Protected Health Information Management Tool (PHIMT)

User Admin
Version 3.0
April 2011

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 the user roles and responsibilities within the PHIMT
Introduction to PHIMT
Introduction to PHIMT

Objectives

Upon completion of this lesson 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
- 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
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
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.
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
User Admin Functionality
User Admin Functionality

Objectives

Upon completion of this lesson you should be able to:

− Setup a workflow
− Setup a queue
− Create requester favorites
User Admin 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
User Admin Functionality
Main Screen

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

Workflow Setup (1 of 5)

- 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 User’s work will be routed to a Privacy Specialist for approval or denial.
User Admin Functionality

Workflow Setup (2 of 5)

1. Scroll to the bottom of the User Profile screen (Regular User)
2. Click on the New button next to the word Privacy Specialists
User Admin Functionality

Workflow Setup (3 of 5)

3. Enter Search Criteria for the Privacy Specialist that you want to add
4. Click on the Search button

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
User Admin Functionality
Workflow Setup (4 of 5)

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.
User Admin Functionality

Workflow Setup  (5 of 5)

6. Set the Relationship Start Date/End Date  (The end date is optional)
7. 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.
User Admin Functionality

Queue Setup (1 of 7)

- 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
Queue Setup (2 of 7)

1. Select the Admin Tab
2. Select the Queue Users hyperlink

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Parent Name</th>
<th>Address</th>
<th>Contact Person</th>
<th>Contact Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>1006</td>
<td>10th MED GROUP-USAF ACADEMY CO</td>
<td>USAFA</td>
<td>4102 Pinion Drive Ste 4000</td>
<td>USAF Academy</td>
<td></td>
</tr>
<tr>
<td>1109</td>
<td>10th Med GROUP- PETERSON AFB</td>
<td>HQ AIR FORCE SPACE COMMAND</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>967</td>
<td>11TH MED GRP-BOLLING</td>
<td>HQ Air Force (Direct reporting unit)</td>
<td>238 Brookley Avenue RM 125 Bolling AFB, DC 20032</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1070</td>
<td>11th Wing</td>
<td>US Air Force</td>
<td>11 MDG/SGHQ 238 238 Brookley Ave Bolling AFB, DC 20032</td>
<td></td>
<td></td>
</tr>
<tr>
<td>833</td>
<td>121ST GEN HOSP SEOUL</td>
<td>18th MEDCOM - KOREA</td>
<td>Unit # 15244 APO AP 96205</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
User Admin Functionality
Queue Setup (3 of 7)

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

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

Queue Setup (4 of 7)

4. Click on the New button
User Admin Functionality
Queue Setup (5 of 7)

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

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
User Admin Functionality
Queue Setup (6 of 7)

8. Select the Queue you created 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.
User Admin Functionality
Queue Setup *(7 of 7)*

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

10. 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.*
User Admin Functionality

Requester Favorites  (1 of 6)

- 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
Requester Favorites (2 of 6)

1. Select the Admin Tab
2. Select the Organization’s hyperlink
3. Select the ID hyperlink for your Origin Organization

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
User Admin Functionality
Requester Favorites (3 of 6)

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

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
User Admin Functionality
Requester Favorites (4 of 6)

5. Enter organization search criteria
6. Click on the Search button

Any data herein that may be construed as personal information is fictitious and intended for training and operational purposes only.
User Admin Functionality
Requester Favorites (5 of 6)

7. Select the correct organization by clicking on the name

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

Requester Favorites (6 of 6)

- If the requester you are looking for is not listed, scroll to the bottom to add a new organization or person.

<table>
<thead>
<tr>
<th>Where are you</th>
<th>Yes 1305 23, Arlington, VA 22268</th>
</tr>
</thead>
<tbody>
<tr>
<td>Williams Medical Insurance Claims</td>
<td>Yes 1303 222 Taylor, Arlington, VA 22201</td>
</tr>
<tr>
<td>Legal Law Services</td>
<td>Yes 202 686 Post Ln. Suite 1, Carlisle, PA 17013-0003</td>
</tr>
<tr>
<td>health and human services [1234]</td>
<td>Yes 1191 1234 Sth, Hanover, LA 1234-0006</td>
</tr>
<tr>
<td>big test inc.</td>
<td>Yes 1176 Asaf, Asaf, Asaf, CA 35986</td>
</tr>
<tr>
<td>doctor ltd.</td>
<td>Yes 1201 Drexel, Salf, Salford, AL 44444-4444</td>
</tr>
<tr>
<td>dienento locare health clinic [0560]</td>
<td>Yes 1281 5801 Army Pentagon, Washington, DC 20310-5801</td>
</tr>
<tr>
<td>doctor</td>
<td>Yes 1154 111, West CO 98373</td>
</tr>
<tr>
<td>take facility</td>
<td>Yes 1264 1807 Mission Way, Lewiston, AK 50867-1234</td>
</tr>
<tr>
<td>fear of fish of micha pham</td>
<td>Yes 1262 200 E San Antonio, Smithfield, TX 22222-5555</td>
</tr>
<tr>
<td>new requesters</td>
<td>Yes 1155 111 First, York, AK 12344</td>
</tr>
<tr>
<td>cibiceston</td>
<td>Yes 1126 5912 Hoburn Rd, Temple Hills, MD 22302</td>
</tr>
<tr>
<td>north west union</td>
<td>Yes 1174 Fort Lewis, Tacoma, WA 98433</td>
</tr>
<tr>
<td>till</td>
<td>Yes 1150 Dalleke, Earth, SD 57706</td>
</tr>
<tr>
<td>till a nui</td>
<td>Yes 1169</td>
</tr>
<tr>
<td>till a having</td>
<td>Yes 1206 North Door, Here, AL 12121-2111</td>
</tr>
<tr>
<td>robert dayton</td>
<td>Yes 1152 28756 River Dr. Libertyville, IL 60099</td>
</tr>
<tr>
<td>self</td>
<td>Yes 1127 Set, Asaf, CA 22222</td>
</tr>
<tr>
<td>us primary training organization [1115]</td>
<td>Yes 1241</td>
</tr>
<tr>
<td>valencia hall day care</td>
<td>Yes 1269 3952 N Market St, St. Louis, MO 63113</td>
</tr>
<tr>
<td>valencia hall daycare</td>
<td>Yes 1271 2936 Olive St. St. Louis, MO 63113</td>
</tr>
<tr>
<td>valley Read</td>
<td>Yes 1130 15156 Royal Georgian Rd., Gurnee, IL 24567</td>
</tr>
<tr>
<td>well disney</td>
<td>Yes 1131 3202 Hoburn Ln., Temple Hills, MD 22302</td>
</tr>
</tbody>
</table>

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

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

Summary

- You should now be able to:
  - Setup a workflow
  - Setup a queue
  - Create requester favorites
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
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