

JUNE 7-8, 2011

# TMA Privacy Weekly

TMA Privacy and Civil Liberties Office  
2011 DATA PROTECTION SEMINAR



## Complying with the HIPAA Privacy and Security Rules



# Complying with the HIPAA Privacy and Security Rules

## Purpose

The purpose of this presentation is to provide an overview of the health privacy and security requirements, including the Health Insurance Portability and Accountability Act (HIPAA) of 1996 Privacy and Security Rules and Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act (ARRA) of 2009, and to discuss how these requirements apply to your work processes.



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## Objectives

- Upon completion of this presentation, you should be able to:
  - State the purpose of privacy and security rules, to whom they apply, and what they safeguard
  - Identify the key DoD regulations that mirror the HIPAA Privacy and Security Rules
  - Explain the general requirements in these rules
  - Describe the applicability of these requirements to your work environment
    - Explain the exceptions to the rules and how they apply to your work environment



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## Legislative Baseline

- HIPAA was enacted to improve the efficiency and effectiveness of the health care system by standardizing the electronic exchange of administrative and financial data
  - Congress recognized that an individual's privacy could be at risk when data is exchanged electronically
  - HIPAA included a placeholder for either additional legislation or regulation to safeguard patient privacy
- Congress passed HITECH as part of ARRA to increase use of health information technology



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## Regulatory Baseline

- Congress did not pass legislation to safeguard health information exchanged electronically
- Instead, the Department of Health and Human Services (HHS) published rules to implement these safeguards
- The rules apply to:
  - Covered entities (CEs)
    - Healthcare entities that transmit health information electronically in connection with certain transactions described in the regulation
  - Business associates (BAs)



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## Regulatory Baseline (continued)

- HHS rules became effective April 14, 2003
- HITECH mandates changes to the HHS privacy rules
  - BAs
  - Breaches
  - Restrictions
  - Accounting of Disclosures



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## DoD Regulatory Baseline

- DoD 6025.18-R, “Health Information Privacy Regulation”, January 24, 2003, implements the HHS HIPAA Privacy Rule throughout DoD
- Defines the baseline health information privacy requirements for use and disclosure of protected health information (PHI) by CEs and BAs:
  - Regulates how CEs use and disclose PHI
  - Limits use and release of health records
  - Establishes safeguards to protect PHI
  - Holds violators accountable with civil and criminal penalties that can be imposed if they violate a patient’s privacy rights
  - Enables patients to find out how their health information may be used and what disclosures have been made



HEALTH AFFAIRS



TRICARE®

TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## DoD Regulatory Baseline (continued)

- Applies the federal rule in most cases
  - “State laws pertaining to healthcare are not applicable to healthcare programs and activities of the Department of Defense”
  - Exception: Cases involving PHI of a minor adhere to state law
- CEs must also comply with the:
  - Privacy Act
  - Freedom of Information Act
  - Alcohol, Drug Abuse, and Mental Health Administration Reorganization Act



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## DoD Regulatory Baseline (continued)

- DoD 8580.02-R, “DoD Health Information Security Regulation”, July 12, 2007, implements the HIPAA Security Rule to apply technical, physical, and administrative security specifications for electronic PHI (ePHI) within DoD
  - Specific standards with a risk-based approach
  - May be “required” or “addressable”
    - Required means that the CE must carry out the implementation specification at its facility
    - Addressable means that CE must assess whether the implementation specification is reasonable and appropriate, based on specified factors
- Complements DoD information assurance (IA) controls



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## When the Rules Do NOT Apply

- Privacy and Security Rules do not apply to:
  - DoD's drug testing program
  - Health care to foreign national beneficiaries when care is provided outside the United States
  - Armed Forces Repository of Specimen for the Identification of Remains
  - Health care to prisoners of war, retained personnel, civilian internees
  - Education records maintained by DoD schools



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## When the Rules Do NOT Apply (continued)

- Privacy and Security Rules also do not apply to:
  - DoD daycare center records
  - Military Entrance Processing Stations
  - Reserve component medical activities practicing outside of a military treatment facility (MTF)
  - Reserve components practicing outside of an MTF who do not engage in covered electronic activities



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## CEs and BAs Explained

- A CE is a health plan, a healthcare clearinghouse, or a healthcare provider that transmits health information in electronic form in connection with a transaction for which the HHS has adopted a standard
  - TMA is a health plan (CE)
  - MTFs are providers (CEs)
- A BA is an organization that has an arrangement with a CE to furnish services for the CE involving use and disclosure of the PHI under the CE's control
  - Contractors are often BAs of TMA



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## CEs and BAs Explained (continued)

- CEs and BAs must enter into business associate agreements (BAAs)
  - These agreements outline the BA's responsibility to protect PHI
  - BAs are obligated to ensure that their subcontractors agree to the same restrictions and conditions that apply to the BA
- HITECH made BAs subject to direct HHS enforcement and penalties with respect to certain provisions of the HIPAA Privacy and Security Rules



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## Who is in the Workforce?

