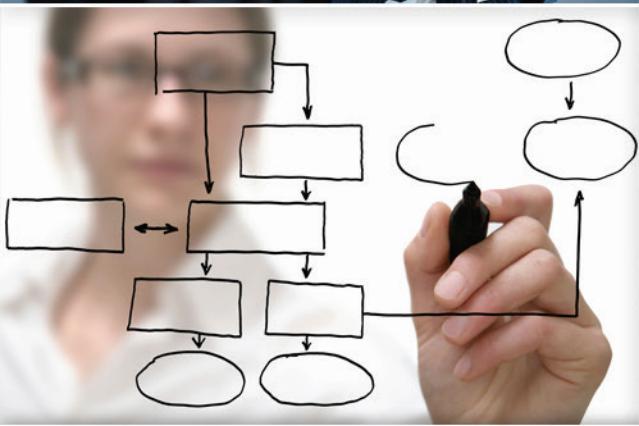


TMA PRIVACY AND CIVIL LIBERTIES OFFICE

# 2012 HEALTH INFORMATION PRIVACY & SECURITY TRAINING



## Complying with the HIPAA Privacy and Security Rules

**THE POWER OF TEAM WORK**

Committed to Protecting Beneficiary Data

# Complying with the HIPAA Privacy and Security Rules

## Purpose

The purpose of this presentation is to review the Health Insurance Portability and Accountability Act (HIPAA) of 1996 Privacy and Security Rules and the Health Information Technology for Economic and Clinical Health (HITECH) Act, and to discuss HIPAA hot topics.



# Complying with the HIPAA Privacy and Security Rules

## Objectives

- Upon completion of this presentation, you should be able to:
  - Express a general understanding of the HIPAA Privacy and Security Rules and their implementation
  - Identify provisions of the HIPAA Privacy and Security Rules that have or will be modified by the HITECH Act and anticipate further guidance and regulations from the Department of Health and Human Services (HHS)
  - Discuss current and relevant HIPAA Security issues including impending changes to DoD 8580.02-R, “Health Information Security Regulation”, current guidance on cloud computing, and security considerations for teleworkers



# Complying with the HIPAA Privacy and Security Rules

## HIPAA Basics

- HIPAA applies to covered entities (CEs)
- HIPAA protects protected health information (PHI)
- The HIPAA Privacy Rule – all paper, electronic, and verbal PHI
  - Minimum privacy protections
  - Minimum rights
  - Administrative obligations
- The HIPAA Security Rule – electronic PHI (ePHI)
  - Administrative safeguards
  - Physical safeguards
  - Technical safeguards



The HIPAA Privacy Rule is implemented through DoD 6025.18-R, "DoD Health Information Privacy Regulation"  
The HIPAA Security Rule is implemented through DoD 8580.02-R, "DoD Health Information Security Regulation"



# Complying with the HIPAA Privacy and Security Rules

## HIPAA Scenarios

- Scenario 1 – Have any individual rights granted by the HIPAA Privacy Rule been violated?
- Scenario 2 – What are the HIPAA Security Rule implications?
- Scenario 3 – Was the HIPAA Privacy Rule violated?



## Complying with the HIPAA Privacy and Security Rules

# HIPAA Updates – The HITECH Act

- The HITECH Act is contained within the American Recovery and Reinvestment Act (ARRA) of 2009, also known as the “Stimulus Bill”, Title 13, Subtitle D – Privacy
- Enacted on February 17, 2009
- Purpose:
  - Promote health information technology – striving for universal electronic health records (EHR) by 2014
  - Strengthen HIPAA’s privacy and security protection of PHI



# Complying with the HIPAA Privacy and Security Rules

## HITECH Act Modifications

- **Business associates (BA)** are directly subject to certain HIPAA privacy and security requirements “in the same manner that [the requirements] apply to the covered entity”
  - Awaiting HHS guidance
- CEs are required to comply with an ***individual's request to restrict disclosure*** of PHI if: (1) Disclosure is to a health plan for payment or healthcare operations, **and** (2) The patient pays provider “out of pocket in full”
  - Effective 2/17/10 and awaiting HHS guidance
- The ***Minimum Necessary Rule*** restricts use and disclosure of a “limited data set” or, if necessary, to minimum necessary when the rule applies
  - Effective 2/17/10 and awaiting HHS guidance



