

JUNE 7-8, 2011

# TMA Privacy Weekly

TMA Privacy and Civil Liberties Office  
2011 DATA PROTECTION SEMINAR



## The HITECH Act: Privacy and Security Changes



# The HITECH Act: Privacy and Security Changes

## Purpose

The purpose of this presentation is to provide an overview of the Health Information Technology for Economic and Clinical Health (HITECH) Act as it affects the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules.



HEALTH AFFAIRS



TRICARE  
Management Activity

# The HITECH Act: Privacy and Security Changes

## Objectives

- Upon completion of this presentation, you should be able to:
  - Identify the areas of the HIPAA Privacy and Security Rules modified by the HITECH Act
  - Discuss changes that have been made as the result of new Department of Health and Human Services (HHS) regulations on enforcement, breach notification, and business associates (BAs) and the effective dates of those changes
  - Anticipate further guidance and regulations from HHS that will further impact privacy and security requirements



HEALTH AFFAIRS



TRICARE  
Management Activity

# The HITECH Act: Privacy and Security Changes

## Overview

- 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
  - Most provisions effective on date of enactment
  - Other effective dates depend on the issuance of regulations or guidance
- Purpose:
  - Promote widespread adoption of health information technology, striving for interoperable electronic health records (EHRs) by 2014
  - Strengthen HIPAA’s privacy and security protection of protected health information (PHI)



HEALTH AFFAIRS



TRICARE®

TRICARE  
Management Activity

# The HITECH Act: Privacy and Security Changes

## Enhanced Enforcement

- Increased penalties for HIPAA violations (effective immediately)
- Penalties tiered, based on fault and whether corrective action was taken
- \$100 per violation
- Up to \$50,000 per violation for violations due to willful neglect that are not corrected



HEALTH AFFAIRS



TRICARE  
Management Activity

## The HITECH Act: Privacy and Security Changes

# Enhanced Enforcement (continued)

- 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
  - Including compliance with the HIPAA Privacy and Security Rules
  - Including audits of covered entities (CEs) and BAs



HEALTH AFFAIRS



TRICARE  
Management Activity

## The HITECH Act: Privacy and Security Changes

# TMA Breach Notification Requirements

- HHS breach notification requirements are less stringent and **do not** supersede TMA breach notification requirements
- All breaches within the Military Health System (MHS) are to be reported
  - Within **1 hour** of discovery, to [www.us-cert.gov](http://www.us-cert.gov)
  - Within **24 hours** of discovery, to the TMA Privacy and Civil Liberties Office (Privacy Office)
- A breach is defined as an actual or possible loss of control, unauthorized disclosure of, or unauthorized access of, personal information where persons other than authorized users gain access or potential access to such information for other than authorized purposes and where one or more persons will be adversely affected



HEALTH AFFAIRS



TRICARE  
Management Activity

## The HITECH Act: Privacy and Security Changes

# TMA Breach Notification Requirements (continued)

- The Privacy Office will determine whether a breach meets the criteria of the HHS breach notification rule and what actions are necessary to ensure compliance
- The Privacy Office will report qualifying breaches to HHS
- Media notification
  - Each MHS component is responsible for establishing protocol for media notification
  - The Privacy Office will advise the MHS component when media notification is required under the HHS Breach Notification Rule
- Guidance memo was provided to the Services and MHS contractors and detailed information is on the Privacy Office Web site



HEALTH AFFAIRS



TRICARE  
Management Activity

## The HITECH Act: Privacy and Security Changes

# Breach Notification under the HITECH Act

- Interim Final Rule released August 2009, effective September 2009, and enforcement commenced February 2010
- Requires HIPAA CEs and BAs to report breaches of “unsecured PHI”
- Unsecured PHI: PHI that has not been encrypted or destroyed
  - National Institute of Standards and Technology (NIST) encryption standards for electronic data in use
  - NIST standards for purging or destructing electronic media
  - Shedding or destructing hard-copy media



HEALTH AFFAIRS



TRICARE®

TRICARE  
Management Activity

## The HITECH Act: Privacy and Security Changes

# Breach Notification under the HITECH Act (continued)

- Conditions for breach reporting:
  - Breach must involve unsecured PHI and violate the HIPAA Privacy Rule
  - Breach must pose significant risk of harm
    - To whom disclosed
    - Possibility of mitigation
    - Type and amount of information disclosed
  - Risk analysis must be conducted and documented
  - “Burden of proof” on CE and BA of CE



HEALTH AFFAIRS



TRICARE  
Management Activity

## The HITECH Act: Privacy and Security Changes

# Breach Notification under the HITECH Act (continued)

- Exceptions to breach reporting:
  - Good faith unintentional access by authorized person
  - Inadvertent disclosure by one authorized person to another
  - Unauthorized disclosure to a person who cannot reasonably retain it
- Report, with specific elements, must be given to:
  - The individual
  - Prominent media outlets if  $\geq 500$  individuals of the state are affected
  - HHS concurrently if  $\geq 500$  individuals are affected; otherwise annual log



HEALTH AFFAIRS



TRICARE®

TRICARE  
Management Activity

## The HITECH Act: Privacy and Security Changes

# Breach Notification under the HITECH Act (continued)

- Notice must be given without unreasonable delay, and no later than 60 days following disclosure (i.e., when breach is known or should have been known with reasonable diligence)
  - Specified method for providing notice
  - Substitute notice if CE does not have contact information
- Notice must be delayed at the request of law enforcement officials for the period requested (but written request is required for a delay more than 30 days)
- Reminder: TMA breach notification timelines and rules must be followed, and the Privacy Office will take or otherwise direct any follow-up action required in order to comply with the HHS breach notification requirements



