HIPAA/HITECH Compliance: Where We are Today & Where You Should Be Headed

HCCA Compliance Institute
May 1, 2012

HIPAA/HITECH Law & Regulations:

- 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
Laws & 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

American Recovery & Reinvestment Act of 2009 (ARRA)

- “Stimulus Package”
- First major changes to HIPAA since 2001
- Privacy changes incorporated into the **HITECH Act**
- **Health Information Technology for Economic & Clinical Health (HITECH) Act**
- Updated HIPAA Administrative Simplification Regulations
What’s All The Fuss?

- HIPAA is an entirely different ‘animal’ under HITECH
- Much stiffer penalties & improved enforcement
- Patients have growing expectation that their privacy will be protected by health care entities
- Organizations are finding out protecting privacy is good business

What May Be Causing you the Most Heartburn?

- Breach Notification Responsibilities
- Improved Enforcement
  - Mandatory Audits
  - Increased Fines
  - More Case Workers from Office of Civil Rights
- New or Revised Documents
  - Notice of Privacy Practices
  - Business Associate Agreements
  - Policies & Procedures
- Operationalizing it all!
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>

Both Frequency & Severity of Enforcement Is Increasing...

Source: Davis Wright Tremaine LLP; 7.12.11
Dates

- Increased fines effective on signing (2/17/09); most other provisions took effect February 18, 2010
- Notice of Proposed Rulemaking (NPRM) to implement HITECH published in Federal Register July 14th, 2010
- CEs and BAs have 180 days after the Rule is finalized to be in compliance with most it
- Business associate agreements’ compliance will have additional 180 days

Business Associate (BA)

- A person or entity that receives PHI from a CE in order to perform a function or activity for the CE
- Before HITECH: Relationship protected contractually with a Business Associate Agreement (BAA)
- After HITECH: BAA still in place but BAs required to comply with parts of Privacy Rule and all of Security Rule
  - Example: BAs must apply minimum necessary to any use, disclose or request of PHI
  - Example: BAs must do a security risk assessment & assign a security contact/officer
- Federal government can audit, penalize and fine business associates directly
Business Associates

- Clarification of who is a BA
  - Patient Safety Organizations (PSOs)
  - Health Information Exchanges (HIEs)
  - Vendors of Personal Health Records
  - E-Prescribing Gateways, etc.

- Clarification of who is not a BA
  - “Conduits” of PHI still exempt
    - i.e. fed express, post office
  - Treatment exception still applies

Business Associate Subcontractor

- Before HITECH: mentioned infrequently in HIPAA
- After HITECH:
  - New definition: “A person who accesses PHI and acts on behalf of a business associate”
  - Arrangement protected through use of BAA

- HHS Stated Goal: “to protect downstream PHI”

- Business Associate responsible for its subcontractors (not the CE!)
Practical Advice – Business Associates

- Understand who is and who is not a business associate
- Be prepared to revise your BAA
  - In some cases – again!
- Consider ways to audit or monitor your BAs more closely
- Remember: a breach by BA is still the CE’s breach

Definition of PHI

- Previously all PHI was protected under HIPAA, no matter how old
- Now only extends 50 years after death
- Allows for historical archiving etc.
- HHS - “Change will benefit family members and historians who may seek access to the medical information of these decedents for personal and public reasons”
Decedents’ Personal Representatives

- Most POAs or Medical POAs expire upon death
- Privacy Rule requires CE to “treat the personal representative as the individual as long as the person has the authority under law to act for the decedent or the estate”
- Can get very confusing

POA = Power of Attorney

Minimum Necessary

- HIPAA - Always key concept
- HITECH – CE must limit PHI to extent practicable to Limited Data Set (LDS) or, if not possible, to minimum necessary
- HHS has requested public comment on what aspects would be most helpful to have federal government address
Practical Advice - Minimum Necessary

- Make MN principle a key part of your HIPAA training
- Have a system in place to identify who needs access to what PHI, and limit access to only that PHI
- Train workforce on MN examples with both paper and electronic PHI
- Make sure you have policies and procedures addressing this!

