HIPAA/HITECH for Health Plans: Sifting through New Requirements to Achieve Compliance

Managed Care Compliance Conference
February 13, 2012

“The Regulation Waiting Game”

- Devin McGraw, Director of the Health Privacy Project at the Center for Democracy & Technology
Today’s Discussion

- What’s Going on While We’re Waiting?
- Where are we Today with the “new” HIPAA?
- What you can and should be doing now
- What to expect in the coming weeks/months

The American Recovery & Reinvestment Act of 2009 (ARRA)

- “Stimulus bill”
- HITECH Act (Health Information Technology for Economic and Clinical Health)
  Subtitle D – Privacy
- First major changes to HIPAA since 2001
- “HIPAA on steroids”
Both Frequency & Severity of Enforcement Is Increasing...

Resolution through CIVIL MONETARY PENALTIES

- New Civil Monetary Penalties under HITECH in effect since 2/2010
- Mandatory penalties for “willful neglect”

<table>
<thead>
<tr>
<th>Level of Intent/Neglect</th>
<th>Each Violation</th>
<th>All Identical Violations per CY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Without Knowledge</td>
<td>$100 - $25,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Based on reasonable cause</td>
<td>$1000 – $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful neglect</td>
<td>$10,000 – $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful neglect, not corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

David Holtzman, OCR, HCCA Compliance Institute, April 2010
UCLA Health System Settles Potential Violations of the HIPAA Privacy and Security Rules

- July 2011

The University of California at Los Angeles Health System (UCLAHS) has agreed to settle potential violations of the HIPAA Privacy and Security Rules for $865,500...

Resolution Agreement resolves 2 separate complaints on behalf of two celebrity patients who received care at UCLAHS

Complaints alleged that UCLAHS employees repeatedly and without permissible reason looked at the electronic protected health information of these patients.

Massachusetts General Hospital Settlement

$1 Million dollar settlement February 2011

Entered Corrective Action Plan (CAP) with federal government

Case stems from paper records lost on a subway
$4.3 Million Civil Money Penalty for Violations of HIPAA Privacy Rule

Cignet Health, MD (October 2010)

CMP based on the violation categories and increased penalty amounts authorized by HITECH Act

Violated 41 patients’ rights by denying them access to their medical records

• $1.3 million for denying access to patients
• $3.0 million for failing to cooperate with OCR’s investigations. Failure to cooperate was due to Cignet’s willful neglect to comply with the Privacy Rule.

Criminal Conviction for Man Who Accessed Computer of Competing Medical Practice

• January 24, 2012; Atlanta, Georgia
• Eric McNeal sentenced for:
  – intentionally accessing competing medical practice’s computer (former employer)
  – taking personal information of patients
  – sending marketing materials to patients at the other practice
• Sentenced to 1 year, 1 month in prison to be followed by 3 years of supervised release, and ordered to perform 120 hours of community service
• Inappropriate access; “cybercrime”
HITECH: Breach Notification

- Breach = an “unauthorized acquisition, access, use or disclosure of protected health information which compromises the security or privacy of the protected health information”.
  - Effective September 23, 2009
  - Must be a violation of the HIPAA Privacy Rule
  - Definition of PHI important

Privacy Rule Standards (56)

1. Permitted & required uses and disclosures of PHI
2. Minimum Necessary
3. Uses & disclosures subject to agreed upon restriction
4. Uses & disclosures of de-identified data
5. Disclosures to business associates
6. Deceased individuals
7. Personal representatives
8. Confidential communications
9. Uses & disclosures consistent with Notice
10. Disclosures by Whistleblowers & workforce member crime victims
11. Business associate contracts
12. Requirements for group plans
13. Requirements for CEs with multiple covered functions
## Privacy Rule Standards

