Clinical Practices - Applying a Common Sense Approach to HIPAA Compliance

Objectives

• Common Sense & HIPAA – Really?
• Is Your Organization Meeting HIPAA Requirements?
• What are the HIPAA Rules?
• Permitted and Authorized Disclosures
• How to Determine Probably of a HIPAA Breach?
• Compliance vs. Business Continuity
• What Have We Learned from HIPAA Enforcement?
• Q&A
RISK MITIGATION

• It is steps taken to control or prevent a hazard from causing harm and to reduce risk to a tolerable or acceptable level.

• HIPAA is about mitigating the risk of a potential breach of patient health information.

Your Philosophy

“Apply a Common Sense Approach to HIPAA Compliance”

The HIPAA Privacy Rule

• The HIPAA Privacy Rule created national standards to protect individuals’ medical records and other protected health information (PHI), especially in light of electronic healthcare transactions.

• Created safeguards that must be used to protect PHI.

• Set limits on the use and release of health records.
Permitted Disclosures of PHI

A healthcare provider is permitted, but not required, to use and disclose protected health information, without an individual’s authorization, for the following purposes or situations:

- To the individual (unless required for access or accounting of disclosures)
- Treatment, payment, and health care operations
- Opportunity to agree or object
- Incident to an otherwise permitted use and disclosure
- Public interest and benefit activities for national priority purposes
- Limited data set for the purposes of research, public health or health care operations
- Public Health Emergencies

Permitted Disclosure

Even when the patient is not present or it is impracticable because of emergency circumstances or the patient’s incapacity;

A healthcare provider can discuss patient care or payment with a family member or other person??

A healthcare provider may share this information with the person when, in exercising professional judgment, it determines that doing so would be in the best interest of the patient.

The HIPAA Privacy Rule permits a healthcare provider to discuss a patient’s health status, treatment, or payment arrangements with the patient’s family, legal guardians, caregiver, and personal representative.
**Authorized Uses and Disclosures of PHI**

- A healthcare provider must obtain the individual’s written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule.
- A healthcare provider may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances.

**Authorization Form**

**Patient Request for Health Information**

<table>
<thead>
<tr>
<th>Action Information (Name Print)</th>
<th>First Name</th>
<th>Middle Initial</th>
<th>Last Name</th>
</tr>
</thead>
</table>

- Date of Birth: MM/DD/YY
- Phone: 
- Email: 
- Address: 
- City: 
- State: 
- Zip: 

- [ ] Primary Name [ ] Phone Records [ ] Medical Records [ ] Billing Records 
- [ ] Treatment/Rehab [ ] Medical Records [ ] Home Health Services [ ] Other Services [ ]

- Please indicate if you consent above by checking the appropriate boxes.

Source: American Health Information Management Association (AHIMA)

**What is the HIPAA Security Rule?**

- Sets the security standards for the protection of electronic protected health information.
- Requires the implementation of administrative, technical and physical safeguards to ensure the secure transmission, being able to maintain and receive any PHI.
To meet regulatory requirements, an organization must have these 3 requisites in place:

- HIPAA Risk Management Plan
- HIPAA Risk Assessment
- HIPAA Security Awareness Training
The Following Areas Must be Covered with Policy and Procedure in the Plan:

- Administrative Safeguards
- Technical Safeguards
- Physical Safeguards
- General Policies And Procedures

What are Administrative Safeguards?
- Policies and procedures that **direct the conduct of your workforce**.
- Actions put in place to protect PHI.
- ADMINISTRATIVE SAFEGUARDS includes:
  - Contingency Plans
  - Use of Business Associate Agreements
  - Workforce Security Measures
  - Information Management Access

What are Technical Safeguards?
- Policies and procedures that **focus on the technology that protects PHI**.
- Procedures to control and audit access.
- TECHNICAL SAFEGUARDS includes:
  - Unique User Identification
  - Integrity of ePHI
  - Transmission Security
  - Encryption
What are Physical Safeguards?

• Policies and procedures that focus on physical access to PHI.
• Protection for unauthorized access to sensitive data and records.
• PHYSICAL SAFEGUARDS include:
   Facility Access Controls
   Workstation Use
   Workstation Security
   Device and Media Controls
   Keeping file cabinets, doors, and desks locked in areas where PHI is maintained or is accessible.