Fundraising

- Under HITECH:
  - CE must provide individual with “clear and conspicuous opportunity” to not receive further fundraising communications
  - CE may not condition treatment or payment on individual’s choice
  - CE may not send fundraising communications to an individual who has elected not to receive such communications
- Must state this in Notice of Privacy Practices (as under HIPAA)
Practical Advice - Fundraising

- Should already be in your Notice if you do it
- Consider new and/or revisions to P&P
- Figure out how you operationalize this – especially the opt out provision

Marketing Communications

- Marketing requires patient authorization
- Exceptions to marketing:
  - If about a CE’s own products or services (and not an up-sell)
  - related to treatment
  - case management, care coordination, or treatment/therapy/settings recommendations
  - AND does not involve “financial remuneration” for such communications
- Statutory Exception:
  - a description of a drug or biological previously prescribed and payment is ‘reasonable’
Practical Advice – Marketing Communications

- Analyze your business practices that might involve financial remuneration for your organization
- These activities now require specific Authorization that states that remuneration is involved
- Remember that communication to promote health in general is NOT marketing
  - It's important to maintain a healthy diet!
  - Get your annual physical exam!
- Think "population-based" communications to be safe

Prohibition on Sale of PHI

- HIPAA did not specifically prohibit sale of PHI
- HITECH
  - Requires patient authorization
  - Requires special authorization form
  - If you do it, must be included in your Notice
- Limited Exceptions
  - public health activities
  - cost & prep of research activities
  - Treatment & Payment
  - sale, transfer, merger of CE
  - pursuant to business associate activity
  - for individual access to his/her PHI
  - Limited Data Set
  - if Secretary determines it necessary by regulation.
Practical Advice – Sale of PHI

- Include this in the Revision of Your NOTICE OF PRIVACY PRACTICES
- Create an Authorization Form specific to this purpose – must state that remuneration is involved
- Create Policy & Procedure regarding how this will look & how it will be operationalized.

Data Breach Notification

- If you access, lose or disclose patient PHI inappropriately, you must notify the affected patient(s)
- **Notify**
  - **Each individual**
    - includes timeliness and content provisions specified
    - Method of notification is specified
    - burden of proof in demonstrating notification, including any delay
  - **Media**
    - if breach involves > 500 individuals
  - **The federal government**
    - <500 individuals - annually (60 days after end of year)
    - 500 or more individuals - immediately notify DHHS which will post the breach, including name of CE, on their website
Breach Defined

- The unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule which:
  - Compromises the security or privacy of PHI
  - Poses a significant risk of financial, reputational, or other harm to an individual (Risk Assessment)
  - Any form (i.e. verbal)
  - Exceptions for incidental uses or disclosures

Unsecured PHI Defined

“PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through use of technology or methodology specified by Secretary in the guidance”

- Data that is encrypted or destroyed cannot be breached
  - Encryption = according to National Institute for Standards & Technology (NIST) standards
  - Destruction = shredded appropriately; cannot be reconstructed
Harm Risk Assessment

• Key: Significant risk of financial, reputational or other harm
• Documentation of assessment is key
• Per HHS: reputational harm – “as cognizable a form of harm as physical or financial harm”

Notable Reported Breaches

- TRICARE military health plan
  - 4.9 million; backup tapes stolen from business associate’s employee car
- Health Net, Inc.
  - 1.9 million; loss of server drives by business associate
- New York City Health & Hospitals Corporation’s North Bronx Healthcare Network
  - 1.7 million; computer backup tapes stolen from truck that was transporting them to secure storage location
- AvMed, Inc.
  - 1.22 million; theft of laptop computers
- The Nemours Foundation
  - 1.05 million; backup tapes stored in a locked cabinet believed to have been removed during a facility remodeling project
- Blue Cross Blue Shield of Tennessee
  - 1.02 million; theft of hard drives
The “Run” 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!

What to do if a Violation?