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.</td>
<td>TPO: permitted uses &amp; disclosures</td>
</tr>
<tr>
<td>15.</td>
<td>Consent for uses &amp; disclosures</td>
</tr>
<tr>
<td>16.</td>
<td>Authorizations for uses &amp; disclosures</td>
</tr>
<tr>
<td>17.</td>
<td>Uses &amp; disclosures for facility directories</td>
</tr>
<tr>
<td>18.</td>
<td>Uses &amp; disclosures for involvement in individual’s care &amp; notification purposes</td>
</tr>
<tr>
<td>19.</td>
<td>Uses &amp; disclosures required by law (beginning of 164.512)</td>
</tr>
<tr>
<td>20.</td>
<td>Uses &amp; disclosures for public health activities</td>
</tr>
<tr>
<td>21.</td>
<td>Disclosures about victims of abuse, neglect or domestic violence</td>
</tr>
<tr>
<td>22.</td>
<td>Uses &amp; disclosures for health oversight activities</td>
</tr>
<tr>
<td>23.</td>
<td>Disclosures for judicial &amp; administrative proceedings</td>
</tr>
<tr>
<td>24.</td>
<td>Disclosures for law enforcement purposes</td>
</tr>
<tr>
<td>25.</td>
<td>Uses &amp; disclosures about decedents</td>
</tr>
<tr>
<td>26.</td>
<td>Uses &amp; disclosures for cadaveric organ, eye or tissue donation purposes</td>
</tr>
<tr>
<td>27.</td>
<td>Uses &amp; disclosures for research purposes</td>
</tr>
<tr>
<td>28.</td>
<td>Uses &amp; disclosures to avert a serious threat to health or safety</td>
</tr>
<tr>
<td>29.</td>
<td>Uses &amp; disclosures for specialized government functions</td>
</tr>
<tr>
<td>30.</td>
<td>Disclosures for worker compensation (end of 164.512)</td>
</tr>
<tr>
<td>31.</td>
<td>De-identification of PHI</td>
</tr>
<tr>
<td>32.</td>
<td>Minimum necessary requirements</td>
</tr>
<tr>
<td>33.</td>
<td>Limited data set</td>
</tr>
<tr>
<td>34.</td>
<td>Uses &amp; disclosures for fundraising</td>
</tr>
<tr>
<td>35.</td>
<td>Uses &amp; disclosures for underwriting and related purposes</td>
</tr>
<tr>
<td>36.</td>
<td>Verification requirements</td>
</tr>
</tbody>
</table>
# Privacy Rule Standards

<table>
<thead>
<tr>
<th>37.</th>
<th>Notice of Privacy Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>38.</td>
<td>Right to request privacy protection for PHI</td>
</tr>
<tr>
<td>39.</td>
<td>Confidential communications requirements</td>
</tr>
<tr>
<td>40.</td>
<td>Access to PHI</td>
</tr>
<tr>
<td>41.</td>
<td>Right to amend</td>
</tr>
<tr>
<td>42.</td>
<td>Right to accounting of disclosures of PHI</td>
</tr>
<tr>
<td>43.</td>
<td>Personnel designations</td>
</tr>
<tr>
<td>44.</td>
<td>Training</td>
</tr>
<tr>
<td>45.</td>
<td>Safeguards</td>
</tr>
<tr>
<td>46.</td>
<td>Complaints</td>
</tr>
<tr>
<td>47.</td>
<td>Sanctions</td>
</tr>
<tr>
<td>48.</td>
<td>Mitigation</td>
</tr>
<tr>
<td>49.</td>
<td>Refraining from intimidating or retaliatory acts</td>
</tr>
<tr>
<td>50.</td>
<td>Waiver of Rights</td>
</tr>
<tr>
<td>51.</td>
<td>Policies &amp; procedures</td>
</tr>
<tr>
<td>52.</td>
<td>Changes to Policies &amp; procedures</td>
</tr>
<tr>
<td>53.</td>
<td>Documentation</td>
</tr>
<tr>
<td>54.</td>
<td>Group health plans</td>
</tr>
<tr>
<td>55.</td>
<td>Effect of prior authorizations</td>
</tr>
<tr>
<td>56.</td>
<td>Effect of prior contracts or other arrangements with business associates</td>
</tr>
</tbody>
</table>

*Standard: a rule, condition or requirement… with respect to the privacy of individually identifiable health information*
Breach cont.

