



HEALTH AFFAIRS



TRICARE  
Management  
Activity

# Privacy Essentials: A Day in the Life of a Privacy Officer

2007 Quarterly Training

TMA Privacy Office



# Objectives

- Upon completion of this module, you should be able to:
  - Explain the Responsibilities of a Privacy Officer
  - Explain transition planning and compliance binder
  - Describe what the NoPP is
  - Identify what are Patient Rights
  - Explain the authorization process
  - Describe how to maintain documentation
  - Identify a BA
  - Describe how to train staff on HIPAA
  - Explain how to oversee a Privacy Program

# Privacy Officer Roles & Responsibilities

(1 of 2)

- Each DoD CE must appoint in writing a Privacy Official responsible for developing and implementing its privacy policies and procedures by:
  - Overseeing ongoing activities related to compliance with the HIPAA Privacy Rule and related Security components
  - Developing, implementing and maintaining MTF/DTF policies and procedures
  - Establishing procedures to track access, use and disclosure of PHI
  - Ensuring adherence to MHS policies and procedures at MTF level

# Privacy Officer Roles & Responsibilities

(2 of 2)

## ■ Roles and Responsibilities

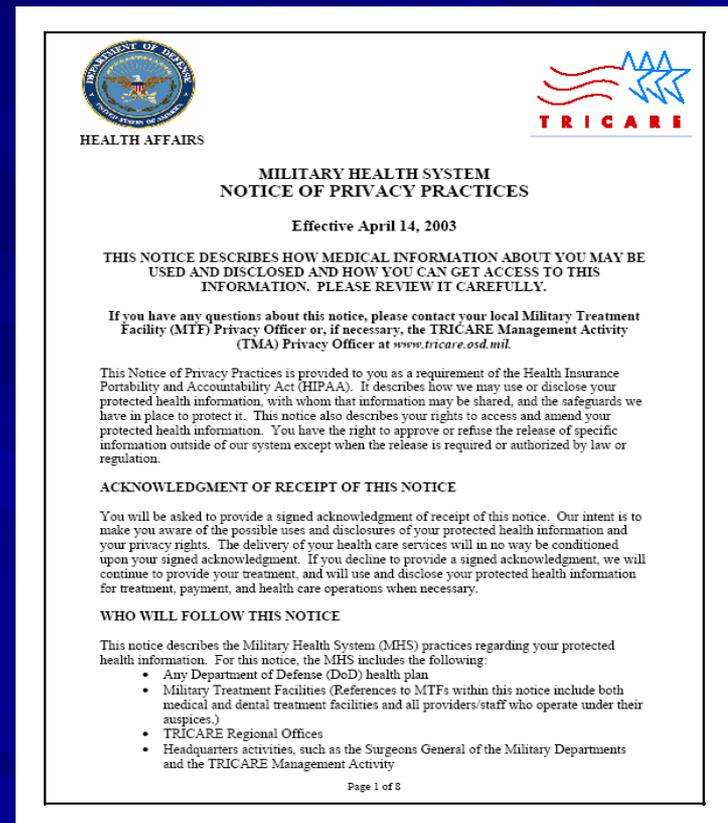
- Training the workforce
- Monitoring BAAs related to privacy concerns
- Investigating patient complaints regarding privacy infractions
- Communicating of the NoPP
- Maintaining and updating compliance binder
- Providing a transition plan for newly appointed PO

## A Day in the Life of a Privacy Officer

# Notice of Privacy Practices (1 of 2)

### ■ PO must be knowledgeable of what is outlined within the NoPP

- MHS Duty to protect PHI
- Patient Rights
- Patient complaint procedures
- The OCR/HHS



# Notice of Privacy Practices (2 of 2)

- Each facility should have posted the NoPP in plain view identifying who the MTF PO is with the phone number and email address
- To obtain a copy of the NoPP poster a PO can:
  - submit an email to [privacymail@tma.osd.mail](mailto:privacymail@tma.osd.mail)
  - Go to <http://www.tricare.osd.mil/TRICARESmart>
- Patients should contact the MTF PO for issues, concerns, complaints, and questions