- Determine what mitigation steps will reduce harm to the individual

- Determine what went wrong & what to do about it

- If possible, improve safeguards

- Re-train staff (even for slight violations)

- Consider sanctions, if appropriate

- Document EVERYTHING
Patient Rights under HIPAA:

- Access a copy of his/her "record"
- Request restriction of PHI uses and disclosures for TPO
- Request confidential forms of communication (i.e. contact on cell phone only)
- Receive an accounting of the disclosures of a patient’s PHI
  - not including those for treatment, payment and operations
- Request amendments to the medical record
- Complain (to the feds or to the CE)

HITECH Added:

- Ability to restrict disclosures to a health plan if the patient pays for the service out-of-pocket and in-full
- If PHI is in electronic form, patient may request it electronically
- Patient may direct you to send their PHI to another entity (electronic or paper)
- If you have an electronic health record, patient may request an accounting of disclosures for all disclosures including for treatment, payment and operations
  - Could apply to all information held electronically as part of your designated record set (NPRM)
Electronic Health Record

- Definition of EHR:
  - electronic record of health-related information on an individual that is created, gathered, managed and consulted by authorized health care clinicians and staff.

Potential Changes to Notice of Privacy Practices

- Changes to wording on general uses & disclosures
- Statement that remuneration must have authorization
- Statement that most uses/disclosures of psychotherapy notes and for marketing purposes require authorization
- Treatment communications with financial remuneration = opt out provision and stated in Notice
- Fundraising communications = opt out provision and stated in Notice
- New patient Right to restrict information going to health plan
Changes to Business Associate Agreements

- BA Contract (Agreement) must make clear that BA will report breaches of unsecured PHI as required by breach notification rules

- Process for notification

Volunteers

- Train them on HIPAA as part of your “workforce”

- Make sure your security termination procedures include volunteers when they leave!
Security Risk Assessment

- Extremely important aspect of compliance with Security Rule (per feds)
- Must be done at least every 3 years or whenever there is a significant change in the environment
  - Review every year
- Assess threats and vulnerabilities
- Groundwork for P&P and subsequent Security Training

Practical Advice – Security Risk Assessments

- Make sure you have one
- Make sure it is up-to-date
- Make sure any recommendations from it are implemented
- Ensure policies & procedures are modified to reflect changes
- Train on any modifications
- Document!
NIST HIPAA Security Rule Toolkit


- 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

Two Avenues for Possible Investigations/Audits

- Complaints
  - If possible willful neglect violation, feds required to conduct compliance review
  - CE or BA

- Breaches
  - Investigations:
    - > 500 individuals involved – will open an investigation
    - < 500 individuals – may open investigation
  - May conduct compliance review
  - May audit
  - CE or BA
Enforcement by OCR

- Secretary’s discretion to consider:
  - Nature of violation
    - time period
    - number of individuals affected
  - Circumstances
  - Degree of culpability of CE
  - History of prior compliance
    - “prior violations” changed to “indications of non-compliance”
    - CE’s history of compliance is relevant
  - Financial condition of CE
  - “Other matters as justice may require”

Increased Fines – after HITECH

- Willful neglect: “conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated”
  - if preliminary investigation of the facts of the complaint indicates...a possible violation due to willful neglect, the Secretary of HHS is required to investigate

- Lack of Knowledge no longer a defense

- Timely correction important
  - If violation corrected within 30 days, and not willful neglect, can reduce penalties
Heightened Enforcement by AGs

- State attorney general enforcement authority to file suit on behalf of their residents
  - [Link](http://www.ct.gov/ag/cwp/view.asp?Q=453916&A=3869)
  - Connecticut examples
  - Not too much activity recently

- Courts can award damages, costs, and attorney’s fees related to HIPAA violations

- January 2012: Minnesota AG Files First HIPAA Enforcement Action Against Business Associate

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
Example: 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 a timely manner as required by state law

Note: Sutter was in the process of encrypting its computers when the theft occurred

CRIMINAL PENALTIES

- For knowingly obtaining or disclosing identifiable health information relating to an individual in violation of the Rule:
  - Up to $50,000 & 1 year imprisonment
  - If done under false pretenses - up to $100,000 & 5 years
  - If intent to sell, transfer, or use for commercial advantage, personal gain or malicious harm - Up to $250,000 & 10 years

- Enforced by Department of Justice (DOJ)

- Applicable to individuals

- Jail time
  - For “snooping” for individual with no real malicious intent (Huping Zhou)
  - For individual who hacked into previous employers' records and stole client information to market new employer’s practice (Eric McNeal)
On a Positive Note…

“The best thing about the future is that it only comes one day at a time.”

Abraham Lincoln

Time to get moving…!
Questions?

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