A HIPAA-Critical Moment

Securing Health Information
Complying with the Law

2018 CAPLAW National Training Conference
Albuquerque, New Mexico
June 21, 2018
Presented by: Edward I. Leeds

Critical Moment

Forces coming together
• Information as valuable asset
• Threats to information
• Regulatory enforcement
Critical Moment

Information is a particularly valuable asset

Critical Moment

Threats evolving constantly
Critical Moment

HIPAA enforcement through audits and investigations

Health Insurance Portability and Accountability Act (HIPAA)
HIPAA

Agenda

• HIPAA Fundamentals
• Privacy and Security Rules
• Breaches
• Enforcement

HIPAA Fundamentals
HIPAA Fundamentals

Administrative Simplification Provisions

- Electronic Transaction Standards
- Privacy Rule
- Security Rule

Privacy Rule

A Covered Entity may use or disclose Protected Health Information only as HIPAA expressly Requires or Permits that use or disclosure
HIPAA Fundamentals

Security Rule

- **Covered Entities** must secure **electronic Protected Health Information**
- Preserve confidentiality, accessibility, and integrity
- Protect against anticipated threats
- Protect against impermissible uses and disclosures

HIPAA Fundamentals

Protected Health Information (PHI)

- Any information in any form or medium that:
  - Is created or received by a health care provider, health plan, employer, or health care clearinghouse; AND
  - Relates to the past, present or future physical or mental health or condition of an individual, or the provision or payment for health care for an individual; AND
  - Is individually identifiable
HIPAA Fundamentals

Covered Entity

- Health Plans
- Certain Health Care Providers
- Health Care Clearinghouses

Health Care Clearinghouse

An entity that translates data received from another entity from a standard HIPAA format to a non-standard HIPAA format or vice-versa
HIPAA Fundamentals

Health Care Provider

- Health care provider defined broadly, but not without limitations
- To be Covered Entity, provider must transmit data electronically in a HIPAA-covered transaction

HIPAA Fundamentals

Common Covered Transactions by Health Care Provider

- Health care claim or equivalent encounter information transaction
- Health plan eligibility or coverage inquiry
- Request for authorization to provide health care or make referral
- Inquiry into status of a health care claim
- Claims attachments
HIPAA Fundamentals

Health Plans include

- Group health plans
- Insurers and HMOs
- Government-funded health plans, such as Medicare, Medicaid, and CHIP

HIPAA Fundamentals

Health Plans do not include

- Government-funded programs that provide healthcare directly or through grants for direct care
- Plans or programs other than health plans
- Employer/Plan Sponsor
- Vendors of a health plan or health care provider
HIPAA Fundamentals

Business Associate

- Vendor of covered entity
- Obtains PHI in performing services on behalf of covered entity
- Covered entity must require it to enter into business associate agreement (BAA) imposing specified privacy and security requirements

<table>
<thead>
<tr>
<th>Before HITECH</th>
<th>After HITECH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not subject to HIPAA</td>
<td>Subject to HIPAA</td>
</tr>
<tr>
<td>Not liable for violations</td>
<td>Subject to penalties</td>
</tr>
<tr>
<td>Need BAA</td>
<td>Need BAA</td>
</tr>
<tr>
<td>Assurances from agents and subcontractors</td>
<td>BAAs with agents and subcontractors</td>
</tr>
</tbody>
</table>
HIPAA Fundamentals

Required Uses and Disclosures

• HHS request in assessing HIPAA compliance
• Individual Rights

Individuals have the following rights under HIPAA’s privacy rules

• Right to Request Restrictions on Uses and Disclosures of PHI
• Right to Access PHI in Designated Record Set
• Right to Amend Designated Record Set
• Right to Obtain Accounting of Disclosures
• Right to Receive Notice of Privacy Practices
HIPAA Fundamentals

Permitted Uses and Disclosures

• Treatment, payment, health care operations

• Specified activities, including
  - Compliance with other laws
  - Public health
  - Law enforcement
  - Judicial proceedings
  - Research

• Otherwise, obtain individual’s authorization or de-identify information

HIPAA Fundamentals

Compliance Measures Required

• Evaluation and management
• Safeguards
• Specific allocations of responsibility and designations
• Documentation
• Training
• Internal Sanctions
• Ongoing responsibilities
Privacy And Security Rules

Evaluation & Management

Process particularly important for security

- Security Risk Assessment
- Security Risk Management
- Privacy Review
Safeguards

Three Types of Safeguards

• Physical
• Technical
• Administrative

Administrative Safeguards under Privacy Rule include

• Minimum Necessary Rule
• Sensible De-identification
• Verification Before Disclosure
• Practical Protections
Safeguards