- **Safe Harbors**
  - Encryption
    - Successful use depends upon strength of algorithm
    - Decryption key must also be secure
    - Federal Information Processing Standards (FIPS) 140-2
  - Destruction (of paper)
    - Standard is: can’t be reconstructed

- **You must notify:**
  - Each affected individual (always)
  - The federal government (always)
  - The media (sometimes)
  - Size matters!
    - 500 or greater affected individuals = “large”

Breach Harm Risk Assessment

- “poses a significant risk of financial, reputational or other harm to individual”

- Members of Congress not happy with harm provision; wrote letter to Secretary of HHS demanding it be removed

- We’ll see… awaiting Final Rule
The Statistics

- **385**: Breaches reported to OCR affecting 500 or more individuals*


- **19 million**: number of individuals affected by large breaches

- **>34,000**: Number of reports of breaches submitted to OCR affecting fewer than 500 individuals

*as of January 23, 2012

The Cost of Breaching PHI

- **Tangible:**
  - Average cost of data loss per individual (U.S.) = $214

- **Intangible:**
  - Cost to defend against class action lawsuits; AG actions
  - Reputational harm
Big Breach: Nemours Healthcare System

- Computer backup tapes lost (October 2011)
  - Records had been locked in cabinet believed to have been removed from a building during remodeling
- Information lost included names, addresses, dates of birth, Social Security numbers, insurance information, medical treatment information and direct deposit bank account information on 1.6 million patients and their guarantors, vendors and employees
- From 5 sites in DE, FL, NJ and PA
- Notifying individuals and offering one year of free credit monitoring and identity theft protection

Bigger Breach: New York City Health and Hospitals Corp.

- Backup tapes belonging to New York City Health and Hospitals Corp. stolen from truck while being transported to off-site storage
- 1.7 million individuals may have been affected
- Stolen data included names, addresses, Social Security numbers, and more, dating back 20 years

“Although the data were not encrypted, it exists in a proprietary program that scrambles the records and would make it difficult for individuals without specialized technical expertise and access to the right software and computer hardware to view the private information.”
**Biggest Breach (so far): TRICARE Breach**

- 4.9 million TRICARE military health plan beneficiaries notified of breach of their PHI
- Backup tapes stolen from business associate’s employee car (Science Applications International Corp.)
- Lost: Social Security numbers, names, addresses, phone numbers, personal health data (clinical notes, lab tests and prescriptions)
- Individuals not offered credit monitoring services at first; later changed their minds

**State of Colorado’s “Big Breaches”**

- Stolen Computer Hard drive; July 2010
  - 105,000 individuals affected
  - PHI included name, state ID, category of aid clients were receiving service under
  - 4 new policies
  - 3 policies revised
  - All hard drives encrypted
  - Encrypted flash drives purchased
  - Training revised

- CD Lost in mail; June 2011
  - 3,600 individuals affected
  - PHI included name, county in which applying for aid, paragraph describing special circumstances
  - 1 new policy (encryption)
  - New encryption software purchased (to replace outdated software)
  - Training revised
New Trend: Getting Around HIPAA’s Lack of “Private Right of Action”

- State Law Remedies
  - Consumer protection laws
  - Financial information privacy laws
  - Medical information privacy laws
  - State security breach notification laws

- “Standard of care” Argument
  - "negligence per se claim" - you had the duty to protect this info under HIPAA, and you didn’t so you are liable

- Even if cases are eventually thrown out, can be costly to defend

Sutter Health Breach & Resultant Law Suit(s)

Unencrypted desktop computer stolen from administrative office (October 2011)
- 2 lawsuits
  - One seeks > $4.2 billion in damages
  - One seeks $944 million (for most extensive information lost)

- Alleged organization violated state law by failing to adequately safeguard its computers and data; failing to notify affected individuals in timely manner as required by state law

Note: Sutter was in the process of encrypting its computers when the theft occurred
Cyber Crime & Hacking

- Lockheed Martin (May 2011)
- Sony (since April 2011); various attacks
- NASA's Goddard Space Flight Center
- InfraGard, an FBI affiliate
- The European Commission
- Blogging platform WordPress
- The Institute of Electrical and Electronics Engineers (IEEE)
- TripAdvisor
- Gawker Media
- Speed trap warning service Trapster
- Pentagon's official credit union

“...a lax attitude, coupled with cybercriminals who are technologically savvy enough to perform sophisticated network intrusions, has made 2011 a year dozens of major companies will remember — and hopefully never repeat.”

