HIPAA IN THE WORKPLACE
September 27, 2013
Deborah C. Hiser
Julianne P. Story

Agenda

- HIPPA/HITECH overview.
- Employee conduct posing risk.
  - Social media (photography, posting, blogging).
  - Snooping.
  - Lost laptops.
  - Communicating with patients (email, texting).
- Best practices to minimize risk.
- Penalties.
HIPAA/HITECH Overview: How are Things Different?

- HITECH Omnibus Final Rule Changes:
  - Business Associate Requirements
  - Limits on Fundraising and Marketing
  - Sale of PHI
  - Expanded Patient Rights (NPP, Restrictions, Access, Gina)
  - Breach Notification
  - Penalties

BIG Changes for Business Associates and Subcontractors

Chain of Trust Concept

- A subcontractor means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of the workforce of such business associate
BIG Changes for Business Associates and Subcontractors

Subcontractors Must

- Comply with the technical, administrative, and physical safeguard requirements under the Security Rule and are liable for Security Rule violations
- Comply with use or disclosure limitations expressed in its contract and those in the Privacy Rule and criminal and civil liabilities attach for violations

Not a completely new concept for Texas BUT……

- Liability flows to all subcontractors
- CE under an obligation to get written assurances from their BAs

Expanded Rights: Notice of Privacy Practices

NPP to Include a Statement That:

- Uses and disclosure of PHI for marketing requires authorization
- Disclosures that constitute a sale of PHI require authorization
- If CE intends to contact an individual to raise funds, patient has the right to opt out
- If health plan uses PHI for underwriting, CE is prohibited from using genetic information for those purposes
- CE has to agree to certain restrictions if patient has paid in full, out-of-pocket
- CE must notify affected patients following a breach (check state laws of breach!)
Expanded Rights: Requests for Restriction

**Change of Law**
- CE must agree to a requested disclosure restriction if:
  - Disclosure is for payment or health care operations purposes and is not otherwise required by law; and
  - The PHI pertains solely to a health care item or service for individual, or person other than the health plan on his/her behalf, has paid covered entity in full.

**Action Item**
- Update policies and procedures
- Update BA Agreements

Expanded Rights: Access

**Change of Law**
- If CE uses or maintains an EHR with PHI of an individual, individual shall have the right to obtain from CE a copy of such information in electronic format and individual may direct CE to transmit such copy directly to the individual's designee, provided that any choice is clear, conspicuous, and specific.
- TX Law: H.B. 300 has a faster turnaround time!

**Action Items**
- Update policies and procedures
- Update patient forms
- Update BA
Expanded Rights: Genetic Information

GINA Provisions:

- Requires “Genetic Information” be treated as PHI
- Prohibits Health Plans from using/disclosing genetic information for underwriting purposes
- Terms and definitions track regulations prohibiting discrimination in provision of health insurance based on genetic information

Marketing

Change In Law

- Authorization required for all treatment and health care operation communications where CE receives financial remuneration for making communications
- Exceptions (refill reminders, treatment, case management)

Action Items

- Update policies and procedures
- Don’t forget to incorporate state law, if any
- Update authorization form
Prohibition on Sale Of PHI

**Update**
- PHI cannot be sold without patient authorization
- Many exceptions:
  - Public health
  - Research (limited to cost-based fee)
  - Treatment/Payment
  - Sale, transfer, merger/consolidation
- CEs/BAs need to evaluate all situation where PHI is sold

**BREACH**

The interim final regulation clarified that statute incorporated a “risk of harm” threshold – notice is required where there is a “significant risk of financial, reputational or other harm.”

CEs have been reporting breaches under this standard for two years.
**BREACH**

The Big News

Two significant changes:

- Modified the “presumption” for breach reporting
- Notification is required to affected individuals unless CE/BA “demonstrate there is a low probability that the PHI has been compromised based on a risk assessment.”

---

**BREACH**

Risk Assessment

- CE/BA must perform a “risk assessment” to determine if there is a low probability of a “compromise” of the PHI.
- If risk assessment reveals a low probability of compromise, notification is not required.
- CE/BA can provide notice without a risk assessment.
BREACH: Elements of Risk Assessment

- The nature and extent of PHI involved, including types of identifiers and likelihood of re-identification;
- The unauthorized person who used the protected health information or to whom the disclosure was made;
- Whether the protected health information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated—Can it be used, for example, for ID theft, Medical ID Fraud, hackers to destroy integrity, can forensics say it was accessed/used?