HIPAA Risk Assessment

• Determines Vulnerabilities and Threats to ePHI
  - Gap Analysis
  - Remediation
• Systematic way to track remediation
  Compliance Requirement

HIPAA Security Awareness Training

➢ Annual Requirement for all members of a Covered Entity workforce
➢ Must be Documented
Must Cover: 4 Implementation Specifications:
➢ Periodic Security Reminders
➢ Malicious Software - Detect, Guard, Report
➢ Log-In Monitoring - Attempts & Discrepancies
➢ Password Management & Safeguards
Should Cover: HIPAA Privacy & Security Rules
What is a HIPAA Data Breach?

• A HIPAA data breach is a release of unsecured PHI to an unauthorized entity or in an insecure environment, whether intentional or unintentional.
• An impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach.

Unless the organization, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on an assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

Breach Rule Notification Requirements

<table>
<thead>
<tr>
<th>Breaches affecting 500 or more individuals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breaches affecting fewer than 500 individuals</td>
</tr>
</tbody>
</table>

Breach Rule Notification Requirements
78% of HIPAA Breaches Are Caused by This....

**Human Error**

---

**How Did the Breach Occur?**

- Theft 40%
- Hacking/IT 17%
- Unauthorized Access/ Disclosure 27%
- Loss 8%
- Improper Disposal 3%
- Other 5%
- Unknown 1%

As of 7/31/17
Source: HHS – Office for Civil Rights

---

**Top Five Issues in Investigated Cases Closed with Corrective Action, 2013-2015**

<table>
<thead>
<tr>
<th>Year</th>
<th>Issue 1</th>
<th>Issue 2</th>
<th>Issue 3</th>
<th>Issue 4</th>
<th>Issue 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>Improper Uses &amp; Disclosures</td>
<td>Safeguards</td>
<td>Administrative Safeguards</td>
<td>Access</td>
<td>Technical Safeguards</td>
</tr>
<tr>
<td>2014</td>
<td>Improper Uses &amp; Disclosures</td>
<td>Safeguards</td>
<td>Administrative Safeguards</td>
<td>Access</td>
<td>Technical Safeguards</td>
</tr>
<tr>
<td>2013</td>
<td>Improper Uses &amp; Disclosures</td>
<td>Safeguards</td>
<td>Access</td>
<td>Administrative Safeguards</td>
<td>Minimum Necessary</td>
</tr>
</tbody>
</table>
Compliance vs Business Continuity

Consideration Must Be Given To:

- Confidently of Patient Records
- Claims/Billing Data
- Press – Poor Publicity for the Practice or Organization
  - Reputation Hit
  - Loss of Patients
  - $$$ Loss of Revenue; Cash Flow

Seven Potential Costs of a Healthcare Data Breach

<table>
<thead>
<tr>
<th>Cost</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Post-Breach Costs</td>
<td>$440K</td>
</tr>
<tr>
<td>HIPAA Fines</td>
<td>$1.1 MM</td>
</tr>
<tr>
<td>Brand Value</td>
<td>$500K</td>
</tr>
<tr>
<td>Lost Business</td>
<td>$3.7MM</td>
</tr>
<tr>
<td>Lawsuits</td>
<td>$880K</td>
</tr>
<tr>
<td>Notification</td>
<td>$560K</td>
</tr>
<tr>
<td>Forensics</td>
<td>$610K</td>
</tr>
</tbody>
</table>

Source: Protenus

HHS Breach Portal (Wall of Shame)

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
HIPAA Violations
Enforcement Case Examples

What Have We Learned?

It is not so much the breach, but the OCR investigation

$5.55 million settlement
- Largest to-date settlement against a single entity in 2016
- Breaches affected the ePHI of approximately 4 million individuals

Investigation revealed Advocate failed to:
- Conduct an accurate and thorough risk assessment
- Implement policies and procedures and facility access controls to limit physical access to the electronic information systems
- Obtain satisfactory assurances in the form of a written business associate contract that its business associate would appropriately safeguard all ePHI in its possession
- Reasonably safeguard an unencrypted laptop when left in an unlocked vehicle overnight
$2.75 million settlement
- Breach of unsecured ePHI affecting approximately 10,000 individuals
- Likely stolen by a visitor to the ICU who had inquired about borrowing one of the laptops

Investigation revealed that UMMC failed to:
- Implement policies and procedures to prevent, detect, contain, and correct security violations;
- Implement physical safeguards for all workstations that access ePHI to restrict access to authorized users;
- Assign a unique user name and/or number for identifying and tracking user identity in information systems containing ePHI;
- Notify each individual whose unsecured ePHI was reasonably believed to have been accessed, acquired, used, or disclosed as a result of the breach.

