IIA HIPAA and Other Sensitive Measures

April 21, 2021
Agenda

• Background on HIPAA/HITECH
• Overview of HIPAA Privacy, Security, and Breach Rules
• Who is Required to Comply?
• Important Agencies and Enforcement
• PII vs. PHI
• HIPAA Security Rule Requirements
• Final Reminders
HIPAA Background
HIPAA Background (continued)

- HIPAA 1996
- HITECH 2009
- Final Rule 2013
HIPAA - 1996

- Congressional bill also known as the Kennedy-Kessebaum Act
- Signed by Bill Clinton
- Five titles regarding healthcare – Title II is the “Administrative Simplification” that sets Privacy and Security requirements around patient information
- Privacy Rule was effective in 2003
HITECH - 2009

• Passed as part of the American Recovery and Reinvestment Act of 2009 (ARRA or Recovery Act)
• Signed by Barack Obama
• Encourages usage electronic health records (EHR) and meaningful use
• Also spurred population health focus
• Required notification of data breaches to US Department of Heath and Human Services (HHS)
• Extended full Privacy and Security rule compliance to Business Associates
• INTERIM Rule
Final Rule - 2013

- Finalized HITECH interim rule
- Establish better accounting and disclosure requirements
- Expanded patient rights
- Contained clearer rule enforcement
HIPAA Rule Overview
Overview of the HIPAA Rules

• Privacy
  • Patient Rights
  • Authorizations for use/disclosure of Protected Health Information (PHI)
  • Business Associates
  • Notice of Privacy Practices

• Security
  • Administrative
  • Physical
  • Technical

• Breach
  • Timing
  • Content
  • Contact, etc.
Who is Required to Comply?
Compliance

- Covered Entities
  - Healthcare provider
    - Hospitals
    - Physician offices
    - Senior living communities
    - Mental health centers
    - Departments of Public Health
  - Health Plans
    - Health insurance companies
    - Health Maintenance Organizations (HMOs)
    - Self-funded plans
    - Medicare/Medicaid
  - Healthcare Clearinghouses (data normalization)
Compliance (continued)

- Business Associates
  - Performing activities and functions on behalf of the covered entity that require the disclosure and/or use of PHI
  - Third-party administrators (TPAs) and pharmacy benefit management for claims processing
  - CPA firm providing bookkeeping or auditing to covered entity
  - Law firms/attorneys
  - Consultants
  - Transcriptionists
  - Managed data hosting and colocation organizations (e.g. TierPoint)
  - Document storage and destruction

**NOTE #1** – Organizations with *incidental* contact with PHI are **excluded** (e.g. janitorial services)

**NOTE #2** – Private Employers are NOT required to comply with HIPAA unless they are a business associate
Important Agencies and Enforcement
Important Agencies

- HHS – U.S. Department of Health and Human Services
- OCR – HHS’ Office for Civil Rights
  - Charged with enforcement of HIPAA Privacy and Security Rules
- CMS – Center for Medicare and Medicaid Services
HIPAA Enforcement Actions

• “Since the compliance date of the Privacy Rule in April 2003, OCR has received over 254,940 HIPAA complaints and has initiated over 1,067 compliance reviews. We have resolved ninety-eight percent of these cases (250,987).” [as of 1/31/21]

• Case Examples https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/all-cases/index.html

• Resolutions (fines) https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html

• Wall of Shame https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
## HIPAA Enforcement Actions – Wall of Shame

<table>
<thead>
<tr>
<th>Expand</th>
<th>Name of Covered Entity</th>
<th>State</th>
<th>Covered Entity Type</th>
<th>Individuals Affected</th>
<th>Breach Submission Date</th>
<th>Type of Breach</th>
<th>Location of Breached Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>o</td>
<td>Harbor Health Services, Inc.</td>
<td>MA</td>
<td>Healthcare Provider</td>
<td>901</td>
<td>04/09/2021</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>o</td>
<td>University Health</td>
<td>TX</td>
<td>Healthcare Provider</td>
<td>2704</td>
<td>04/08/2021</td>
<td>Unauthorized Access/Disclosure</td>
<td>Network Server</td>
</tr>
<tr>
<td>o</td>
<td>Harrington Physician Services</td>
<td>MA</td>
<td>Healthcare Provider</td>
<td>4393</td>
<td>04/08/2021</td>
<td>Unauthorized Access/Disclosure</td>
<td>Network Server</td>
</tr>
<tr>
<td>o</td>
<td>Aloha Practice Management LLC</td>
<td>CA</td>
<td>Business Associate</td>
<td>3835</td>
<td>04/07/2021</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>o</td>
<td>Maestro Health, LLC</td>
<td>IL</td>
<td>Business Associate</td>
<td>2016</td>
<td>04/06/2021</td>
<td>Hacking/IT Incident</td>
<td>Email</td>
</tr>
<tr>
<td>o</td>
<td>Trinity Health</td>
<td>MI</td>
<td>Business Associate</td>
<td>586869</td>
<td>04/05/2021</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>o</td>
<td>Total Health Care Inc.</td>
<td>MI</td>
<td>Health Plan</td>
<td>221454</td>
<td>04/05/2021</td>
<td>Hacking/IT Incident</td>
<td>Email</td>
</tr>
<tr>
<td>o</td>
<td>Bricker &amp; Eckler LLP</td>
<td>OH</td>
<td>Business Associate</td>
<td>420532</td>
<td>04/02/2021</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>o</td>
<td>Belden Inc.</td>
<td>MO</td>
<td>Health Plan</td>
<td>6348</td>
<td>04/02/2021</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
</tbody>
</table>