# Patient Rights

- Patients Rights that are outlined in the NoPP:
  - Inspect and Obtain a Copy of their PHI
  - Request an Amendment to incorrect or incomplete PHI
  - Designate a Personal Representative to act on their behalf
  - Request a Confidential Communications
  - Request Restrictions on all or part of their PHI
  - Request an Accounting of Disclosures
  - Submit a Complaint to PO, OCR/HHS
  - Receive a copy of the NoPP

# Inspect and Obtain a Copy of their PHI

(1 of 2)

- Individuals may request access to, or copies of, their PHI
- Includes:
  - Medical records
  - Billing records
  - Other records used in making decisions concerning the individual
- Does not include:
  - Psychotherapy notes
  - Information compiled in anticipation of, or use in, a civil, criminal or administrative action or proceeding
  - PHI that is subject to law that prohibits access

# Inspect and Obtain a Copy of their PHI

(2 of 2)

- Request must be in writing
- You must grant or deny request within:
  - 30 days for records you possess
  - 60 days for PHI maintained or accessible only at another site
- You may extend time by no more than 30 days if you provide the individual with written:
  - Explanation as to why there is a delay
  - Date for final action

## A Day in the Life of a Privacy Officer

# Granting Access

- Notify individual and provide access or copies within required time period
- If PHI is duplicated at more than one location you only have to provide it once
- Produce in requested format if reasonable
  - If not, provide in readable hardcopy or other agreed upon format
- Provide summary or explanation of PHI only when the individual agrees in advance
- You may impose a reasonable cost based fee for supplies and labor in accordance with service policy
  - You must inform the individual of those fees in advance

## A Day in the Life of a Privacy Officer

# Denying Access (1 of 5)

### ■ When a patient requests access to:

- Psychotherapy notes

  - Must know state law

  - Adhere to most stringent rule



- Information compiled for use in a civil, criminal or administrative action or proceeding

- Disclosure prohibited under the Clinical Laboratory Improvements Amendments of 1988

- Disclosure prohibited under the Title 10, USC, Section 1102, Confidentiality of medical quality assurance records

### ■ PHI was obtained from someone other than a provider under promise of confidentiality and providing access could reveal the source