WHERE ARE WE TODAY?
**HIPAA Compliance Audit Program**

- 8 health plans (40%)
- 2 claims clearinghouses (10%)
- 10 provider organizations (50%)
  - 3 hospitals
  - 3 physicians' offices
  - 1 laboratory
  - 1 dental office
  - 1 nursing/custodial facility
  - 1 pharmacy

**What will the Audits look like?**

- Initial request for information
  - i.e. HIPAA privacy and security compliance policies, plan for complying with the HIPAA breach notification rule, security risk assessment
- Site visit
  - Interviews of key personnel; will observe processes and operations
- Draft report shared with entity describing findings and actions CE is taking
- CE will be able to share actions it has taken to resolve identified compliance issues before final report issued
Regulations Out Already:

- HITECH Act (as part of ARRA) - February 2009
- Breach Notification for Unsecured PHI; Interim Final Rule - August 2009
- HIPAA Administrative Simplification: Enforcement; Interim Final Rule - November 2011
- Modifications to the HIPAA Privacy, Security and Enforcement Rules under HITECH: Notice of Proposed Rulemaking (NPRM) - July 2010

Regulations, cont.

- HIPAA Privacy Rule Accounting of Disclosures Under HITECH: Notice of Proposed Rulemaking (NPRM) - May 2011
- Guidance: Specifying the Technologies and Methodologies That Render PHI Unusable, Unreadable, or Indecipherable … for Purposes of the Breach Notification Requirements - April 2009
What is Still “Due”:

- Modifications to the HIPAA privacy, security and enforcement rules (Omnibus Rule)
- The breach notification Final Rule
- Privacy provisions under the Genetic Information Nondiscrimination Act (GINA)
- Accounting for Disclosures Rule
- Additional Rules in coordination with the Office of the National Coordinator (ONC) for Health Information Technology
- “New ways to protect against new vulnerabilities”
  - Susan McAndrew, deputy director for health information privacy at OCR

Still Due: De-identified Data Safe Harbor Analysis

- Report due last February
- Recommendations on best practices for de-identifying data for research studies to protect patient privacy
- Team includes University of Chicago & HHS’ Office of National Coordinator for Health Information Technology (ONC)
- HIPAA safe harbor: 18 common identifiers must be stripped out of data for it to qualify as de-identified so it can be shared for research purposes
- IS THIS GOOD ENOUGH?
Still Due: Minimum Necessary Guidance

- HITECH: default minimum necessary standard = limited data set (LDS)
  - virtually useless outside research setting
- Can use HIPAA’s minimum necessary if LDS won’t suffice
- Proposed rules ONLY requested public comments
- Once final rules issued, HITECH Act section defining minimum necessary as the LDS will sunset

So, What is a Compliance Officer to Do?

Make sure you’re doing what you can to avoid:

*Willful Neglect*
Do An Inventory of your Protected Data (including PHI)

- Address the entire life cycle of electronic and hard copy PHI in your organization
- Identify where such information is created, how it is maintained and how it is disposed of
- Ensure your policies incorporate all of the above

Assess your Policies & Procedures & Training Program

- Conduct a comprehensive review of policies, procedures, other documentation...
  - Or start with the one that concerns you the most
- Update as necessary
- Make sure all are consistent with actual privacy and security practices in your organization!
Recognize Your Weakest Link

- Insiders are responsible for over 70% of data breaches (usually inadvertent)
  - Aetna breach (May 2010)
    - a file cabinet (containing lots of PHI including SS#s) not cleaned out before it was given to a vendor for removal
    - 6,372 individual affected
  - Blue Cross & Blue Shield of Rhode Island (April 6, 2010)
    - inadvertently donated filing cabinet to a non-profit organization containing LOTS OF PHI (including SS#s)
    - 12,000 individuals affected approximately
  - Insider threats also exist
    - Snooping, selling information, etc.