- Members of the workforce are those individuals who are under the direct control of the entity:
  - Military and civilian employees
  - Volunteers
  - Trainees
  - Students
  - Contract personnel



HEALTH AFFAIRS



TRICARE  
Management Activity

## Complying with the HIPAA Privacy and Security Rules

# What is PHI?

- PHI includes the following individually identifiable data elements, when combined with health information about that individual, including:
  - Names
  - All geographic subdivisions smaller than a state
  - All elements of dates (except year) for dates directly related to an individual including birth date, admission date, discharge date, date of death
  - Telephone numbers
  - Fax numbers
  - Electronic mail (e-mail) addresses
  - Social security numbers
  - Medical record numbers
  - Health plan beneficiary numbers



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## What is PHI? (continued)

- Additional PHI elements include:

- Account numbers
- Certificate/License numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web universal resource locators (URLs)
- Internet protocol address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code, with some exceptions



# Complying with the HIPAA Privacy and Security Rules

## Individual Rights

- Individuals:
  - Are entitled to **accounting of disclosures** of their PHI upon request, subject to certain exceptions
  - Have a **right of access** to their PHI, with some exceptions
    - Access may be denied for psychotherapy notes
  - Have the right to **confidential communications**, including request communications of PHI by alternative means or at alternative locations
  - Have the **right to request amendments** to their PHI
  - Should not be denied a **request to restrict disclosure** of a record if payment for a particular service was out of pocket in full



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## Using and Disclosing PHI

- Use: Sharing information within the entity that maintains the information
- Disclosure: Releasing, providing access to, or divulging in any manner, PHI outside the entity maintaining it
- Rules on use and disclosure apply to all forms of PHI, including verbal, paper, and electronic



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## Using and Disclosing PHI (continued)

- Disclosure of PHI for purposes of treatment, payment, and health care operations (TPO) is permitted without signed authorization from the individual
- Health care operations include:
  - Quality assessment and improvement activities
  - Reviewing competence for qualifications of health care professionals
  - Health insurance or benefit contract functions
  - Review, audit, and compliance functions
  - Business planning and management functions



HEALTH AFFAIRS



TRICARE  
Management Activity

## Complying with the HIPAA Privacy and Security Rules

# Using and Disclosing PHI (continued)

- All other disclosures require an authorization from the patient or the patient's personal representative using the Authorization for Disclosure of Medical Information (DD Form 2870)
- CEs must be able to account for disclosures upon request
- HIPAA-exempted disclosures for purposes of TPO from the disclosure request
- HITECH did away with this exemption
  - Effective January 2014, a request for an accounting of disclosure must include disclosures made for TPO
  - Expect a proposed rule to implement this change sometime this summer



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## Minimum Necessary

- Minimum Necessary Standard
  - Organizations should limit the use or disclosure of PHI, including disclosures for payment and/or healthcare operations, to the “minimum necessary to accomplish the intended purpose of the use, disclosure, or request”
  - This standard does not apply to disclosures of PHI for treatment purposes



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## Facility Directory

- Give advance notice
  - Notice may be given orally
  - Patient has the right to object to be included in the directory
- Contents of directory:
  - Name
  - Location in facility
  - Condition in general terms
  - Religious affiliation (for clergy only)



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## Allowable Disclosures

- Specialized government functions
  - Armed Forces personnel
- A CE may use and disclose PHI of active duty “for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission”



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## **Allowable Disclosures** (continued)

- Required by law
- Public health activities
- Victims of abuse, neglect, or domestic violence
- Health oversight
- Judicial and administrative proceedings
- Law enforcement
- Decedents
- Organ donation
- Research involving minimal risk
- To avert serious threat to health or safety
- Workers compensation