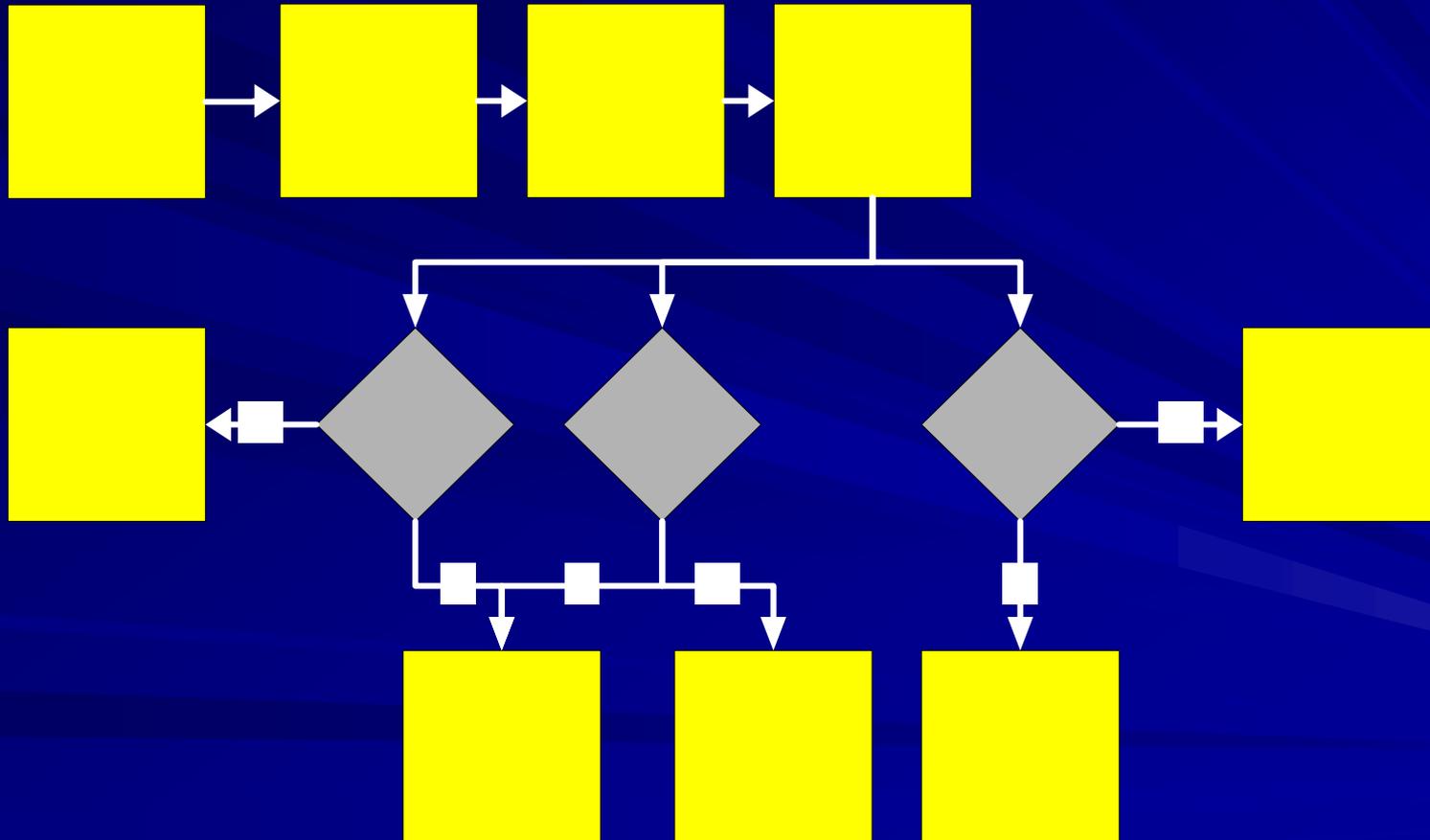
## Denying Access (2 of 5)

- To an inmate in correctional institution if access would jeopardize the health, safety, security, custody or rehabilitation of the individual, other inmates, or any officer employee or other person at the facility
- Individual is participating in a research project and they have signed a consent clause suspending right of access
  - Only while the research is in progress

# A Day in the Life of a Privacy Officer

## Denying Access (3 of 5)

### ■ Denial Access to Records Flow Chart



## Denying Access (4 of 5)

- Denials must be written in plain language and contain:
  - A basis for the denial
  - A description of how the individual may exercise their right to a review
  - How the individual may file a complaint to both the DoD and the Secretary of HHS
- If individual requests a review you must:
  - Provide review by licensed health care official not involved in initial denial
  - Provide review in reasonable period of time
  - Notify individual of result in writing

## Denying Access (5 of 5)

- If the denial pertains to only part of the request, you must provide access to any other requested PHI
- If you do not maintain the PHI requested and know where it is located, you must inform an individual where to direct their request
- Note: Access to most PHI is also subject to the Privacy Act. You must grant access to PHI unless access can be denied under the DoD implementing policies for **both** laws

# Right to Request an Amendment

- Individuals have the right to request that you amend the PHI you maintain
- You must grant or deny the request within 60 days
  - You may extend the time period only once for no more than 30 days if you inform the individual in writing and include the reason for the delay and date they can expect a decision

