 3)

Monday, April 9, 2007 Patient Search Logoff

Patient User Admin Requests Requester

Current Request:
Simple Disclosure Request

1 Select Patient 2 Disclosure Details

- Create New Request
- Search for a Request

Disclosure Details

Fields marked with an asterisk (*) are required.

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

* Disclosure Frequency (the frequency, periodicity, or number of disclosures made)
 Single Disclosure Multiple Disclosures for the same Purpose
Occurs once [N/A] or [0] times from [] to []

* Requester (the organization or person requesting the disclosure)

Name:
Address:
Phone:
Contact Person:

Tool Enhancements- Multiple Disclosure (3 of 3)

* Disclosure Type *(the type of disclosure)*

Not Selected

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

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

* Origin Organization *(where the disclosure originated)*

US TMA

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

Undefined

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

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

Complete Health Record(s)

Tool Enhancements- Uploading Documents to Disclosures (1 of 2)

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

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

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

Please select a file you wish to attach

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

Please select a file you wish to attach

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

Please select a file you wish to attach

Action *(action for this request)*

Route to Privacy Specialist ▼

Tool Enhancements- Uploading Documents to Disclosures (2 of 2)

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

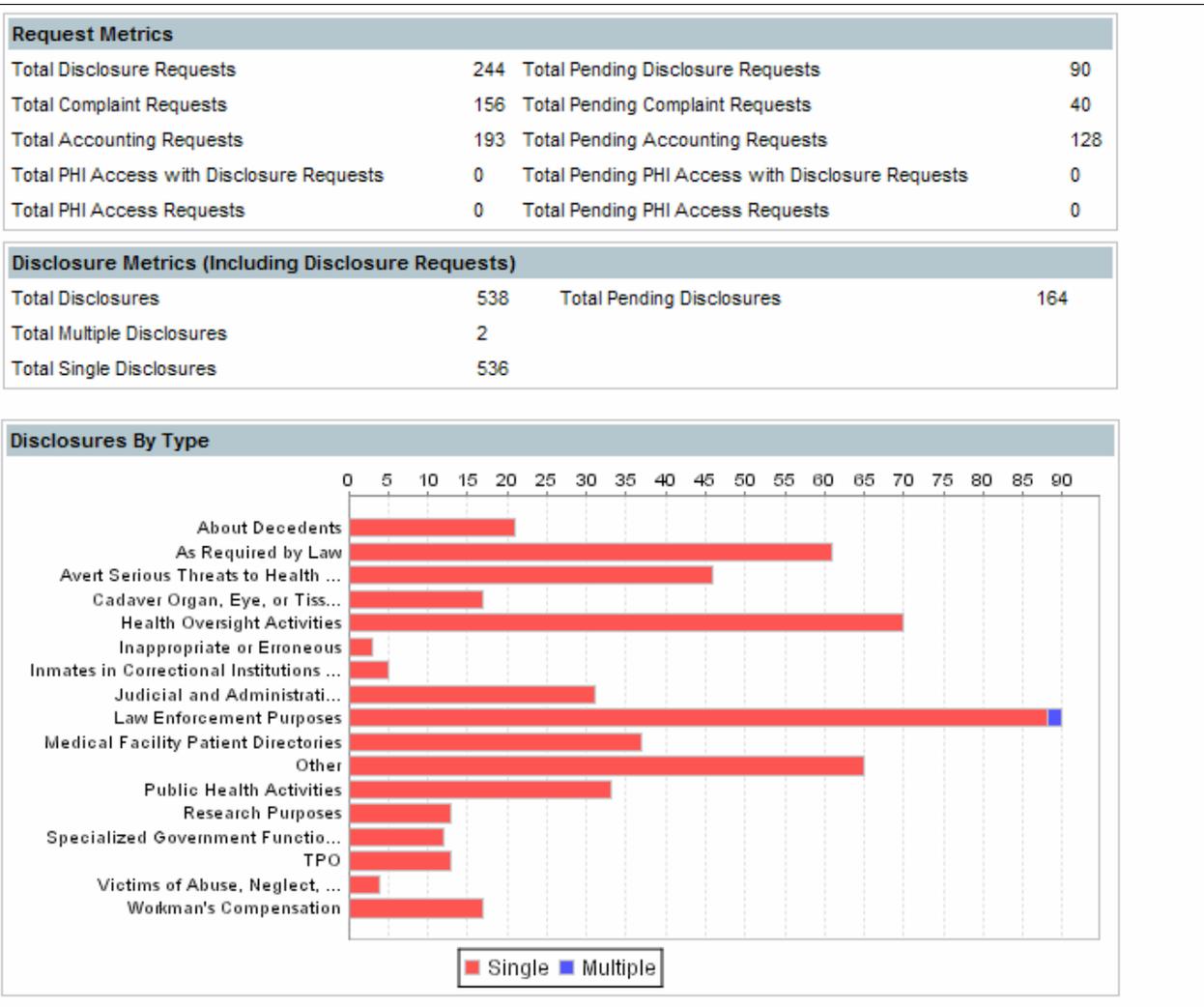
Improper Disclosure Description *(the details about the improper disclosure)*

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

Associated Documents

ID	Date	Title
868	04/09/2007	Test Doc

Tool Enhancements- Summary Reports



Presentation Summary

- You should now be able to:
 - Identify the use of the PHIMT in meeting the Accounting of Disclosures requirement of the HIPAA Privacy Rule
 - Describe the necessary policies and procedures
 - Describe the user roles and responsibilities within the PHIMT
 - Describe and interpret the data that the PHIMT can provide for compliance measurement
 - Implement PHIMT at your facility
 - Identify the latest tool enhancements

Resources

- DoD 6025.18-R, “DoD Health Information Privacy Regulation”, January 2003
- DoD 8580.X-R, DoD Health Information Security Regulation (Draft)
- <http://www.tricare.osd.mil/tmaprivacy/HIPAA.cfm>
- <http://www.tricare.osd.mil/tmaprivacy/Mailing-List.cfm> to subscribe to the TMA Privacy Office E-News
- <https://hipaasupport.tricare.osd.mil> for tool related questions
- Privacymail@tma.osd.mil for subject matter questions
- Service HIPAA Representatives