Employee Conduct Posing Risk: Social Media

- Many benefits:
  - Easy & effective mode of communication
  - Marketing opportunity
  - Bolster professional relationships
- Downside: Immediate and broad dissemination of information. Disgruntled employees use social media to criticize employers/patients
- Deliberate vs. inadvertent disclosure
Employee Conduct Posing Risk: Social Media – Examples:

Innovis Health – use of Facebook to communicate unauthorized shift change updates to co-workers;
Westerly Hospital – Rhode Island physician posted information on personal Facebook page regarding trauma patient.
Byrnes v. Johnson County Community College – nursing student posted photo of placenta on FB.
Nurse fired for posting on personal FB page she treated a “cop killer” after many news accounts named the accused shooter and the hospital at which he was treated.

Employee Conduct Posing Risk: Snooping

- Kaiser Permanente’s Bellflower Hospital – (2009) fined $250,000 for failing to prevent employees from accessing Octomom’s records.
- Cedars Sinai Medical Center – (2013) 6 employees terminated after accessing records of Kardashian baby.
- UCLA Health System settlement with OCR (2011) after employees snooped into celebrity medical records.
  - Monetary payment of $865,000
  - Implement new security privacy rules
  - Improve employee training
  - Discipline employees for violations
  - Designate independent compliance monitor
Employee Conduct Posing Risk: Camera Phones

- Photography is easy.
- Photos can be easily shared, including on social media.
- Once shared cannot be deleted (breach can be ongoing)
- Can be done surreptitiously.
- Photos can be PHI (even without patient name).

Examples:
- Mayo Clinic’s Phoenix Hospital – inappropriate photograph of a patient under anesthesia.
- University of New Mexico Hospital – photos of ER patient’s injuries posted on MySpace.
- Martin Medical Center in Florida – photos of shark attack victim shared with friends (2010)

National Labor Relations Act

- Employees have the right to self-organization, to form, join or assist labor unions, to bargain collectively, and to engage in “concerted activities” for mutual aid or protection (Section VII).
- It shall be an unfair labor practice for an employer to interfere with, restrain or coerce employees in the exercise of the rights guaranteed by Section VII.
- NLRB standard: Whether the rule would unreasonably tend to chill employees in the exercise of their Section VII rights.
NLRB: Social Media Can Be “Concerted Activity”

- Employees have a legal right under the NLRA to discuss their working conditions on social media websites.
- Concerted activity v. individual employee rights.
- Unique tension in Healthcare environment.

Employee Conduct: Communications With Patients

- Email and Texting
  - April 2012 survey: 73% of physicians text other physicians at work.
  - Do texts constitute “medical record”.
  - Security-Privacy/preservation concerns.
  - Check state law
Employee Conduct: Lost or Stolen Laptop

- Hacking/IT Incident: 7%
- Improper Disposal: 5%
- Other: 1%
- Unauthorized Access/ Disclosure: 18%
- Theft: 50%
- Loss: 17%

First HIPAA breach settlement involving less than 500 patients

Hospice of North Idaho
$50,000

- Stolen laptop with ePHI of 441 patients
- Failed to include laptops and other mobile devices in security risk assessment
Best Practices: Laptops

- No PHI on personal laptops
- All PHI on laptops is encrypted
- If company issued laptops are removed, check in-check out system
- All laptops have kill switch
- Same policies re: mobile phones & iPads/Notebooks

Best Practices: Policies

- Confidentiality
  - Emphasize policy
  - Identify Privacy Officer
- Security
  - Encryption
  - Encourage reporting of violations
  - Address texting
  - Address photography
Best Practices: Policies

- Employee Discipline
  - Clearly specific prohibited conduct
  - Clearly specify consequences of violation
  - Follow through

- Social Media
  - Clearly describe protection for PHI
  - Prohibit posting or discussing patient information on social media (even if name is not used)
  - Use specific examples
  - Consider banning access to social media on work computers
  - Cannot prohibit use of logo
  - Be mindful of NLRA protections

- Computer use

Employee Training

- When:
  - New hires
  - Periodic/regular update
  - Follow-up training
  - Check state law

- What:
  - Confidentiality obligations
  - Define PHI
  - Social media/computer use
  - Discipline – set forth disciplinary consequences for violations
  - Allow for discretion in enforcement
  - Enforce consistently
Audits: What to Expect