# Granting an Amendment

- If you agree to make the amendment:
  - Notify the individual in writing
  - Make reasonable effort to notify other persons the individual identifies and agrees should know of the amendment
  - Provide the amendment to other people, including business associates, who possess the PHI and may use it to the individual's detriment
  - You may amend the PHI by identifying the records that are affected and appending or providing a link to the amendment

# Denying an Amendment (1 of 3)

- You may deny a request for an amendment for the following reasons:
  - You did not create the PHI, unless the individual provides reason to believe the originator of the information is no longer available
  - The affected PHI is not part of the designated record set
  - The individual does not have a right of access to the affected PHI
  - The PHI is accurate and complete

# Denying an Amendment (2 of 3)

- When denying the request (in whole or in part) you must provide individual with a denial written in plain English that contains:
  - A basis for the denial
  - A description of how the individual may submit a written statement of disagreement including the basis for disagreement
  - How the individual may file a complaint to both the TMA Privacy Office and the Secretary of HHS
  - The Individuals right to request that you include the original request for amendment and the denial with any future disclosures of the affected PHI

# Denying an Amendment (3 of 3)

- You may limit a statement of agreement and summarize the statement for inclusion with disclosures
- You may prepare a written rebuttal for inclusion if you provide the individual with a copy
- You must identify the disputed PHI and append or otherwise link the individual's request for amendment, the denial, the statement of disagreement, if any, and the rebuttal, if any to the record
- You must include the above documentation with all future disclosures of the disputed PHI
- You must amend the affected record when you receive an amendment to an individual's PHI from another covered entity

# Designated Personal Representative

- The HIPAA Privacy Rule allows providers, health plans and clearinghouses to treat an individual's Personal Representative (PR) as if they were the individual
- Categories:
  - Adult or emancipated minor
  - Unemancipated minor
  - Deceased individuals
  - Abuse, neglect, and endangerment situations

# Personal Representative Adult or Emancipated Minor

- PR is a person with legal authority to make health care decisions on behalf of an individual
- Examples:
  - Health care power of attorney
  - Court appointed legal guardian
  - General power of attorney

# Personal Representative Unemancipated Minor

- PR is a parent, guardian, or other person acting *in loco parentis* with legal authority to make health care decisions on behalf of the minor child
- Examples:
  - Parent
  - Court appointed guardian
  - Healthcare or general power of attorney

# Personal Representative Deceased Individual (1 of 2)

- PR is a person with legal authority to act on behalf of the decedent to the estate (not restricted to health care decisions)
- Examples:
  - Executor of the estate (Will)
  - Administrator (No Will)

# Personal Representative Deceased Individual (2 of 2)

- Rights and protections granted under HIPAA continue to apply to the PHI of deceased individuals
- You must continue to protect the confidentiality of the PHI
- Deceased persons PR may exercise control over use and disclosure of PHI (right of access, authorizations for disclosure etc.)
- You may disclose PHI without an authorization to:
  - Coroners and medical examiners
  - Funeral directors
  - Organizations aiding in the transplantation of organs, eyes and tissue

# A Day in the Life of a Privacy Officer

## What the PR Can Do

- The PR may:
  - Be provided with information about the individual's care and condition
  - Use PHI to make health care decisions
  - Authorize disclosures of PHI
  - Exercise the individual's rights, e.g. ask for accounting of disclosures

# PR Limitations and State Laws

- If authority to act is limited, then rights with respect to PHI is limited
  - e.g., if power of attorney is limited to use of artificial life support, then PR can access PHI related to that health care decision
- Rule defers to state law with regard to rights of parents/guardians of minors

# PR Exceptions (1 of 2)

- Do not treat the PR as the individual when:
  - An MTF has a reasonable belief that the individual may be subject to domestic violence, abuse or neglect by the PR
  - Treating the PR as the individual could in some way endanger the individual
  - An MTF believes, in its professional judgment, that it is not in the best interest of the individual to treat the PR as the individual