# Complying with the HIPAA Privacy and Security Rules

## HITECH Act Modifications

- If a CE maintains an EHR, the CE is required to ***account for treatment, payment, and health care operations (TPO) disclosures***, extending back three years
  - Effective 1/1/11 or date of acquisition for CEs who acquired EHR after 1/1/09
  - Will be effective 1/1/14 for CEs who acquired EHR before 1/1/09
  - Secretary may postpone for up to two years
- The ***sale of PHI*** is restricted unless an individual signs a written HIPAA Authorization, with the exception of public health, cost of preparation/transmittal of data for research, treatment, sale of the entity, payment to BAs, and payment by individuals for a copy of their record
  - Will be effective six months after final regulations



# Complying with the HIPAA Privacy and Security Rules

## HITECH Act Modifications

- Enhanced enforcement: Increased penalties for HIPAA violations (effective 2/17/09)
  - Penalties tiered, based on fault and whether corrective action was taken – \$100 per violation and up to \$50,000 per violation for violations due to willful neglect that are not corrected
  - Permits State's Attorneys General to bring civil suits under HIPAA for penalties and attorney's fees
  - Clarifies that individuals (employees) can be prosecuted criminally under HIPAA
  - Beginning 2012, requires formal civil monetary penalties for violations involving willful neglect
  - Requires HHS to conduct periodic HIPAA compliance audits of CEs and BAs with the HIPAA Privacy and Security Rules



# Complying with the HIPAA Privacy and Security Rules

## HITECH Act Modifications

- Permits individuals the ***right to obtain a copy of PHI in an EHR in an electronic format***, and to direct the CE to transmit an electronic copy to a third party
  - Effective 2/17/10 and awaiting HHS guidance
- Prohibits a CE to be paid by a third party for ***marketing*** the CE's products, services, or benefits ("remuneration"), except:
  1. Reasonable remuneration for communications concerning drugs and biologicals currently being prescribed
  2. Payment to BAs for communications on behalf of CEs
  - Effective 2/17/10
- An opt-out by the individual to ***fundraising communications*** is treated as a revocation of authorization
  - Awaiting final regulations



# Complying with the HIPAA Privacy and Security Rules

## Rulemaking Status

- Omnibus Final Rulemaking was sent to the Office of Management and Budget (OMB) for review on 3/24/12
- OMB had 90 days to review (until 6/25/12), and may have requested clarification and/or further action from HHS
- If and when OMB approves the HHS's final rules, they will be published in the Federal Register

### Key Takeaways

- The HITECH Act strengthens the HIPAA Privacy and Security Rules, most notably through enhanced enforcement, extending HHS's reach to BAs, and updated breach response procedures (focus of another session)
- We are awaiting final regulations, which will be published in the Federal Register



# Complying with the HIPAA Privacy and Security Rules

## HIPAA Hot Topics: Privacy Overlay

- The HIPAA Security Rule is implemented through DoD 8580.02-R, “DoD Health Information Security Regulation”
- The development of the Privacy Overlay began with the Certification & Accreditation Transformation Initiative and efforts from the DoD and intelligence community to align Information Assurance processes with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 (revision 3) control catalog
- Designed to identify the security control specifications required to address privacy risks to national security systems. It applies to national security systems containing any of these three types of personally identifiable information (PII)
  - PII, about U.S. citizens and legal permanent residents
  - Records in a Privacy Act system of records
  - PHI



## HIPAA Hot Topics: Privacy Overlay

- The TMA Privacy and Civil Liberties Office (Privacy Office) participated in the Committee on National Security Systems (CNSS) working group chartered to develop the Privacy Overlay to ensure HIPAA Security Rule requirements were incorporated
  - A map and gap analysis was performed between the HIPAA Security Federal Rule and NIST SP 800-53 (rev 3) security controls
  - The working group selected controls and developed supplemental guidance to meet federal privacy regulations and best practices
    - The controls were included in the CNSS baseline, several of which required additional supplemental guidance above that provided in NIST SP 800-53 to meet the intended purpose of privacy or specific regulatory intent



## HIPAA Hot Topics: Privacy Overlay

- What's next?
  - The Privacy Overlay will be reviewed by stakeholders before final approval
  - DoD 8580.02-R, “DoD Health Information Security Regulation” will be modified to incorporate and account for the efficiencies the Privacy Overlay introduces

### Key Takeaways

- The Privacy Overlay is part of the IA Transformation initiative
- As a result of the Overlay, DoD 8580.02-R will be modified and aligned more closely with the Federal Rule
- The Privacy Overlay will improve implementation compliance



