Getting Hip to the HIPAA and HITECH Act Compliance

NaNotchka M. Chumley, D.O., M.P.H.
Family Medicine Physician
Los Angeles, CA

“Integrating Global Trade & Logistic and Cybersecurity”
Westin St. Francis, Union Square, San Francisco, CA
November 13, 2015
MODERATOR
Dr. NaNotchka M. Chumley
Family Medicine
Panelists

Dr. Katrina Peters
• General and Forensic Psychiatrist

Dr. Suzanne Cutter
• Surgical Oncologist
HIPAA: Health Insurance Portability and Accountability Act

- Health Insurance Portability and Accountability Act of 1996, law 104-191, 110 Statute 1936
- Enacted August 21, 1996 by United States Congress and signed by former President Bill Clinton
- AKA: The Kennedy-Kassebaum Act. named after 2 of its leading sponsors
- It defines policies, and guidelines procedures for maintaining the privacy and security of individually identifiable health information
- Outlines numerous offenses relating to healthcare and sets civil and criminal penalties for violations
- Creates several programs to control fraud and abuse within the healthcare system
- Requires the establishment of National standards for electronic healthcare transactions (EHR) and National identifiers for providers, health insurance plans and employers
5 HIPAA Rules

1. The Privacy Rule
2. The Transition and Code Sets Rule
3. The Security Rule
4. The Unique Identifiers Rule
5. The Enforcement Rule
The Privacy Rule

• Major goal
  – Assure that your health information is protected
• Includes demographic information that relates to an individual's, past, present or future physical, mental health or condition that can be used to identify a member
• The provision of health care to an individual
• The past, present or future payment for the provision of healthcare to the individual and
• Protected health information, protection to business associates, trading partners and their associates through formal contract
The HIPAA Privacy Regulations Impact

- All functions;
- Information systems;
- Personnel;
- Facilities;
- Policies and Procedures
Major HIPAA Privacy Rule Requirements

• Notice of Information Practices
• Minimum Necessary Information Release
• Patient Privacy Requirements
• Staff Training
• Formal Documentation Requirements
HIPAA Requirements

- Patient Consent
- Patient Authorization
- Minimum Necessary Disclosure
- Oral Communications
- Business Associates
- Right of Access
- Right to Amend
- Right of Accounting for Disclosures of PHI
- Privacy Official
- Dispute Resolution
- Privacy rule documentation
The Security Rule

- Establishes national standards to protect individuals' electronic personal health information that is received, created, used or maintained by a covered entity (organizations subject to the privacy rule)
The Security Rule

• Physical and technical safe guards to ensure
  – The Confidentiality
  – The Integrity and
  – The Availability and
  – The Security of electronic protected health information
The Security Rule

- The security regulations enable much of the confidentiality protection as well as ensuring availability following:
  - Emergencies
  - Natural Disasters
  - Other interruptions to service
The Security Rule

• The security regulations protects the *availability* of the electronic data

• Ensure that
  – It is available when needed by authorized personnel or information systems
  – Not available
    • Inadvertently or
    • Maliciously to personnel not authorized to receive the information
The Security Rule

- Protects the *integrity* of the electronic data
  - Ensures that data is not inadvertently or maliciously altered

- Security measures include
  - Computer and network security
  - Encryption of all data
  - User authentication
TOP 10 Tips for Cybersecurity in Healthcare

- Establish a security culture
- Protect Mobile Devices
- Maintain good computer habits
- Use a firewall
- Install and maintain antivirus software
- Plan for the unexpected
- Control Access to protected Health Information
- Use strong passwords and change them regularly
- Limit Network Access
- Control physical Access
The Enforcement Rule

• Secretary of HHS adopted enforcement and penalties:
  – Compliance
  – Civil money penalties
  – Criminal penalties
# The Numbers

<table>
<thead>
<tr>
<th>Description</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monetary settlements</td>
<td>$21,906,500</td>
</tr>
<tr>
<td>HIPAA Privacy Rule Violations</td>
<td>$4.3 Million</td>
</tr>
<tr>
<td>Monetary Resolution Agreements</td>
<td>$15,581,000</td>
</tr>
<tr>
<td>Complaints received HIPAA Privacy Rule</td>
<td>115,929</td>
</tr>
<tr>
<td>Number of cases Investigated and resolved</td>
<td>23,580</td>
</tr>
</tbody>
</table>
The Numbers

- Lost or stolen laptops, smart phones, and computer tablets account for 39% of the security incidents in healthcare and
- 78% of the records compromised in security breaches
HIPAA Risk Assessment

• The nature and extent of the PHI breach
• The unauthorized person who used the PHI or to whom the disclosure was made
• Whether the PHI was actually acquired or viewed
• The extent to which the risk to the PHI has mitigated
HIPAA 4 Things To Avoid

1. Texting or emailing unencrypted PHI
2. Failure to conduct a Risk Analysis
3. Failing to update the notice of private practices
4. Not providing sufficient training
HITECH Act
Health Information Technology for Economic and Clinical Health Act

- Designed to promote wide spread adoption and standardization of health information technology and requires the DHHS to modify the HIPPA Privacy, Security and Enforcement rules to strengthen the privacy and security protections for health information and to the workability and effectiveness of the HIPPA rules
HIPAA & Medical Providers

• HIPPA becomes a tangle for medical providers
• The law requires that your medical information be protected
  – Keeping your medical records under lock and key, or password protected and file encryption or digital information stored on a hospital's network
  – Requires your doctor to give you a notice telling you all about HIPPA
• The HIPPA privacy rule applies the concept of minimum necessary information consistent with its use
Follow your heart, but take your brain with you.
References

• US Department of Health and Human Services
• Office for Civil Rights
• Medical Economics.com/
• Medical Economics.com/2015-Best- EHRs
• http://www.hhs.gov/ocr/hippa
Acronyms

- HIPPA
  - Health Insurance Portability and Accountability Act (HIPPA)
- PHI
  - Protected Health Information (PHI)
- OCR
  - Office of Civil Rights (OCR)
- HHS
  - U.S. Department of Health and Human Services (HHS)
- HITECH
  - Health Information Technology for Economic and Clinical Health Act (HITECH)
- CI
  - Covered Entities (CI)
    - Health plans, healthcare providers and health care clearing houses
- NPP
  - Notice of Privacy Practices (NPP)
- TPO
  - Treatment, payment and health care operations (TPO)