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

● Upon completion of this training you should 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 and perform all Privacy Specialist functionality
  – Describe and interpret the data that the PHIMT can provide for compliance measurement
  – Implement PHIMT at your facility
Introduction to PHIMT
Introduction to PHIMT

Objectives

- Upon completion of this training you should 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
  - Identify the 14 Permitted Uses and Disclosures
  - Describe the PHIMT terminology, user roles, and permissions
  - Explain the PHIMT Hierarchy
Introduction to PHIMT

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 Defense Health Agency (DHA)
  - Deployed in October 2003 with a series of training supporting the deployment to the Military Treatment Facilities (MTFs)
  - Centrally managed application that is accessed via the Internet
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
- The 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, Defense Health Agency provides an electronic disclosure-tracking tool
Introduction to PHIMT

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
Introduction to PHIMT

Advantages of the PHIMT

- Consolidates multiple tasks into one electronic environment
- Web based, centrally managed system
- Over 2000 users worldwide
- Protects the data
  - Allows for role-based access in maintaining the records and accessing patient information
  - DISA Protected Enclave
  - Defense Information Assurance Certification and Accreditation Process (DIACAP) certified
- Pre-populated drop-down fields
- Streamlined disclosure process
- Multiple Disclosure Accounting
Introduction to PHIMT

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
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

Key PHIMT Terminology

- **User** - an individual assigned to an organization within the tool

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

- **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
Introduction to PHIMT

User Roles and Permissions

- **User Admin** is a local admin for an MTF or a designated Service. This role may 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*
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
- Identify the 14 Permitted Uses and Disclosures
- Describe the PHIMT terminology, user roles, and permissions
- Explain the PHIMT Hierarchy
Privacy Specialist Functionality
Privacy Specialist Functionality
Objectives

- Upon completion of this training you should be able to:
  - Perform the Patient Search
  - Approve/Deny a Request for Disclosure/Accounting of Disclosures
  - Record a Disclosure/Accounting of disclosures
  - Amend a disclosure
  - Create a suspension
  - Record a restriction
  - Generate correspondence
  - Create/sign/revoke an authorization
  - Record a complaint
Privacy Specialist Functionality

Common Access Card

- The PHIMT is Common Access Card (CAC) enabled
- All users must have a CAC in order to login to the PHIMT
Privacy Specialist Functionality
Patient Search (1 of 4)

The first step of all patient activities in the PHIMT is the patient search

1. Select the Patient Tab
2. Enter the patient search criteria
3. Click on the Search button
NOTE: The search limitation within the PHIMT is 600 records. This means that if your search results in over 600 records you must narrow your search.
Privacy Specialist Functionality

Patient Search (3 of 4)

4. Enter additional search criteria (if applicable)
5. Select the patient from the Patient Search Results screen

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

Patient Search (4 of 4)

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

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
Privacy Specialist Functionality
Approving/Denyng a Request (1 of 4)

- 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.

**NOTE:** Those disclosures recorded by the Privacy Specialist 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 the Privacy Specialist’s worklist for later action.
Privacy Specialist Functionality

Approving/Denying a Request (2 of 4)

1. Select the User Tab
2. Select the My Worklist hyperlink
3. Select the Edit hyperlink for the disclosure you want to approve

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
Privacy Specialist Functionality
Approving/Denying a Request (3 of 4)

4. Select Approved from the Activity Status drop-down box
5. Click on the Update button

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

Approving/Denying a Request (4 of 4)

- 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 request is no longer shown in your User Worklist.

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

Recording a Disclosure (1 of 9)

- 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 the request
Privacy Specialist Functionality

Recording a Disclosure (2 of 9)

1. Select the Patient Tab
2. Enter the patient search criteria
3. Click on the Search button
4. Select the patient from the Patient Search Results screen
• The Patient Summary screen appears

**NOTE:** The steps 1-5 for recording a disclosure are the same as steps 1-5 in the Patient Search section. Refer to the Patient Search section for screen displays of steps 1-5
Privacy Specialist Functionality
Recording a Disclosure (3 of 9)

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

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
6. Select the Disclosure Frequency radio button
7. Click on the Change button to change or update the requester

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
Privacy Specialist Functionality
Recording a Disclosure (5 of 9)

8. Select the requester

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
9. Record the Disclosure details: requester authority, form, date, recipient, and disclosure type

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

**NOTE:** All required fields are marked with an asterisk

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

---

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
11. Scroll down the screen and enter: disclosure date, origin organization, disclosure purpose, and PHI description

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
Privacy Specialist Functionality
Recording a Disclosure (8 of 9)

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

Recording a Disclosure (9 of 9)

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

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

Amending Disclosures (1 of 5)

- A Privacy Specialist is 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
Privacy Specialist Functionality
Amending Disclosures (2 of 5)

1. Select the Patient Tab
2. Search for and select the patient

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
Privacy Specialist Functionality
Amending Disclosures (3 of 5)

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

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
Privacy Specialist Functionality
Amending Disclosures (4 of 5)

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

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

Amending Disclosures (5 of 5)

