Privacy & Security Updates Under Health Care Reform

Health TechNet

April 16, 2010

General Overview

- **HIPAA** - The Health Insurance Portability & Accountability Act of 1996
- **The Privacy Rule** – Created national standards to protect the privacy of personal health information.
- **The Security Rule** – Created national standards for the security of electronic health care information.
- **The HITECH Act** – Established security breach notification requirements and revised HIPAA regulations regarding privacy and security
- **PPACA** – The Patient Protection and Affordable Care Act

How HITECH Changes HIPAA

- Prior to the HITECH Act
  - The regulations applied only to “Covered Entities”
  - Indirectly regulated “Business Associates” of Covered Entities
- HITECH Act expands the reach of HIPAA Privacy and Security Rules
  - Business Associates must comply with the HIPAA Security Rule
  - Business Associates are subject to civil and criminal penalties if Business Associate Agreement provisions are violated
- And creates standards for the “meaningful use” of protected health information

The Privacy Rule

pillsbury

What Information is Protected?

- The Privacy Rule protects against the improper use or disclosure of **Protected Health Information** (PHI).
- The Privacy Rule operates to protect the confidentiality of PHI by:
  - increasing patients' rights,
  - limiting a provider's use and disclosure of PHI.
- PHI is defined as individually identifiable health information (IIHI) that is:

  (1) transmitted by electronic media,
  (2) maintained in any electronic media, or
  (3) transmitted or maintained in any other form or medium.

Uses and Disclosures…

"You can't just walk in and ask to access patient records. HIPAA would call that fantasizing."

pillsbury

Disclosures: *Minimum Necessary* Standard

- Covered Entities must make reasonable efforts to limit use or disclosure of PHI to the Minimum Necessary amount to accomplish the intended purpose of the use of the information, when using or disclosing PHI.

- The information disclosed must:
  - be consistent with and directly related to the purpose of the use or disclosure; and
  - take into consideration the ability of the Covered Entity to restrict the amount of information used or disclosed and the relative burden on the entity.

- Minimum necessary guidelines forthcoming …

The Security Rule

pillsbury

The Security Rule

- Complements the Privacy Rule. Deals specifically with electronic PHI (E-PHI).
- General Requirements - Covered Entities must do the following:
  - Ensure confidentiality, integrity, and availability
  - Protect against any reasonably anticipated threats or hazards;
  - Protect against any reasonably anticipated uses or disclosures; and
  - Ensure compliance by the workforce.
- New: Direct applicability to Business Associates

Security Rule Safeguards

- **Administrative Safeguards** – Operational requirements, administrative actions and policies and procedures that build the entity's security infrastructure
- **Physical Safeguards** – Physical measures and policies and procedures needed to protect information systems (and the buildings they are in) from hazards and unauthorized access
- **Technical Safeguards** – Technological requirements and policies and procedures to protect E-PHI

HITECH

The HITECH Act

- Health Information Technology for Economic and Clinical Health Act of 2009
- Business Associates must comply with the HIPAA Security Rule.
  - February 17, 2010 effective date but …
    - …Delay in enforcement.
- Establishes new security breach notification requirements – applicable to breaches of unsecured PHI.

HITECH: Key Privacy Elements

- **Business Associates**
  - The Security Rule: Direct application to Business Associates.
  - Business Associates also subject to civil and criminal penalties for violating HIPAA.
  - Business Associate Agreements remain relevant.
  - If Business Associate knows of a material breach by a Covered Entity, Business Associate must cure or terminate Agreement.
  - If neither cure nor termination is possible, report breach to HHS.
- **"Minimum necessary" exceptions; regulations still outstanding**
- **Accounting for PHI disclosures by Covered Entities using EHRs.**
- **Prohibition on sale of PHI**
  - No sale of PHI without valid patient authorization.
  - Regulations by August 2010.

HITECH: Key Elements

- **New restrictions on using PHI to contact individuals for promotion of products or services**
- **Enforcement through state attorneys general**
- **Increased Penalties**
  - Extends criminal penalties for wrongful disclosure
  - Increased civil penalties for HIPAA violations
  - Authorization of State Attorneys General to bring civil actions against HIPAA violators
- **Patient Privacy Rights**
  - Access Right: Patients may receive an electronic copy of their PHI.
  - Request Restrictions: Patients may request specific PHI not be disclosed.