Lessons Learned From Piedmont

1. Establishing and terminating user’s access to systems housing ePHI
2. Emergency access to electronic information systems
3. Inactive computer sessions (periods of inactivity)
4. Recording and examining activity in information systems that contain or use ePHI
5. Risk assessments and analysis of relevant information that house or process ePHI data.
6. Employee sanction policies
7. Incident reports
8. Audit logs and access reports
9. Listing of all network perimeter devices, i.e. firewalls and routers
Audits: What to Expect

(continued)

10. Remote access activity (network infrastructure platform, access servers, authentication and encryption software)
11. Password and server configurations
12. Antivirus software
13. Maintenance and repairs of hardware, walls, doors, and locks in sensitive areas

---

Audits: What to Expect

(continued)

Site Visits

- Personal Interviews with CE leadership
- Up Close and Personal Examination
- Policy Consistency
- Observation
Audits: What to Expect

Auditor Reports

| Auditors will develop a draft report | Final report submitted to OCR | OCR may initiate compliance review for serious issues | If they do, you will be subject to a CAP |

Penalties

- HIPAA Civil
  - Civil - $100 per violation to maximum of $1.5M per year.
- State Statutory
- State common law tort action
  - Invasion of privacy
  - Intentional/negligent infliction of emotional distress
New Civil Monetary Penalty System

- **Accidental**
  - $100 each violation
  - Up to $25,000 for identical violations, per year
- **Not Willful Neglect, but Not Accidental**
  - $1,000 each violation
  - Up to $100,000 for identical violations, per year
- **Willful Neglect, Not Corrected**
  - $50,000 each violation
  - Up to $1.5 million per year

And...Don’t forget about Criminal Penalties

- **Criminal**
  - Up to $250,000 fine
  - Imprisonment up to 10 years
- **“Knowingly”**
  - $50,000
  - Imprisonment up to one year
- **False pretenses**
  - Up to $100,000 fine
  - Up to five years in prison
- **Intent to sell, transfer, or use for commercial advantage, or for personal gain or malicious harm**
  - $250,000
  - Imprisonment for up to ten years
Recent OCR Enforcement Cases

**Mass. Gen. Hosp.** – Employee left 192 patient files containing HIV/AIDS PHI on subway that were never recorded. $100,000,000 penalty and 3 year CAP

**Phoenix Cardiac Surgery** – failed to secure Patient Calendar Appointment App. $100,000, 3 year CAP

---

**Recent OCR Enforcement Cases**

**WellPoint Inc. Managed Care Company**

- Important message for CEs to take caution when implementing changes to information systems, especially when changes involve updates to Web-based applications or portals that are used to provide access to consumers’ health data using the Internet.

- HHS began investigation following breach report from WellPoint as required by HITECH indicating security weaknesses in an online application database that left ePHI of 612,402 individuals accessible to unauthorized individuals over the Internet.

- **$1.7 million penalty**

- OCR’s investigation indicated that WellPoint did not implement appropriate administrative and technical safeguards as required under the HIPAA Security Rule.
Whether systems upgrades are conducted by covered entities or their BA's, HHS expects organizations to have in place reasonable and appropriate technical, administrative and physical safeguards to protect the confidentiality, integrity and availability of electronic protected health information – especially information that is accessible over the Internet.

Recent OCR Enforcement Cases

- Affinity Health Plan, Inc. - settled potential violations of HIPAA Privacy and Security Rules for $1,215,780.
- Affinity impermissibly disclosed PHI of up to 344,579 individuals when it returned multiple photocopiers to leasing agent without erasing data contained on copier hard drives.
- Affinity failed to incorporate ePHI stored in copier’s hard drives in its analysis of risks and vulnerabilities under Security Rule, and failed to implement policies and procedures when returning hard drives to leasing agents.
2012 Ponemon Institute Study

- Healthcare industry loses $7 billion a year due to HIPAA data breaches
- Average economic impact of a data breach has increased by $400,000 to a total of $2.4 million since 2010
- 94% of CEs have had at least one data breach in the last two years
- Average number of lost or stolen records per breach is 2,769
- Top 3 causes of data breaches:
  - Lost or stolen computing device (46%)
  - Employee mistakes or unintentional actions (42%)
  - Third party snafus (42%)
- 18% of CEs say medical identity theft was a result of a data breach
- Annual security risk assessments are done by less than half (48%) of CEs
- 48% of data breaches in 2012 involved medical files
- Primary activity by CEs to comply with HIPAA training is awareness training of all staff (56%), followed by vetting and monitoring of third parties, including business associates (49%)

Questions?