The Record Disclosure screen will display
5. Scroll to the bottom of the screen and place a check in the Improper Disclosure checkbox
6. Enter a description of the Improper Disclosure and mitigation
7. Click on the Update button

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

Creating a Suspension (1 of 5)

- 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
Creating a Suspension (2 of 5)

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

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
Privacy Specialist Functionality
Creating a Suspension (3 of 5)

3. Select the Specific Disclosure hyperlink

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
Privacy Specialist Functionality
Creating a Suspension (4 of 5)

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*

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
Privacy Specialist Functionality
Creating a Suspension (5 of 5)

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

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

Recording a Restriction (1 of 4)

- DoD 6025.18-R Chapter 10 describes the rights to request privacy protection for PHI
  - The CE is not required to agree to such requests
  - Requests may be made orally or in writing, but must be documented
  - The 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

Recording a Restriction (2 of 4)

1. Search for and select a patient record
2. Select the Disclosure Restrictions hyperlink

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
Privacy Specialist Functionality
Recording a Restriction (3 of 4)

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

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
Privacy Specialist Functionality
Recording a Restriction (4 of 4)

4. Enter the Disclosure Restriction details: disclosure type, start and end date, restriction destination (to whom information is being restricted) and details
5. Select Approved or Denied from the Outcome drop-down box
6. Click on the Save button

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

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
Privacy Specialist Functionality
Creating an Authorization (1 of 5)

- The MHS uses the DD Form 2870 (Authorization for Disclosure of Medical or Dental Information)
- It 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
- The form can also be generated using PHIMT
Privacy Specialist Functionality
Creating an Authorization (2 of 5)

1. Select the Patient Tab
2. Search for and select the patient record
3. Select the Authorization hyperlink

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
4. Select the Authorization Type from the drop-down box
5. Enter the Authorization Details: reason for request, releasing organization, and recipient

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
Privacy Specialist Functionality
Creating an Authorization (4 of 5)

6. Scroll down the screen and enter: authorization start and expiration date, treatment type, and treatment start and end date
7. Place a check in the Generate Authorization checkbox
8. Click on the Save button

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

Signing an Authorization (1 of 3)

- 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
Privacy Specialist Functionality
Signing an Authorization (2 of 3)

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

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
Privacy Specialist Functionality
Signing an Authorization (3 of 3)

2. Scroll to the bottom of the page to the Signed Status box
3. Place a check in the Signed Status checkbox
4. Select the date and the authorizing person’s identity from the drop-down box
5. Click on the Update button
Privacy Specialist Functionality
Revoking an Authorization (1 of 3)

- 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
    - The authorization is for insurance coverage
Privacy Specialist Functionality
Revoking an Authorization (2 of 3)

1. Select the Authorization ID hyperlink

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
Privacy Specialist Functionality
Revoking an Authorization (3 of 3)

2. Scroll to the bottom of the screen to the Revoked Status box
3. Place a check in the Revoked check box
4. Select the date and the revoking person’s identity in the drop-down box
5. Click on the Update button

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

Recording a Complaint  (1 of 9)

- Individuals have the right to make a complaint concerning DHA's implementation and compliance with the HIPAA Privacy 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
Privacy Specialist Functionality
Recording a Complaint (2 of 9)

- Privacy/Security Officers are able to track complaints using the PHIMT
- The PHIMT allows for easy tracking and documentation of complaints in one centrally managed application
- Privacy/Security Officers can quickly create complaint reports
Privacy Specialist Functionality
Recording a Complaint (3 of 9)

1. Select the Requests Tab
The Create New Request Screen will appear

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
Privacy Specialist Functionality
Recording a Complaint (4 of 9)

2. Click the Complaint radio button
3. Click on the Next button
Privacy Specialist Functionality
Recording a Complaint (5 of 9)

4. Enter Patient Search criteria
5. Click on the Search button
Privacy Specialist Functionality
Recording a Complaint  (6 of 9)

6. Select the Patient
The Complainant Details Screen will appear

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
Privacy Specialist Functionality
Recording a Complaint (7 of 9)

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

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

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
9. To attach any documents, type in the document title
10. Click on the Browse button to attach the file
11. Click on the Next button

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
12. Select the appropriate action from the drop-down box
13. Click on the Save button

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

Summary

- You should now be able to:
  - Perform the Patient Search
  - Approve/Deny a Request for Disclosure/Accounting of Disclosures
  - Record a Disclosure/Accounting of disclosures
  - 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 training you should be able to:
  – Run Administrative Summary Reports
  – 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 Privacy Specialists
Administrative Summary Reports

1. Select the Admin Tab
2. Select the Administrative Summary hyperlink

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
3. Select your Organization from the drop-down box

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

Summary

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

- Responsible for:
  - Creating user accounts
  - Updating user accounts
  - Assisting users with questions and/or issues

- Contact Information
  - mhssc@timpo.osd.mil
  - CONUS: (800) 600-9332
  - OCONUS: visit the MHS Help Desk web site (https://mhssc.timpo.osd.mil) for a list of access numbers
PHIMT 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 and perform all Privacy Specialist functionality
  - Describe and interpret the data that the PHIMT can provide for compliance measurement
  - Implement PHIMT at your facility