



HIPAA Privacy & Security

Marlene H. Bowen, LUTCF, RHU
MEEPICNGER & ASSOCIATES
Marlene@MeEPICngerAssociates.co
m



HIPAA Overview

- Health Insurance Portability and Accountability Act of 1999
- Privacy Rule Dec 00, modified Aug 02
- Security Rule Feb 03
- Correction of Expiration Date of Int Final Rule Apr 03
- Procedures for Investigations, Imposition of Penalties, and Hearings - Int Final Rule Apr 03
- Extension of Expiration Date of Int Final Rule Sep 04
- HIPAA Enforcement Rule – Proposed Rule Apr 05
- Extension of Expiration Date of Int Final Rule Sep 05
- HIPAA Enforcement Final Rule Feb 06
- Correction of Expiration Date of Int Final Rule Apr 03
- Procedures for Investigations, Imposition of Penalties, and Hearings Int Final Rule Apr 03
- Extension of Expiration Date of Int Final Rule Sep 04
- HI-TECH Act & Breach Notification Rule Feb 09
- HITECH & Enforcement Int Final Rule Oct 09
- Final Omnibus Rule Jan 13



HIPAA Overview

- HIPAA Portability
 - Open Enrollment
 - Special Enrollments
 - Marriage/ Divorce
 - Birth/ Adoption
 - Loss of Coverage



HIPAA Overview

- HIPAA Accountability (Administrative Simplification)
 - Electronic Transmissions and Code Set Standards –2003
 - Privacy Requirements –2003
 - Security Requirements –2005
 - National Identifier Requirements
 - Employer – EIN
 - Provider – National Provider Identifier 2007
 - Health Plan Identifier Requirements 2014



HIPAA Overview

- HIPAA Protected Health Information (PHI):
 - Information relating to an individual's past, present or future physical or mental health condition; **or** provision of health care to that person;
 - Information relating to an individual's past, present or future payment of person's health care; and
 - Information that specifically identifies an individual or causes reasonable belief that an individual may be covered.



HIPAA Overview

- Protected Health Information (PHI):
 - Names;
 - All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes;
 - All elements of dates for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates indicative of such age;
 - Telephone numbers;
 - Fax numbers;



HIPAA Overview

- Protected Health Information (PHI):
 - Account numbers;
 - Electronic mail addresses;
 - Social security numbers;
 - Medical record numbers;
 - Health plan beneficiary;
 - Certificate/license numbers;
 - Vehicle identifiers and serial numbers, including license plate numbers;



HIPAA Overview

- Protected Health Information (PHI):
 - 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.***



HIPAA Privacy

- Covered Entities: Health Care Providers, Health Plans, Health Care Clearinghouses
 - Able to access information for permitted uses
 - Cannot disclose PHI to non-covered entities
 - Exceptions:
 - Treatment, Payment & Health Care Operations (TPO)
 - Business Associates – chain of trust
 - Public Policy
 - HI-TECH Reg 2010: “reclassified” Business Associates as Covered Entities



HIPAA Privacy

- General Requirements:
 - Privacy Procedures/Notification
 - Privacy Officer
 - Current Assessment of Procedures
 - Employee Training
 - Record Retention



HIPAA Privacy

- General Requirements:
 - Minimize Incidental Uses and Disclosure
 - Minimum Necessary Standards
 - Reasonable Safeguards
 - Personal Representatives
 - Business Associate Agreements



HIPAA Privacy

- Health Plan Requirements:
 - Firewalls between covered and non-covered functions
 - PHI not used for employment or administration of any other plan



HIPAA Security

- HIPAA Security - Confidentiality, Integrity & Availability of ePHI
 - Administrative Safeguards
 - Technical Safeguards
 - Physical Safeguards



HIPAA Security

- Administrative Safeguards
 - Policies and Procedures designed to prevent, detect, contain and correct security violations



HIPAA Security

- Physical Safeguards
 - Assigned Security Responsibility
 - Media Controls
 - Accountability
 - Data Backup
 - Disposal of PHI



HIPAA Security

- Technical Safeguards
 - Access Control
 - User Name/Password
 - Audit Controls
 - Authorization Controls
 - Data & Entity Authentication
 - Automatic Log-off
 - Unique User ID



HIPAA Security

- HI-TECH (2010) – Security Breach Requirements
 - Notification to Individuals Affected
 - Reporting to Covered Entity
 - Reporting to HHS



HIPAA Non-Compliance

- HI-TECH (2010)
 - Formal investigation on all complaints
 - Mandatory audits
 - Required imposition of penalties
 - Increased penalty amounts
 - State attorney general may file suit
 - Allows penalties to be assessed against organization ***and individual***



HIPAA Non-Compliance

TABLE 2.—Categories of Violations and Respective Penalty Amounts Available

Violation Category – Section 1176(a)(1)	Each Violation	All Such Violations of an Identical Provision in a Calendar Year
(A) Did Not Know	\$100 - \$50,000	\$1,500,000
(B) Reasonable Cause	\$1,000 - \$50,000	\$1,500,000
(C)(i) Willful Neglect-Corrected	\$10,000 - \$50,000	\$1,500,000
(C)(ii) Willful Neglect-Not Corrected	\$50,000	\$1,500,000



HIPAA Non-Compliance

- \$750,000 - University of Washington Medicine, Need for Organization Wide Risk Analysis 12/14/15
- \$3.5 Million - Triple-S Management Corporation, Minimum Necessary use of PHI 11/30/15
- \$850,000: Lahey Hospital and Medical Center, unencrypted laptop stolen 11/25/15
- \$750,000 - Cancer Care Group, P.C, unencrypted laptop stolen 09/02/15
- \$218,400 - St. Elizabeth's Medical Center, use of internet-based document sharing application to ePHI store documents without analysis of associated risks 07/10/15
- \$125,000 - Cornell Prescription Pharmacy, disposal of unsecured documents containing PHI



Privacy & Security

Q & A