Business Associate Present: No
HIPAA Enforcement (continued)

From the compliance date to the present, the compliance issues investigated most are, compiled cumulatively, in order of frequency:

• Impermissible uses and disclosures of protected health information;
• Lack of safeguards of protected health information;
• Lack of patient access to their protected health information;
• Lack of administrative safeguards of electronic protected health information;
• Use or disclosure of more than the minimum necessary protected health information
HIPAA Enforcement (continued)

The most common types of covered entities that have been required to take corrective action to achieve voluntary compliance are, in order of frequency:

- General Hospitals;
- Private Practices and Physicians;
- Outpatient Facilities;
- Pharmacies; and
- Health Plans (group health plans and health insurance issuers).
HIPAA Enforcement – OCR Audits

• OCR Audit Protocol last updated July 2018
• KPMG did first 20 audits
• Second round audits completed
• Third round was expected to start in late 2019 (No update as of January 2021)
• $13,554,900 in fines issued to 19 organizations in 2020
  • $1,040,000 to Lifespan Health for stolen laptop (July)
  • $2,300,000 to CHSPSC LLC for data breach (September)
  • $6,850,000 to Premera Blue Cross for data breach (September)

• $5,445,000 in fines so far in 2021
  • $200,000 to Banner Health for Right of Access violation
  • $5,100,000 to Lifetime Health Companies (d/b/a Excellus Health Plan) for data breach affecting 9.3M people

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html
HIPAA Enforcement – Recurring Violations

- Lack of Business Associate Agreements
- Lack of Risk Analyses
- Failure to Manage Identified Risk (e.g. encryption)
- Lack of Transmission Security
- Lack of Appropriate Auditing
- Patching of Software
- Insufficient Data Backup and Contingency Planning
- Individual Right to Access
PII vs. PHI
PII vs. PHI

- **PII – Personally Identifiable Information**
  - Protected by the Privacy Act
  - Social Security Numbers
  - Dates and places of birth
  - Mother’s maiden name
  - Biometric Records

- **PHI – Protected Health Information**
  - Protected by HIPAA
  - Individually identifiable health information
  - Subset of health information, including demographics
  - Physical health, mental health, or genetic information
  - Provision of healthcare to an individual
  - Payment for such healthcare
PII vs. PHI (continued)

Fun Fact: Each state has different interpretation of PII

Magnum P. I. I.
Missouri PII Definition (MO Rev Stat §407.1500)

(9) “Personal Information”, an individual’s first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or unusable:

   a) Social Security Number;

   b) Driver’s license or other unique ID number created or collected by a government body;

   c) Financial account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account;

   d) Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual’s financial account;

   e) Medical information; or

   f) Health insurance information.

Personal information does not include information that is lawfully obtained from publicly available sources, or from federal, state, or local government records lawfully made available to the general public.
Defining PHI

• Ask: “Can I connect an identity with a condition, payment, or eligibility?

• PHI is any information in a medical record that can be used to identify an individual, and that was created, used, or disclosed to a covered entity and/or their business associate(s) in the course of providing a health care service, such as a diagnosis or treatment.

• Protected Health Information (PHI) is the combination of health information and personally identifiable information (PII).
PHI Identifiers – *Health Information Plus:*

- Patient names
- Addresses
- Dates — Including birth, discharge, admittance, and death dates.
- Telephone and fax numbers
- Email addresses
- Social Security numbers
- Driver’s License information
- Medical record numbers
- Account numbers
- Health plan beneficiary numbers
- Certification/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Names of relatives
- Internet Protocol (IP) address numbers
- Biometric identifiers — including finger and voice prints.
- Full face photographic images and any comparable images.
Examples of PHI

• Billing information from your doctor
• Explanation of benefits
• Appointment reminders
• An MRI scan
• Lab results
• Phone recordings
• Payroll deductions for health plan
• Nutrition/meal plans for in-patients
What is Not PHI?

• Student health records (covered under FERPA – Family Educational Rights and Privacy Act of 1974)
• Workers’ compensation
• Wearables
  • Steps on a pedometer
  • Calories burned
  • Blood sugar, blood pressure, and heart rate readings without an identity
PHI Grey Areas

Might suggest a condition:
• Allergy-free vaccinations
• Envelopes from specialty care
• Home hospice vehicle parked outside of a house
HIPAA Security Rule
Balancing Patient Care with Security

If your priorities are to keep patients alive and healthy, should security get in the way?