Memorial Hermann Health System (MHHS)
$2.4 million settlement
- Multiple media reports suggesting that MHHS disclosed a patient’s protected health information (PHI) without an authorization.
- Patient at one of MHHS’s clinics presented an allegedly fraudulent identification card to office staff.
- Staff immediately alerted appropriate authorities of the incident, and the patient was arrested. This disclosure of PHI to law enforcement was permitted under the HIPAA Rules.
- MHHS subsequently published a press release concerning the incident in which MHHS senior management approved the impermissible disclosure of the patient’s PHI by adding the patient’s name in the title of the press release.

$2.5 million settlement
- Breach affected 1,391 individuals
- A workforce member’s laptop was stolen from a parked vehicle outside of the employee’s home

Investigation revealed:
- Insufficient risk assessment and risk management processes in place at the time of the theft.
- Policies and procedures implementing the standards of the HIPAA Security Rule were in draft form and had not been implemented.
- Organization was unable to produce any final policies or procedures regarding the implementation of safeguards for ePHI, including those for mobile devices. (Mobile Device Management Policy)
Center For Children's Digestive Health (CCDH)

$31,000 Settlement

- Investigation of Business Associate, File Fax
- File Fax stored records containing protected health information (PHI) for CCDH.
- Neither party could produce a signed Business Associate Agreement (BAA)

Memorial Healthcare System

$5.5 Million Settlement

- Breach affected 115,143 individuals
  - MHS is a nonprofit corporation which operates six hospitals, an urgent care center, a nursing home, and a variety of ancillary health care facilities throughout the South Florida area. MHS is also affiliated with physician offices through an Organized Health Care Arrangement (OHCA).
  - Impermissible access by its employees and impermissibly disclosed to affiliated physician office staff.
  - MHS failed to implement procedures with respect to reviewing, modifying and/or terminating users' right of access.
  - MHS failed to regularly review records of information system activity on applications that maintain electronic protected health information by workforce users and users at affiliated physician practices.

Presence Health

$475,000 settlement

- PHI of 836 individuals affected
- Paper based operating room schedules missing
- Presence Health failed to notify, without unreasonable delay and within 60 days of discovering the breach, each of the individuals affected by the breach, prominent media outlets
- Violations of the Breach Notification Rule
$650,000 Settlement

- Theft of a CHCS mobile device (iPhone) compromised the protected health information (PHI) of 412 patient records.
- CHCS provided information management services to 6 skilled care facilities.
- CHCS had no policies addressing the removal of mobile devices containing PHI from its facility.
- No security incident policy.
- No risk analysis or risk management plan.
- 1st time OCR settled with a Business Associate.

$2.2 million settlement

- Unauthorized filming (NY Med series).
- NYP allowed individuals receiving urgent medical care to be filmed without their authorization by ABC.
- OCR also found that NYP failed to safeguard protected health information.

$750,000 Settlement

- Offices located in Indiana.
- Radiation oncology private physician practice.
- Stolen laptop containing unencrypted ePHI of 55,000 patients.
- Investigation revealed widespread non-compliance with the HIPAA Security Rule.
- No risk assessment.
Summary

• Your commitment to protect confidential and protected health information by understanding the rules.
• Totality of all the safeguards
• Use a Common Sense Approach
• FAILURE TO COMPLY WITH HIPAA REGULATIONS CAN CAUSE:
  — Loss of overall trust, workforce trust and public trust.
  — Embarrassment and poor publicity for organization.
  — Potential for fines and criminal prosecution by State and Federal government.

Questions & Discussion

Contact Information

Jay Hodes

202-669-1140

jhodes@colingtonsecurity.com

http://colingtonsecurity.com