HITECH: Breach Notification Rule

HHS Breach Notification Rule - Breach of Unsecured PHI

- Breach notification only applies to “unsecured” PHI

- Only two methods for securing PHI:
  - Encryption
  - Destruction
    - Complete destruction such that information cannot be read or reconstructed (*e.g.*, shredded, destroyed or erased)

HHS Breach Notification Rule - Breach of Unsecured PHI

- "Breach" means:
  - Unauthorized access, use or disclosure of PHI
  - That compromises the security, privacy or integrity of the PHI
    - "Significant risk of financial, reputational or other harm to the individual."
  - Does not include unintentional disclosures if made in good faith and within course and scope of employment or Business Associate relationship

Steps to Determine Whether a Use or Disclosure of PHI is a Breach

- Was the PHI “unsecured”?
- Was the use or disclosure of PHI permissible?
- If impermissible, did the use or disclosure compromise the privacy or security of PHI by creating significant risk of financial, reputational, or other harm to the individual?
- Is the incident excluded from the definition of a breach?
  - Unintentional use?
  - Inadvertent disclosure?
  - Inability to retain PHI?

Notice Requirements – Timing

- Notice must be provided "without unreasonable delay" and no later than 60 calendar days after discovery
  - 60-day period is outer limit
  - *"facts and circumstances" test*
- Deemed knowledge of a breach if the breach is known, or by exercising reasonable diligence, would have been known
  - To any person, other than the person committing the breach
  - Who is a workforce member or agent of the Covered Entity (or an employee, officer or other agent of the Business Associate)

Responsibility for Notice

- HITECH Act requires Covered Entities to notify each individual whose unsecured PHI has been or is reasonably believed to have been accessed, acquired, or disclosed
  - Business Associate Agreement may shift this responsibility to the Business Associate
- Business Associates must notify Covered Entities of a breach and identify affected individuals

Other HITECH Regulations

HITECH Regulations

CMS Notice of Proposed Rule Making (NPRM) for EHR Incentive Program

Defines the provisions for incentive payments to eligible professionals and hospitals participating in Medicare and Medicaid programs that adopt and meaningfully use certified EHRs.

ONC Interim Final Rule (IFR) on Standards and Certification Criteria

Proposes initial set of standards, implementation specifications, and certification criteria to "enhance the interoperability, functionality, utility, and security of health IT and to support its meaningful use."

- Encryption requirements

ONC Rule on Certification Process (*forthcoming*)

Will address the process by which EHR systems will be certified or by which accreditation/certification entities can become recognized by CMS in order to certify EHR systems.

Patient Protection and Affordable Care Act

PPACA – Privacy Implications

- Data collection/reporting
  - HHS to collect data on quality measures to support health care delivery – must be aligned with the expansion of HIT systems under ARRA
  - Review Medicare claims data to measure the performance of providers and suppliers in ways that protect patient privacy
  - Modernization of CMS's computer and data systems to support improvements in care delivery
- Standards/measures
  - Administrative simplification – efficiency through reducing clerical burden on providers, patients, and health plans
  - Interoperability of systems

HITECH Compliance Steps and Action Items

- Identify systems that have covered data
- Secure PHI – Encrypt or Destroy
- Evaluate existing privacy and security policies and procedures – assess whether current administrative, technical, and physical safeguards are sufficient
- Adopt incident response plan with breach notification policy

HITECH Compliance Steps and Action Items

- Review and negotiate Business Associate Agreements
  - Specify timing for Business Associate to notify Covered Entity of a breach
  - Specify scope of information to be reported
  - Assign responsibility for preparing and sending notifications
- Workforce training – explain when a breach occurs and how to report it

Best Practices

pillsbury

Contact:

Douglas A. Grimm, FACHE

Pillsbury Winthrop Shaw Pittman LLP

2300 N Street, N.W.

Washington, D.C. 20037

202-663-8283

douglas.grimm@pillsburylaw.com

Cathy Gomez, MPA

Compliance Officer

Fairfax Neonatal Associates, P.C.
Management Consultants for
Affiliated Physicians, Inc.

2730-B Prosperity Avenue

Fairfax, Virginia 22031

703-289-1429

cgomez@mcapmd.com