• Observe “Minimum Necessary” rule
• Never intended to interfere with treatment of patient

Specific to COVID-19

• Providers can disclose PHI to public health authorities
• Providers can share PHI with family members or anyone else to lessen the serious and imminent threat to public health and safety.

Public health disclosures have always been permitted under HIPAA but have been emphasized during the current pandemic
HIPAA Security Rule – Required vs. Addressable

• Only in the Security Rule does HHS make some requirements “addressable”. This was to accommodate organizations of different sizes and complexity.

• During an assessment addressable requirements are treated as “Required”.

• If organization cannot meet an “Addressable” requirement, they must document why, such as financial, technical, or workforce limitations.
HIPAA Security Rule – Prescriptive Controls?

• The Security Rule doesn’t really contain prescriptive controls

• Example #1: Password length not defined
  • They require you to document password requirements in a policy
  • They require you to implement those passwords according to policy

• Example #2: Periodic technical and non-technical evaluations
  • How frequent?
  • What is technical vs. non-technical?

• 72 Security requirements
Controls Follow CIA triad

• Confidentiality
  • Logical and physical access control, authorization, authentication

• Integrity
  • “Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.”

• Availability
  • “Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.”
# HIPAA Security – Administrative Safeguards

<table>
<thead>
<tr>
<th>Topic</th>
<th>Subtopic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigned Security Responsibility</td>
<td>164.308(a)(2) Security Officer</td>
</tr>
<tr>
<td>Workforce Security</td>
<td>164.308(a)(3) Authorization and/or Supervision Workforce Clearance Procedure Termination Procedures</td>
</tr>
<tr>
<td>Security Incident Procedures</td>
<td>164.308(a)(6) Response and Reporting</td>
</tr>
<tr>
<td>Contingency Plan</td>
<td>164.308(a)(7) Data Backup Plan Disaster Recovery Plan Emergency Mode Operation Plan Testing and Revision Procedure Applications and Data Criticality</td>
</tr>
<tr>
<td>Evaluation</td>
<td>164.308(a)(8) Periodic Technical and Nontechnical Evaluation</td>
</tr>
<tr>
<td>Business Associate Contracts and Other Arrangements</td>
<td>164.308(b)(1) Written Contract or Other Arrangement</td>
</tr>
</tbody>
</table>
## HIPAA Security – Physical Safeguards

<table>
<thead>
<tr>
<th>Category</th>
<th>Rule Section</th>
<th>Description</th>
</tr>
</thead>
</table>
| Facility Access Controls        | 164.310(a)   | Contingency Facility Security Plan  
|                                 |              | Access Control and Validation Procedures  
|                                 |              | Maintenance Records                                                          |
| Workstation Use                 | 164.310(b)   | Policies and Procedures                                                     |
| Workstation Security            | 164.310(c)   | Physical Safeguards                                                          |
| Device and Media Controls       | 164.310(d)(1)| Disposal Media Re-use                                                        |
|                                 |              | 164.310(d)(2) | Accountability  
|                                 |              | Data Backup and Storage                                                      |
## HIPAA Security – Technical Safeguards

<table>
<thead>
<tr>
<th>Category</th>
<th>Regulation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Control</strong></td>
<td>164.312(a)</td>
<td>Unique User Identification, Emergency Access Procedure, Automatic Logoff, Encryption and Decryption</td>
</tr>
<tr>
<td><strong>Audit Controls</strong></td>
<td>164.312(b)</td>
<td>Hardware, Software, and/or Procedural Mechanisms</td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td>164.312(c)</td>
<td>Mechanism to Authenticate Electronic Protected Health Information</td>
</tr>
<tr>
<td><strong>Person or Entity Authentication</strong></td>
<td>164.312(d)</td>
<td>Verification Procedures</td>
</tr>
<tr>
<td><strong>Transmission Security</strong></td>
<td>164.312(e)</td>
<td>Integrity Controls Encryption</td>
</tr>
</tbody>
</table>
Emerging Concerns

• SMS
  • Not compliant for transmitting PHI
  • Secure messaging (e.g. end-to-end encrypted messages) would meet compliance

• Telehealth
  • Providers need to use HIPAA compliant solutions or provide BAA
    • Good: Epic MyChart, Zoom, Google Hangouts, GoToMeeting
    • Bad: FaceTime, TikTok, Facebook Live, Twitch, WhatsApp
  • OCR is relaxing enforcement for telehealth amidst COVID-19

• Big data
  • Data encryption, de-identifying PHI, limiting access, use/disclosure/sale of information
Auditing HIPAA Compliance
Who should we audit?

• Covered Entities
• Business Associates
• Clearinghouses

What should we audit?

• People who touch PHI
• Systems handling PHI
• Place's housing PHI
Format

• Standards comparison
• No “Certification”
Questions?