Agenda

- Background
- Notice of Privacy Practices
- Increased Patient Rights
- New Limits on Uses and Disclosures of PHI
- Business Associates and Subcontractors
- Breach Notification Rule
- Increased Enforcement
- Questions
Timeline

1996 Health Insurance Portability and Accountability Act (HIPAA)

2003 Privacy Rule

2005 Security Rule

2006 Enforcement Rule

February 2009 American Recovery and Reinvestment Act (ARRA), including Title XIII Health Information Technology for Economic and Clinical Health (HITECH) Act

September 2009 Interim Final Breach Notification Rule

October 2009 Interim Final Enforcement Rule

July 2010 Proposed Omnibus Rule

September 23, 2013 Compliance Date

January 25, 2013 Final Omnibus Rule Published
NOTICE OF PRIVACY PRACTICES
Notice of Privacy Practices

- Describes how medical information is **used** within the Covered Entity (CE)
- Describes how medical information is **disclosed** to others outside the CE
- Describes how patient’s can get **access** to their health information
- Describes the **rights** patient’s have regarding their health information
- CE **legal duties** with respect to Protected Health Information (PHI)
- Notifies the patient of a **breach** of their unsecured PHI
- Which healthcare **providers** does the notice cover
- Where **concerns, complaints or questions** may be sent
- Effective **date**
Notice of Privacy Practices
Change in Content Requirements

- Authorization
  - Description of the types of uses and disclosures that require an authorization
  - HHS clarifies that to mean a statement that most uses and disclosures of psychotherapy notes (where appropriate), for marketing, and sale of PHI need authorization
  - Statement that other uses and disclosures (other than as provided in the NPP) will be made only with authorization
  - Statement that individual may revoke authorization

- Make sure NPP accurately describes actual privacy practices (e.g., reflects Omnibus Rule changes, day-to-day operations)
Notice of Privacy Practices
Change in Content Requirements

- Prohibition on sale of PHI
- Duty to notify affected individuals of a breach of unsecured PHI
- Right to opt out of fundraising (if applicable)
- Right to restrict disclosures of PHI when paid out of pocket
- Limit on use of genetic information (certain health plans only for underwriting)
- Deletion of appointment reminders or information about treatment alternatives
Notice of Privacy Practices

Distribution Requirements - Providers

- Requirements have not changed
  - No later than the **date of the first service delivery**, including service delivered electronically
  - OR
  - Emergency treatment situation, as soon as **reasonably practicable** after the emergency treatment situation
  - **Post** the notice is a clear and prominent location
  - When **revised**, make available upon request on or after effective date
  - If CE has **web site**, must post and make notice available
  - Organized Health Care Arrangement (OHCA) – Joint Notice
Notice of Privacy Practices
Distribution Requirements – Health Plan

- Reprieve for health plans on distributing NPP
  - Post on consumer-facing web site by date of material change
  - Include revised NPP (or information about NPP) in next annual mailing
  - If no web site must provide NPP (or information about NPP) to covered individuals within 60 days of material change
INCREASED PATIENT RIGHTS
Patient Rights

- Right to request information about you
- Right to request to amend or supplement information that you believe incorrect
- Right to get a list of certain disclosures of Information about you
- Right to request restrictions for TPO
- Right to request confidential communications
- Right to a copy of the provider’s or health plan’s Notice of Privacy Practices
Electronic Copy of PHI

**Old Rule**
- Form or format requested, if readily producible
- If not readily producible, then readable hard copy

**New Rule**
- If maintained electronically, produced electronically, unless patient requests hard copy
Electronic Copy of PHI

- Individual may designate third party to receive copy
  - Must be in writing
  - Clearly identify the designated person
  - Clearly identify where to send the copy
Restriction for Out-of-Pocket Payments

- Covered entity must agree to individual’s request to restrict disclosure to health plan
  - For payment or health care operations
  - Unless required by law
  - Individual or person on individual’s behalf pays for item or service out of pocket in full
NEW LIMITS ON USES AND DISCLOSURES OF PHI
Uses and Disclosures of PHI

- General rules for CE/BA permitted uses or disclosures according to HIPAA Rules
  - To the individual
  - For treatment, payment, health care operations (TPO)
  - To HHS Secretary to investigate/determine compliance

- Prohibited uses
  - Several for health plan
  - Sale of PHI
The Good News: Fundraising

- Adds categories of PHI that may be used or disclosed for fundraising:
  - Department of service
  - Treating physician
  - Outcome information
  - Health insurance status
The Good News: Research

