

2010 Data Protection Seminar

TMA Privacy Office



HIPAA Privacy and Security Overview



HEALTH AFFAIRS



HIPAA Privacy and Security Overview

Purpose

Provide an overview of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 Privacy and Security Rules, and identify changes enacted by the Health Information Technology for Economic and Clinical Health (HITECH) Act provisions of the American Recovery and Reinvestment Act (ARRA) of 2009



HEALTH AFFAIRS



HIPAA Privacy and Security Overview

Objectives

- Upon completion of this presentation, you should be able to:
 - Identify the key DoD regulations that mirror the HIPAA Privacy and Security Rules
 - Explain the general requirements set forth in DoD Health Information Privacy Regulation and DoD Health Information Security Regulation
 - Describe the applicability of requirements to safeguard data



HIPAA Privacy and Security Overview

DoD 6025.18-R, “Health Information Privacy Regulation”

- Implements the HIPAA Privacy Rule throughout DoD
- Defines the baseline health information privacy requirements for use and disclosure of protected health information (PHI) by covered entities (CEs) and business associates (BA):
 - 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 patients' privacy rights
 - Enables patients to find out how their health information may be used and what disclosures have been made



HEALTH AFFAIRS



HIPAA Privacy and Security Overview

DoD 8580.02-R, “Health Information Security Regulation”

- Implements the HIPAA Security Rule throughout DoD
- Implements policy and assigns responsibilities for applying Technical, Physical, and Administrative security specifications for electronic PHI (ePHI) within DoD
- Complements DoD Information Assurance (IA) controls in accordance with DoD Directive 8500.1, DoD Instruction 8500.2, and Information Security Requirements, in accordance with DoD 5200.1-R



HEALTH AFFAIRS



HIPAA Privacy and Security Overview

DoD 8580.02-R, “Health Information Security Regulation”

- Addresses the implementation of Administrative, Physical, and Technical Safeguards to protect the confidentiality, integrity, and availability of data
 - Implementation specifications support specific standards with a risk-based approach
 - May be “required” or “addressable”
 - Required means that CE must carry out the implementation specification at their facility
 - Addressable means that CE must assess whether the implementation specification is reasonable and appropriate in the environment, based on specified factors



HIPAA Privacy and Security Overview

Privacy Act

- The Privacy Act of 1974
 - Safeguards records of information pertaining to individuals that Federal agencies or components own and maintain
 - Implemented in DoD via the DoD 5400.11-R, “Department of Defense Privacy Program”, May 14, 2007



HEALTH AFFAIRS



HIPAA Privacy and Security Overview

Key Definitions and Concepts

- Under DoD 6025.18-R, a CE is a health plan, a health care clearinghouse, or a health care provider who transmits health information in electronic form in connection with a transaction for which the Department of Health and Human Services (HHS) has adopted a standard
 - TRICARE Management Activity (TMA) is a health plan and thus a CE
 - Military treatment facility (MTF) is also considered CE
- CEs enter into arrangements with other organizations for provision of services involving use and disclosure of PHI
 - These organizations are called “business associates”
 - Contractors are often BAs of TMA



HIPAA Privacy and Security Overview

Key Definitions and Concepts (continued)

- DoD 6025.18-R requires that CEs and BAs enter into business associate agreements (BAAs)
 - These agreements outline the BAs responsibility to protect PHI
 - BAs are obligated to ensure that their subcontractors agree to the same restrictions and conditions that apply to the BA
- The HITECH Act, effective February 17, 2010, makes BAs subject to direct HHS enforcement and penalties with respect to certain provisions of the HIPAA Privacy and Security Rules



HIPAA Privacy and Security Overview

Key Definitions and Concepts (continued)

- BA and Contractors
 - According to the DoD Privacy Program, any contractor who may come in contact with PII/PHI will be recognized as employees of DoD
 - They must be trained in the proper handling and protection of PII/PHI



HEALTH AFFAIRS



HIPAA Privacy and Security Overview

Key Definitions and Concepts (continued)

- Workforce

- DoD 6025.18-R, “DoD Health Information Privacy Regulation” defines the workforce as:
 - “Employees, volunteers, trainees, and other persons whose conduct, in performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity”



HEALTH AFFAIRS



HIPAA Privacy and Security Overview

Key Definitions and Concepts (continued)

- Personally identifiable information (PII)
 - “Information that can be used to distinguish or trace an individual’s identity”
 - PII includes:
 - Name
 - Social Security Number
 - Age
 - Date and place of birth
 - Mother’s maiden name
 - Biometric records
 - Marital status
 - Military Rank or Civilian Grade
 - Race
 - Salary
 - Home/office phone numbers
 - Other personal information including health information, which can be linked to a specific individual



HIPAA Privacy and Security Overview

Key Definitions and Concepts (continued)

- Protected health information (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 addresses
 - Social security numbers
 - Medical record numbers
 - Health plan beneficiary numbers



HIPAA Privacy and Security Overview

Key Definitions and Concepts (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 (IP) 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, except as permitted by paragraph C8.1.4



HIPAA Privacy and Security Overview

Key Definitions and Concepts (continued)

- Minimum Necessary Standard
 - The Minimum Necessary Standard states that an organization should limit the use or disclosure of PHI, including any made for payment and/or healthcare operations, to the “minimum necessary to accomplish the intended purpose of the use, disclosure, or request”
 - It is important to note that this standard does not apply to any disclosure of PHI for treatment purposes



HIPAA Privacy and Security Overview

Using and Disclosing PHI

- Use of PII/PHI includes the sharing of information within the entity that maintains the information
 - Disclosure means the release, provision of access to, or divulging in any manner of, PHI outside the entity maintaining it
 - Rules on use and disclosure apply to all forms of PHI, including verbal, paper, and electronic



HEALTH AFFAIRS



HIPAA Privacy and Security Overview

Using and Disclosing PHI (continued)

- Workforce access and disclosure of PHI for the 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 healthcare professionals
 - Health insurance or benefit contract functions
 - Review, audit, and compliance functions
 - Business planning and management functions



HIPAA Privacy and Security Overview

Individual Rights

- Individuals:

- Are entitled to accounting of disclosures of their PHI upon request, subject to certain exceptions
- Can no longer be denied restrictions on records if the individual has paid for the service out of pocket in full
- Have a right of access to their PHI, subject to certain exceptions
- Have the right to confidential communications: Request communications of PHI by alternative means or at alternative locations
- Have the right to request amendments to their PHI



HEALTH AFFAIRS



HIPAA Privacy and Security Overview

Summary

- You should now be able to:
 - Identify the key DoD regulations that mirror the HIPAA Privacy and Security Rules
 - Explain the general requirements set forth in DoD Health Information Privacy Regulation and DoD Health Information Security Regulation
 - Describe the applicability of requirements in safeguarding data



HIPAA Privacy and Security Overview

Resources

- DoD 6025.18-R, “DoD Health Information Privacy Regulation”, January 24, 2003
- DoD 8580.02-R, “DoD Health Information Security Regulation”, July 12, 2007
- For ARRA/HITECH FAQs go to:
<http://www.tricare.mil/tmaprivacy/breach.cfm>
- To subscribe to the TMA Privacy Office E-News go to:
<http://www.tricare.mil/tma/privacy/maillinglist.aspx>
- E-mail Privacymail@tma.osd.mil for subject matter questions