HEALTH AFFAIRS



TRICARE  
Management Activity

# The HITECH Act: Privacy and Security Changes

## Business Associates

- Effective February 17, 2010 (awaiting HHS guidance)
- BA is directly subject to certain HIPAA privacy and security requirements “in the same manner that [the requirements] apply to the covered entity”
- BA must comply with the HIPAA Security Rule safeguards and documentation requirements
- BA must comply with required terms of the business associate agreement
- BA must comply with additional HIPAA privacy and security provisions of the HITECH Act that apply to CEs, including the same civil and criminal penalties



HEALTH AFFAIRS



TRICARE  
Management Activity

# The HITECH Act: Privacy and Security Changes

## Special Restriction

- Effective February 17, 2010 (awaiting HHS guidance)
- Requires CE to comply with an individual's request to restrict disclosure of PHI if:
  - Disclosure is to a health plan for payment or healthcare operations, ***and***
  - The patient pays provider “out of pocket in full”



HEALTH AFFAIRS



TRICARE  
Management Activity

# The HITECH Act: Privacy and Security Changes

## Minimum Necessary

- Effective February 17, 2010 (awaiting HHS guidance)
- Restricts use and disclosure to a “limited data set” or, if necessary, to minimum necessary when the rule applies
  - Statutory guidance to be replaced by guidance issued by HHS, which was expected within 18 months of the enactment of the HITECH Act
  - Currently, CEs and BAs must continue to adhere to the minimum necessary standard in using and disclosing of PHI



HEALTH AFFAIRS



TRICARE  
Management Activity

# The HITECH Act: Privacy and Security Changes

## Accounting of Disclosures

- Effective:
  - January 1, 2011 or date of acquisition for CEs who acquired EHR after January 1, 2009
  - January 1, 2014 who acquired EHR before January 1, 2009
  - Secretary may postpone for up to two years
- If a CE maintains an EHR, the CE is required to account for treatment, payment, and health care operations (TPO) disclosures
  - Accounting must go back three years



# The HITECH Act: Privacy and Security Changes

## Sale of PHI

- Effective 6 months after final regulations (regulations were to be issued within 18 months of enactment)
- Will restrict sale of PHI unless an individual signs a written HIPAA authorization
- Exceptions:
  - Public health
  - Cost of preparation and transmittal of data for research
  - Treatment
  - Sale of the entity
  - Payment to BAs
  - Payment by individual for copy of record



HEALTH AFFAIRS



TRICARE®

TRICARE  
Management Activity

# The HITECH Act: Privacy and Security Changes

## Electronic Copy

- Effective February 17, 2010 (awaiting HHS guidance)
- 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
- Fee not to exceed CE's labor cost



HEALTH AFFAIRS



TRICARE  
Management Activity

# The HITECH Act: Privacy and Security Changes

## Additional Marketing Restrictions

- Awaiting final regulations
- HIPAA allows a CE to be paid by a third party for marketing the CE's products, services, or benefits (“remuneration”)
- The HITECH Act prohibits remunerated marketing, except:
  - Reasonable remuneration for communications concerning drugs and biologicals currently being prescribed
  - Payment to BAs for communications on behalf of CEs



HEALTH AFFAIRS



TRICARE  
Management Activity

# The HITECH Act: Privacy and Security Changes

## Fundraising

- Awaiting final regulations
- HIPAA requires fundraising communications to contain an opt-out, and requires CEs to make reasonable efforts not to send fundraising communications to individuals who have opted out
- The HITECH Act states that an opt-out is treated as a revocation of authorization



HEALTH AFFAIRS



TRICARE  
Management Activity

## The HITECH Act: Privacy and Security Changes

# Proposed Rules – Other Potential Changes

- Other changes to the HIPAA Privacy and Security Rules in addition to those set forth in the HITECH Act are possible, in light of the proposed regulations, including:
  - Disclosures with respect to decedents
  - Research authorizations
  - Disclosures of immunization information to a school
  - Specific updates to the Notice of Privacy Practices
- Proposed rules are not binding law, but are indicative of the fact that further changes are expected to the HIPAA Privacy and Security Rules



HEALTH AFFAIRS



TRICARE  
Management Activity

# The HITECH Act: Privacy and Security Changes

## Summary

- You should now be able to:
  - Identify the areas of the HIPAA Privacy and Security Rules modified by the HITECH Act
  - Discuss changes that have been made as the result of new HHS regulations on enforcement, breach notification, and BAs and the effective dates of those changes
  - Anticipate further guidance and regulations from HHS that will further impact privacy and security requirements



HEALTH AFFAIRS



TRICARE  
Management Activity

# The HITECH Act: Privacy and Security Changes

## Resources

- 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)
- HITECH Act — Frequently Asked Questions:  
<http://www.tricare.mil/tma/privacy/faqs.aspx#section0>
- Privacy Office Standard Contract Language:  
<http://www.tricare.mil/tma/privacy/contractlanguage.aspx>
- E-mail [Privacymail@tma.osd.mil](mailto:Privacymail@tma.osd.mil) for subject matter questions
- To subscribe to the Privacy Office E-News, go to:  
<http://www.tricare.mil/tma/privacy/maillinglist.aspx>



HEALTH AFFAIRS



TRICARE  
Management Activity