# PR Exceptions (2 of 2)

- A parent is not the PR when:
  - State or other law does not require the consent of a parent before a minor can obtain a particular service, and the minor consents to the service
  - A court determines or other law authorizes someone other than the parent to make decisions for a minor
  - A parent agrees to a confidential relationship between the minor and the physician

# Accounting of Disclosures

- Individual may request an accounting of all disclosures (including to or by BA) during the previous six years except for:
  - Disclosures for TPO
  - To the individual
  - Disclosures that are in response to an authorization
  - For the facility's directory
  - To persons involved in the individual's care
  - For authorized national security or intelligence purposes
  - To correctional institutions or law enforcement officials as authorized
  - Disclosures occurring before April 14, 2003
- Ensure that you retain documents

# Restrictions

- Individual's have the right to ask you to restrict uses and disclosures of PHI for TPO and for involvement in their care
- You may grant or refuse the request
- If you grant the request, you must abide by the agreement except in emergencies
- Requests may be made in writing or orally
- No agreement to restrict applies beyond the CE that agreed to it
- You should respond to a request as soon as practicable and include reasons for a denial
- You may terminate a restriction upon written notice to the individual or the written or oral request of the individual

# Confidential Communications

- Individuals have the right to request receipt of communication from you by alternate means or at alternate locations
- You must agree to such requests when reasonable
- You may require the request in writing with details of specific alternatives
- You cannot require the individual to explain the basis for their request

# Patient Right To Submit a Complaint

- All beneficiaries have the right to complain if they believe their privacy rights have been violated or if they feel the covered entity has failed to meet its responsibilities
- Individuals have the right to make a complaint concerning your or 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 established by the rule or DoD's implementing regulation

# Complaints

- Privacy Officer will need to read and analyze the complaint to determine if it is a valid HIPAA Complaint
- Things to look for:
  - Beneficiary provided information
  - Pursuant to an Authorization
  - PHI correctly used or disclosed as part of TPO
  - PHI released based on 14 Uses and Disclosures
  - Was disclosure recorded
  - Determine if complaint is HIPAA based or based on other privacy laws

# Documentation (1 of 2)

- Document privacy policies and procedures in written or electronic form
- Document required communications, designations, actions and activities
- Record date of creation and last date of effectiveness of documents

# Documentation (2 of 2)

- Maintain required documentation for six years from date of creation or the date when the policy or procedures was last in effect, whichever is later
- Centralize retained documentation
- Clearly delineate title/office and assigned responsibilities

# Who is a Business Associate? (1 of 2)

- “A person or entity who provides certain functions, activities, or services for or to a covered entity, involving the use and/or disclosure of protected health information”
  - Can be a health care provider, health plan, or another CE
  - Cannot be a member of the health care provider, health plan, or other CEs workforce
  - Excludes CEs who disclose PHI to providers for treatment purposes

# Who is a Business Associate? (2 of 2)

- Three basic conditions define a BA, including:
  - Performs, or helps perform, work that uses or discloses IIHI on behalf of the CE
  - Work being performed is a “covered function” (activities that pay for, or provide health care) regulated by the rule
  - Person performing work does not belong to the CEs workforce

## A Day in the Life of a Privacy Officer

# Business Associate Functions

**Functions or activities that involve the use and disclosure of PHI, include:**

- Legal
- Actuarial
- Accounting
- Billing
- Consulting
- Data Aggregation
- Claims Processing

- Utilization Review
- Quality Assurance
- Management
- Administrative
- Accreditation
- Financial Services

# Identifying a Business Associate (1 of 2)

- Inventory existing contracts
- Identify other BAs by performing a data flow analysis of PHI
- Look at the functions performed by the third parties, not just their predominant role
  - For example, a provider may have a payer as a BA if it provides assistance for the provider's 'wellness programs'
  - Clearinghouses may be BAs if they perform translation services
  - Medical supply houses may serve as conduits to move PHI back to manufacturers