Administrative Safeguards under Security Rule include

- Password Protection
- Contingency Plan
- Monitoring Access to EPHI

Allocations of Responsibility

Three officials

- Privacy Official
- Security Official
- Complaint Office or Official
Designations

Certain designations may apply:

- Organized Health Care Arrangement
- Hybrid Entity

Documentation

Notice of Privacy Practices provides basic description of

- Use and disclosure of PHI
- Rules for handling PHI
- Individual rights
Documentation

Notice of Privacy Practices

- Posted on website
- Distributed to employees
- Will be provided to new hires
- Must remind employees of availability
- Must amend for material changes

Documentation

Business Associate Agreements

- Plan must enter into BAA with each business associate
- BAAs must be kept current if rules change
- New business associates require a BAA
Documentation

Plan Amendment
Allows plan and plan vendors to share PHI with plan sponsor for plan administration without individual authorization
• Sets forth permitted uses and disclosures of PHI – plan administration only
• Sets forth who may have access to PHI

Privacy Rule
Certification of Plan Amendment
• Provides health plan and its vendors assurance that plan has been amended
• Allows them to provide PHI to plan sponsor for plan administration
Documentation

Internal Privacy Policies and Procedures

- Administrative practice guide/safeguards
- Routine and recurring uses and disclosures
- Procedures for unusual requests for PHI
- Procedures for addressing individual rights
- Measures in the event of a breach
- Internal sanctions

Documentation

Internal Security Policies and Procedures

- Must have written policies and procedures to address specified standards/safeguards
- Integrate with other policies and procedures
- Enterprise-wide commitment
Authorization Form that meets HIPAA Standards

- To allow Plan to disclose PHI
- To allow other Covered Entities to disclose to Plan or to [COMPANY]

Must document various decisions and actions

- Changes in policy, etc.
- Complaints and incidents
- Investigations and responses
- Certain disclosures
- Compliance measures
Training

Training is mandatory

- Training sessions and materials
- Policies and procedures
- Security reminders

Sanctions

Sanctions are required for violations
Breaches

Breach rules apply

- To a violation of privacy rules
- Involving unsecured PHI
- That results in more than a low probability that PHI has been compromised
Breaches

Breach Evaluation

- Discovery of violation
- Application of exceptions
- Investigation
- Presumption of breach
- Determination

Breach Response

- Notice
  - Affected Individuals
  - Media, if more than 500 in one state affected
  - HHS, immediate if at least 500 affected; otherwise annual
- Mitigation
- Contact for questions
- Documentation
Breaches

Comply with Enforcement

- Through HHS and State Attorneys General
- No private lawsuits, but individuals may share in penalties
- Requirement to investigate in many cases
- Random audits

Breaches

Penalties

- Civil penalties
- Criminal penalties
Breaches

Civil Monetary Penalties

<table>
<thead>
<tr>
<th>Violation Description</th>
<th>Penalty Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did not know and by exercising reasonable diligence would not have known of violation</td>
<td>$100 to $50,000 per violation</td>
</tr>
<tr>
<td></td>
<td>$1.5 million per type per year</td>
</tr>
<tr>
<td>Violation due to reasonable cause</td>
<td>$1,000 to $50,000 per violation</td>
</tr>
<tr>
<td></td>
<td>$1.5 million per type per year</td>
</tr>
<tr>
<td>Willful neglect but corrected problem</td>
<td>$10,000 to $50,000 per violation</td>
</tr>
<tr>
<td></td>
<td>$1.5 million per type per year</td>
</tr>
<tr>
<td>Willful neglect but did not correct problem</td>
<td>$50,000 per violation</td>
</tr>
<tr>
<td></td>
<td>$1.5 million per type per year</td>
</tr>
</tbody>
</table>

Audits

Topics for audit

- Content and provision of Notice of Privacy Practices
- Right to access PHI
- Timeliness and content of breach notifications
- Security risk analysis/management
A few useful websites

- HIPAA for Professionals (HIPAA Rules, guidance on compliance, OCR’s enforcement activities, FAQs etc.)
  https://www.hhs.gov/hipaa/for-professionals/index.html

- HHS Office of Civil Rights (OCR) HIPAA Audit Program
  https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html

- HIPAA Security Risk Assessment Tool

- Ballard Spahr Health Care Reform Dashboard
  https://www.healthcareformdashboard.com/

- Ballard Spahr CyberAdvisor Blog
  https://www.cyberadviserblog.com/