Assess your Training Program

- Workforce defined under HIPAA:
  - employees, volunteers, trainees, and other persons whose conduct, in the 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.

Train on:
- Privacy basics
- Security awareness
- Your policies and procedures

Make sure to mention:
- Definition of PHI
- Minimum necessary
- Security Awareness
- Sanctions policy
- Employee responsibility to report incidents promptly
- Non-Retaliation Policy
Make it *Effective* Training

- Be there – in person
- Tailor training to audience
  - The more specific the training, the more effective it will be.
  - Use examples and past “incidents” as learning moments
- Play a game!
- Reinforce training with regular reminders – emails, posters, etc.
- Ask how they liked it and how it could be improved
- Update *at least* annually

Move Towards Encryption

- Encrypting everything that holds (at rest) or transfers (in transit) PHI
- If not – do a risk assessment to justify why encryption isn’t being utilized on the device, transfer, etc. (and timeframe for when it will be)

It’s simply too expensive not to utilize this technology!
Do/Update Your Security Risk Assessment

1. Look at your systems containing ePHI
   Risk Analysis 164.308(a)(1)(ii)(a): conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI held by the CE

2. Fix what is broken or not protected enough!
   Risk Management 164.308(a)(1)(ii)(b): implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

3. Document it!
   - Must be in written form (electronic counts)

4. Review it periodically to see if it’s working

NIST HIPAA Security Rule Toolkit

- http://scap.nist.gov/hipaa/ (desktop-based application)
- Goal: help organizations better understand, implement and assess requirements of HIPAA Security Rule,
- Target users: HIPAA covered entities, business associates, other organizations such as those providing HIPAA Security Rule implementation, assessment, and compliance services
- Addresses the 45 implementation specifications identified in the HIPAA Security Rule and covers basic security practices, security failures, risk management, and personnel issues
Recognize Vendor Risks

- What are they doing with your data?
- Can they demonstrate compliance?
- New DoD (proposed rule) requiring contractors’ employees to receive training on:
  - privacy protections
  - handling and safeguarding of personally identifiable information;
  

MN Attorney General sues collection agency

- January 2012; Collection agency was business associate of 2 hospitals
  - agency works with hospitals to “maximize revenues”
- Laptop stolen; 23,500 individuals involved
- Suit claims agency:
  - failed to keep health care records confidential
  - did not tell patients just how much it was involved in their health care”

Chicago Tribune, January 19, 2012;
http://www.chicagotribune.com/news/nationworld/sns-bc-mn--patientdata-lawsuit,0,183332.story
Buy-in from the Top

- Tell them (train them on) what is relevant to their roles in the organization
- Tell them ASAP when major incidents or breaches occur
  - Breach policy should include this

WHAT TO EXPECT IN THE COMING WEEKS/MONTHS
My Predictions…

- The Regulations
- Findings from “test” Audits
  - More guidance as a Result
- More Enforcement Examples
  - OCR won’t wait for actions against covered entities
  - Business associates have a little time

Golden Rule in Compliance

- Ensure you document what you do.
- Ensure you do what you document.
- Ensure you validate you do what you document you do.
- Fix it if you don’t.

Modified from HIMSS; Information Security in Healthcare: Managing Risk, 2010
Thank you.

Erika Bol
Erika.bol@state.co.us
303-866-2958

Resources: Security Risk Assessments

- NIST National Vulnerability Database (NVD); http://nvd.nist.gov/
Resources: Hearings

- Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law Hearing: Your Health and Your Privacy: Protecting Health Information in a Digital World; November 9, 2011
  - http://www.judiciary.senate.gov/hearings/hearing.cfm?id=9b6937d5e931a0b792d258d9b332c04d