# Business Associate Safeguards

- HIPAA Privacy/Security Rules extend safeguards for PHI to persons or entities who work with PHI on a CE's behalf
  - The BA must comply with the requirements of the Privacy/Security Rules
- HIPAA requires including the requirement to comply with the safeguards as part of the contracts governing performance of the work (i.e., “business associate agreements”)

# Business Associate Agreements (BAA)

- Privacy BAAs were required to be in place by April 14, 2003; Security BAAs were required by April 20, 2005
- The rule requires CEs to establish agreements between themselves and entities with whom PHI is shared
- The rule does not require CEs to monitor, audit or oversee BAs for HIPAA compliance. They are expected to periodically verify that the BAs are complying with the agreements

# Business Associate Training

- All BAs must complete HIPAA Privacy training
  - If the BAs workspace is within the physical confines of the MTF, the TMA provided web based training tool may be used to train the BA
  - If the BAs workspace is not within the physical confines of the MTF, the BA is responsible for providing its own training

# Workforce Training

- Who should receive Privacy and Security awareness training:
  - Entire current workforce by compliance date
  - New employees within their first 30 days of employment
  - Employees affected after material changes in policies or procedures
  - Follow Service policy
- Workforce: This means employees, volunteers, trainees, and other persons under the direct control of a *CE*, whether or not they are paid by the *CE*
- Training tool: Learning Management System (LMS) utilization

# A Day in the Life of a Privacy Officer

## HIPAA Refresher Training

**Quick Compliance**

Audio on off Exit

### HIPAA 210: The HIPAA Privacy Refresher

How to Use this Course

- ✓ 1. Introduction to HIPAA
- ✓ 2. HIPAA Terminology
- ✓ 3. Protected Health Information
- ✓ 4. Notice and Authorization
- ✓ 5. Patient Rights
- ✓ 6. Security Basics
- ✓ 7. Conclusion



 Click a lesson name to go to the lesson

 Transforming Knowledge into Practice

 Disclaimer 

# Program Oversight (1 of 3)

- Use HIPAA training tools reports to track and document appropriate training to all MTF personnel
- Ensure MTF Policies and Procedures are available for MTF staff to review as part of HIPAA compliance training
- Educate MTF staff on applying most **stringent** law
- Understand DoD privacy regulations and where they differ from HIPAA
- Ensure State and Local Law Exemptions are understood by MTF Staff

## A Day in the Life of a Privacy Officer

# Program Oversight (2 of 3)

- Inform MTF leadership
- Ensure you are aligned with Metrics
- Access TMA Website for
  - Standard language support
  - MHS wide actions
  - Other compliance actions and best practices
  - Information releases
- Know the roles of your TRICARE Regional Offices (TRO) and Service Reps
- Participate in Medical Information Security Readiness Team (MISRT) activities to understand security and privacy interrelatedness
- Know your MTF legal counsel

# Program Oversight (3 of 3)

- Know how to use the HIPAA Compliance Tool (HIPAA BASICS™)
  - Identify Users and User Levels
  - Complete MTF compliance assessments
- Generate plan to achieve full HIPAA Privacy compliance
- Manage personnel to execute compliance plan
- Be prepared to report on MTF compliance status as progress is made
- Maintain compliance binder

# A Day in the Life of a Privacy Officer

## Presentation Summary

- You should now be able to:
  - Explain the Responsibilities of a Privacy Officer
  - Explain transition planning and compliance binder
  - Describe what the NoPP is
  - Identify what are Patient Rights
  - Explain the authorization process
  - Describe how to maintain documentation
  - Identify a BA
  - Describe how to train staff on HIPAA
  - Explain how to oversee a Privacy Program

# 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](mailto:Privacymail@tma.osd.mil) for subject matter questions
- Service HIPAA Representatives