## HIPAA Hot Topics: Cloud Computing

- In December 2010, the U.S. Chief Information Officer (CIO), published the 25 Point Implementation Plan to Reform Federal Information Technology Management
  - Established a “Cloud First” policy mandating that government agencies “default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists.”
- Cloud computing, as defined by NIST
  - “A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”



# Complying with the HIPAA Privacy and Security Rules

## HIPAA Hot Topics: Cloud Computing

- While extremely beneficial, there are numerous privacy and security concerns with using “the cloud” that need to be considered and addressed via guidelines and policy before fully embracing the “Cloud First” directive, especially if considering a non-government regulated/sponsored cloud. For example:
  - Data could be stored on servers (resources) that are not owned, operated, or controlled by TRICARE Management Activity (TMA) or the Federal Government, thereby resulting in a loss of control of the data
  - There is no knowledge of where the resources or systems delivering the services are located or configured and could change without notice if the contract does not explicitly prevent this
  - TMA’s data privacy rights may be disregarded if the ‘fine print’ in the contract with the cloud provider does not specifically restrict them from analyzing or searching the data for its own purposes or to sell to third parties
  - Improperly implemented federal security requirements by the cloud provider (i.e., where they find them cost-prohibitive or cumbersome)
  - The data stored by the cloud provider is breached and they do not properly inform the government or any of the individuals affected by the incident



# Complying with the HIPAA Privacy and Security Rules

## HIPAA Hot Topics: Cloud Computing

- The Assistant Secretary of Defense for Health Affairs issued “Military Health System Cloud First Adoption Directive and Policy Guidance” memorandum on May 22, 2012
  - Memo places “an administrative hold” on cloud technology programs halting all cloud development for the time being. Projects already in progress, or contractually obligated, could continue after they were reported to the MHS CIO office and reviewed
  - MHS Cloud Governance policy is forthcoming

### Key Takeaways

- Use of the ‘cloud’ is on hold until DoD policies are finalized
- Contact the Privacy Office with questions or for help



## HIPAA Hot Topics: Teleworking

- DoD and TMA support teleworking as long as the proper security controls are in place and observed
- Employees are responsible for:
  - Keeping all DoD information, government-furnished equipment (GFE) and government property safeguarded and secure
  - Using government furnished computer equipment, software, and communications, with appropriate security measures, for any telework arrangement that involves controlled unclassified information
  - Not taking classified documents (hard copy or electronic) to their homes or alternative worksites, unless approved
  - Ensuring that access to PII is only done on encrypted GFE requiring two-factor authentication for access



## HIPAA Hot Topics: Teleworking

- Not extracting PII from DoD systems onto GFE used for teleworking unless approved by a manager and logged and erased in accordance with OMB Memorandum 06-16
- Not using personal e-mail accounts for PII transmission. PII may only be e-mailed between government e-mail accounts and must be encrypted and digitally signed
- Never leaving PII unattended while in transit to a telework location
- Reporting the loss or theft of equipment/data immediately

### Key Takeaways

- Only removing the minimum amount of data from the office that is necessary and that is specifically approved
- Ensuring that access to PII is only done on encrypted GFE
- Using personal e-mail accounts for PII transmission is prohibited



# Complying with the HIPAA Privacy and Security Rules Summary

- You should now be able to:
  - Express a general understanding of the HIPAA Privacy and Security Rules and their implementation
  - Identify provisions of the HIPAA Privacy and Security Rules that have or will be modified by the HITECH Act and anticipate further guidance and regulations from HHS
  - Discuss current and relevant HIPAA Security issues including impending changes to DoD 8580.02-R, “Health Information Security Regulation”, current guidance on cloud computing, and security considerations for teleworkers



# 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, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (February 17, 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
- U.S. Chief Information Officer Memorandum, “25 Point Implementation Plan to Reform Federal Information Technology Management”, December 9, 2010



# Complying with the HIPAA Privacy and Security Rules Resources

- National Institute of Standards and Technology Special Publication 800-145, September 2011
- Assistant Secretary of Defense/Health Affairs Memorandum, “Military Health System Cloud First Adoption Directive and Policy Guidance”, May 22, 2012
- DoD Instruction 1035.01, “Telework Policy”, April 4, 2012
- TMA “Guide for Safeguarding Personally Identifiable and Protected Health Information at Alternative Duty Stations”, July 2010



# Complying with the HIPAA Privacy and Security Rules

## Resources

- 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/mailnglist.aspx>