- Covered entities may combine “conditioned” and “unconditioned” authorizations
  - For example, conditioned authorization for clinical trial may be combined with unconditioned authorization for tissue specimen repository
The Good News: Research

- Authorization must differentiate between conditioned and unconditioned portions
- Unconditioned authorization must be opt in, e.g.,
  - Check box
  - Second signature line
The Good News: Research

- HHS changed interpretation on authorization for future research:
  - Prior interpretation – Authorization for research must be study specific
  - New interpretation – Authorization may govern future research
  - Authorization must reasonably put individual on notice of potential future research
The Good News: Student Immunization Records

- Covered entity may release student immunization records to school without authorization
  - If state law requires school to have immunization record
  - Written or oral agreement (must be documented)
The Good News:
Decedent Information

- No longer PHI 50 years after death
- Covered entity may disclose PHI to persons involved in decedent’s care or payment if not contrary to prior expressed preference
The Bad News: Marketing

• Question 1: Communication about a product or service that encourages purchase or use? If yes, marketing.

• Question 2: Describes health-related item or service offered by covered entity or treatment alternative? If yes, no longer marketing.

• (New) Question 3: Financial remuneration received from third party whose item or service is described? If yes, marketing again (authorization required).
The Bad News: Sale of PHI

- Covered entity may not receive remuneration in exchange for PHI

Exceptions (no limit):
- Treatment
- Payment
- Sale of covered entity and related due diligence
- Public Health
- Required by law
The Bad News: Sale of PHI

- Exceptions (no limit)
  - Business associate activities

- Exceptions (limits)
  - Any other permissible purpose if remuneration limited to reasonable, cost-based fee for preparation and transmittal (not in HITECH Act)
  - Research
  - To an individual for access and accounting
The Bad News: Genetic Information

- Clarification that genetic information is health information
- Health plan (other than long-term care plan) may not use or disclose genetic information for underwriting purposes
BUSINESS ASSOCIATES AND SUBCONTRACTORS
Who Is a Business Associate?

- Old definition – Function, activity or service which required individually identifiable health information
- New definition
  - Creates, receives, maintains, or transmits protected health information
Who Is a Business Associate?

- Business associates include
  - Health Information Organization
  - e-Prescribing Gateway
  - Other provider of data transmission services
  - Offerer of PHR on behalf of covered entities
  - Subcontractor
Welcome to the HIPAA Party, Subcontractors!

- Contractor + PHI = Business Associate
- Subcontractor = person to whom a business associate delegates a function, activity, or service and receives PHI
- All the way down the chain
- Subcontractor ≠ workforce member
Liability of Business Associates

- Impermissible uses and disclosures
- Breach notification to covered entity
- Failure to provide e-copy of ePHI as specified in the business associate contract
- Failure to disclose PHI to HHS for HIPAA investigation
- Failure to provide an accounting of disclosures
- Failure to comply with the applicable requirements of the Security Rule
Business Associate Contracts

- Must specify compliance with Breach Notification Rule
- Should specify to whom BA provides electronic access
- If CE delegates HIPAA responsibility, must specify that BA will comply with HIPAA
- Grandfathering may be available
Who Contracts with Whom?

- Covered entities **must have** business associate contracts with their direct business associates
- Business associates **must have** business associate contracts with their subcontractors
- Covered entities **do not need** business associate contracts with subcontractors
BREACH NOTIFICATION RULE
Breach Notification

- HITECH: First federal breach notification law
- Basic requirements stay the same
  - Upon the “discovery” of a
  - “Breach” of
  - “Unsecured” PHI
- Covered entities and business associates must make required notifications
Notice Requirements

• Covered Entities must provide notice to:
  1. Individuals whose PHI was compromised
  2. Office for Civil Rights (OCR)
  3. Prominent media outlet(s) if breach involved more than 500 patients

• Business Associates must provide notice to CEs
Encryption or Destruction

• HHS emphasized that encryption and destruction are the only two methods for rendering PHI
  – unusable,
  – unreadable,
  – or indecipherable
to unauthorized individuals – or “secured” – and thus, exempt from the breach notification requirements. (Safe Harbor Provision)
Breach Notification

- “Breach”
  - Unauthorized acquisition, access, use, disclosure of unsecured PHI
  - In a manner not permitted by the HIPAA Privacy Rule
  - That compromises the security or privacy of the PHI
- So far so good, but . . .
New “Compromise Standard”

- “Significant risk of financial, reputational, or other harm”
- Exception for limited data set without ZIP codes or dates of birth
- An impermissible acquisition, access, use, or disclosure of PHI is
- Presumption of reportable breach, UNLESS the entity demonstrates that there is a low probability that PHI has been compromised after risk assessment
What is “compromised”?