# Complying with the HIPAA Privacy and Security Rules

## Incidental Uses and Disclosures

- Confidential conversations among healthcare providers or with patient within earshot of others
- Posting patient name outside patient room
- Patient chart at the bedside
- X-ray light board
- Discussing patient condition during medical rounds (training)

### Caution

Do not rely on these exceptions to avoid having appropriate safeguards, policies, and procedures in place to safeguard patient privacy



# Complying with the HIPAA Privacy and Security Rules

## Psychotherapy Notes

- Notes recorded (in any medium) by a mental healthcare provider that documents or analyzes the contents of a private counseling session or a group, joint, or family counseling session
  - These are separate from the rest of the individual's medical record
- This **does not** include medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items:
  - Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date



# Complying with the HIPAA Privacy and Security Rules

## Psychotherapy – Special Rules

- One must obtain an authorization for any use or disclosure of psychotherapy notes, except:
  - To carry out the following treatment, payment, or health care operations:
    - Use by the originator of the psychotherapy notes for treatment
    - Use or disclosure by the CE for its own training programs that students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling
    - Use or disclosure by the CE to defend itself in certain legal actions



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## Complaints

- Anyone who feels that privacy rights are being violated may submit a written complaint with TMA or with the HHS Office for Civil Rights
  - All complaints are routed through the TMA Privacy and Civil Liberties Office (Privacy Office)
  - Service complaints are forwarded to Service representatives
  - Any allegations of an impermissible disclosure means that a breach may have occurred
    - The allegation must then be reported as a potential breach
    - The breach report should be revised once a full investigation is completed that either substantiates or unsubstantiates the complaint



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## Security Safeguards – Administrative

- There must be a security management process to include:
  - Risk analysis
  - Risk management
  - Sanction policy
- There must be a HIPAA Security Officer to develop and implement security policies and procedures
- Workforce security:
  - Appropriate access to PHI
  - Authorization
  - Termination when the work ends



HEALTH AFFAIRS



TRICARE  
Management Activity

## Complying with the HIPAA Privacy and Security Rules

# Security Safeguards – Administrative (continued)

- Information access management
- Security awareness and training
- Security incident procedures



HEALTH AFFAIRS



TRICARE®

TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## Security Safeguards – Physical

- Facility access controls
- Workstation use
  - Workstation: Any electronic computing device and electronic media stored in its immediate environment
    - Laptop/desktop computers
    - Personal digital assistants (PDAs)
    - Tablets



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## Security Safeguards – Technical

- Access controls
  - Restrict access
  - Unique user identification
  - Automatic log off
  - Encryption/Decryption



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## Summary

- You should now be able to:
  - State the purpose of privacy and security rules, to whom they apply, and what they safeguard
  - Identify the key DoD regulations that mirror the HIPAA Privacy and Security Rules
  - Explain the general requirements in these rules
  - Describe the applicability of these requirements to your work environment
    - Explain the exceptions to the rules and how they apply to your work environment



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## Resources

- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act (ARRA) of 2009
- DoD 6025.18-R, “DoD Health Information Privacy Regulation”, January 24, 2003
- DoD 8580.02-R, “DoD Health Information Security Regulation”, July 12, 2007



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## Resources (continued)

- DoD Directive 8500.1, “Information Assurance”, October 24, 2002
- DoD Directive 8000.01, “Management of the Department of Defense Information Enterprise”, February 10, 2009
- DoD Instruction 8500.2, “Information Assurance (IA) Implementation”, February 6, 2003
- DoD Instruction 8510.01, “DoD Information Assurance Certification and Accreditation Process (DIACAP)”, November 28, 2007



HEALTH AFFAIRS



TRICARE  
Management Activity

# Complying with the HIPAA Privacy and Security Rules

## Resources (continued)

- OMB Circular No. A-130, Revised, Transmittal No. 4, November 30, 2000
- DoD Manual 8910.1-M, “DoD Procedures for Management of Information Requirements”, June 30, 1998
- Frequently Asked Questions:  
<http://www.tricare.mil/tma/privacy/faqs.aspx>
- To subscribe to the Privacy Office E-News go to:  
<http://www.tricare.mil/tma/privacy/maillinglist.aspx>
- E-mail [Privacymail@tma.osd.mil](mailto:Privacymail@tma.osd.mil) for subject matter questions



HEALTH AFFAIRS



TRICARE  
Management Activity