- Comment to interim final rule suggesting compromise standard indicates that it is whether PHI is
  
  “inappropriately viewed, re-identified, re-discovered, or otherwise misused”
Exceptions to Breach Definition

First Exception

a. Unintentional acquisition, access or use of PHI by a workforce member or individual acting under the authority of CE or BA,
b. if such access or use was made in good faith and within the scope of authority
c. and does not result in a further unauthorized use or disclosure;
Exceptions to Breach Definition

Second Exception

a. Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement in which the CE participates,

b. and the PHI received as a result of such disclosure is not further used or disclosed in an impermissible manner; and
Exceptions to Breach Definition

Third Exception

a. A disclosure of PHI
b. where a CE or BA has a good faith belief
c. that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
Risk Assessment - Four Required Elements

1. Nature and extent of PHI involved
2. The unauthorized person who used the PHI or to whom the disclosure was made
3. Whether the PHI actually was acquired or viewed
4. The extent to which the risk to the PHI has been mitigated
Breach Notification: Spirit of the Rule

The intent behind the obligation to notify

- Put pressure on the healthcare industry to better safeguard patient privacy by protecting PHI
  - use encryption
- Increase patient/consumer confidence in privacy protection
- Mitigate harm to the affected individuals when consequential events occur
Action Items to Comply

• Evaluate use of encryption by the entity
  – PHI at rest and transit
• Review and if necessary, revise BAA
• Revise Notice of Privacy Practices
• Implement or revise policies and procedures
• Train and educate workforce members and other agents
Consequences

• If CE or BA does not comply with Breach Notification Rule
  – HIPAA violation
  – Subject to HHS enforcement actions and
  – Civil money penalties
INCREASED ENFORCEMENT
## Increased Civil Penalties and Enforcement

<table>
<thead>
<tr>
<th>Violation Type</th>
<th>Pre-Final Rule</th>
<th>Annual Max/Repeated Violations</th>
<th>New Final Civil Penalties</th>
<th>Annual Max/Repeated Violations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100 - $25,000</td>
<td>$50,000 / $1.5 million</td>
<td>$100 - $50,000</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$100 - $25,000</td>
<td>$25,000 / $1.5 million</td>
<td>$1,000 - $50,000</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>Willful Neglect (Corrected)</td>
<td>$10,000 - $250,000</td>
<td>$250,000 / $1.5 million</td>
<td>$10,000 - $50,000</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>Willful Neglect (Not Corrected)</td>
<td>$50,000 - $1.5 million</td>
<td>$1.5 million / $1.5 million</td>
<td>$50,000 (minimum)</td>
<td>$1.5 million</td>
</tr>
</tbody>
</table>
Focus on Willful Neglect

- Willful neglect: Conscious, intentional failure or reckless indifference
- OCR will investigate all cases of possible willful neglect
- OCR will impose penalty on all violations due to willful neglect
Other Enforcement Changes

- Revised definition of reasonable cause (fills gap between “did not know ...” and willful neglect)
- Greater OCR discretion to proceed directly to penalty without seeking informal resolution
- Vicarious liability for business associate agents
- Factors impacting CMP calculation
Four Drivers of Increased Risk

1. Direct application of HIPAA’s Security Rule to Business Associates (BA’s)
2. New Breach Notification Requirements Under ARRA (HITECH Act)
   – Distinct from the Act’s attempt to encourage adoption of Electronic Health Records (EHR’s) by incentive payments for “meaningful use”
3. New State Enforcement Authority under HIPAA and Trend of State Legislated Private Right of Action
4. Government Audits
Other HITECH HIPAA Impacts

- Extension of Key Security Provisions to BA
  - Direct exposure to HIPAA civil & criminal penalties
- Penalties increased & “willful neglect” standard now included
- HHS Sec, based on recommendation from GAO Comptroller, required to develop mechanism whereby harmed individuals may obtain a percentage of the penalties by 2/17/12
- Tightening definition of “minimum necessary”
  - Secretary to issue guidance
  - Implication for access controls under Security Rule & will impact BA
What’s Still Missing?

- Accounting of disclosures/access reports
- Minimum necessary guidance
- Distribution of penalties/settlements to harmed individuals
Questions