Preparing for a HIPAA Audit

Anton Ames
IT Management Consultant
Anton Ames Group
Omaha, Nebraska

Marcelle J. Henry
Partner
Cohen, Weiss and Simon LLP
New York, New York

The opinions expressed in this presentation are those of the speaker. The International Foundation disclaims responsibility for views expressed and statements made by the program speakers.
What Is HIPAA?

• Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (HIPAA Rules)
• HIPAA amended by the Health Information Technology for Economic and Clinical Health Act (HITECH) in 2009
• In 2013, Health and Human Services (HHS) issued Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under HITECH (Omnibus Final Rule)
Who’s Subject to HI PAA

• HI PAA Covered Entities (CEs)
  – Health plans, healthcare providers and health care clearinghouses

• Business Associates (BAs)
  – CE vendors who have access to protected health information (PHI)

KEEP CALM and FOLLOW THE RULES
## Covered Entities

- **A CE is one of the following:**

<table>
<thead>
<tr>
<th><strong>A Health Care Provider</strong></th>
<th><strong>A Health Plan</strong></th>
<th><strong>A Health Care Clearinghouse</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Includes:</td>
<td>Includes:</td>
<td>This includes entities that process</td>
</tr>
<tr>
<td>- Doctors</td>
<td>- Health insurance companies</td>
<td>nonstandard health information they</td>
</tr>
<tr>
<td>- Hospitals and clinics</td>
<td>- HMOs</td>
<td>receive from another entity into a standard</td>
</tr>
<tr>
<td>- Psychologists</td>
<td>- Company health plans</td>
<td>(i.e., standard electronic format or</td>
</tr>
<tr>
<td>- Dentists</td>
<td>- Multiemployer welfare plans</td>
<td>data content), or vice versa</td>
</tr>
<tr>
<td>- Chiropractors</td>
<td>- Government programs such as Medicare, Medicaid, and the military and veterans health care programs</td>
<td></td>
</tr>
<tr>
<td>- Nursing homes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Pharmacies</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

... but only if transmit any information in electronic form in connection with a transaction for which HHS has adopted a standard.
Business Associates

• BAs are those who assist CEs in performing activities involving the use and disclosure of PHI

• Services include:
  – Claims processing, billing, repricing, benefit management, data analysis, utilization review
  – Legal, actuarial, accounting, consulting, data aggregation, management, administration, accreditation, financial services
Business Associate Agreements

- BAs are generally not CEs under the law, but they are subject to HIPAA requirements by contract and by law.
- A BA must agree by contract to safeguard a CE’s PHI and otherwise comply with a CE’s privacy practices, including minimum necessary requirements.
- Business Associate Agreements (BAAs) are required to include certain provisions by law and may include additional language such as:
  - CE audit rights
  - Representations regarding a BA’s compliance with the HIPAA Rules
  - BA’s breach notification obligations
  - Indemnification language
HIPAA Privacy Rule

- A CE is permitted to use and disclose PHI without an authorization from the individual for:
  - Treatment
  - Payment
  - Health care operations
  - Other purposes as permitted by law
- Other uses and disclosures require an authorization
HIPAA Security Rule

A CE must ensure the confidentiality, integrity, and availability of all electronic PHI (ePHI) it creates, receives, maintains, or transmits

- Protect against reasonably anticipated threats/hazards to and impermissible uses and disclosures of PHI
- Maintain security and integrity of PHI
Protected Health Information

• What is PHI?
  – Health and demographic information about an individual
  – Created or received by a CE, that relates to the past, present, or future:
    • Physical or mental health condition of an individual,
    • Provision of health care to an individual, or
    • The payment for the provision of health care to an individual
• Examples of PHI
  – Enrollment information in the hands of a plan
  – Claims and appeals information
• Information can be PHI even if it is not clinical or medical information
• Unless information is created or received by a CE, it is not PHI, even if it includes medical information
Locations of PHI (ePHI)

- Paper/film records
- Desktop computer
- Laptops
- Electronic portable devices
- Electronic medical records
- Network servers
- E-mail
- Other
Areas of Vulnerability

- Risk analysis and risk management
- Security evaluation
- Security and control of portable electronic devices
- Proper disposal
- Physical access controls
- Training
Consider Vulnerabilities
Common Causes of Breaches

- Hacking/IT incident
- Theft
- Improper disposal
- Unauthorized access or disclosure
- Loss
- Unknown
- Other
Technical Safeguards

• Access controls
• Intrusion detection systems
• Virtual private networks
• Email encryption tools
• Data loss prevention tools
  – Data in use
  – Data in motion
  – Data at rest
# HIPAA Privacy/Security Officer

<table>
<thead>
<tr>
<th>Privacy Officer</th>
<th>Security Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oversees development and implementation of HIPAA Privacy policies and procedures</td>
<td>Oversees development and implementation of HIPAA Security policies and procedures</td>
</tr>
<tr>
<td>Arranges for privacy staff training</td>
<td>Implements security awareness and security staff training</td>
</tr>
<tr>
<td>Implements BAAs</td>
<td>Confirms that BAAs contain appropriate safeguards</td>
</tr>
<tr>
<td>Investigates complaints</td>
<td>Conducts risk assessment and investigates possible breaches</td>
</tr>
<tr>
<td>Processes participants’ requests to exercise their rights</td>
<td>Reviews security incidents</td>
</tr>
<tr>
<td>Oversees development and distribution of HIPAA Privacy Notice</td>
<td>Coordinates risk management</td>
</tr>
<tr>
<td>Applies sanction policy</td>
<td>Applies sanction policy</td>
</tr>
</tbody>
</table>
Policies and Procedures

- A CE must adopt policies and procedures (P&P) concerning compliance with the HIPAA Rules
  - Maintain P&Ps that are relevant and up-to-date
HIPAA Training

- HIPAA requires all members of the CE’s workforce to receive appropriate training for their position with the CE
- Privacy officer must document training

Staff Training
Security Risk Assessment

• Risk Analysis
  – Security Risk Assessment (SRA)
  – SRA is an ongoing process and must be performed periodically in response to environmental or operational changes affecting the security of ePHI
    • How often is periodically?

• SRA tool available at https://www.healthit.gov/providers-professionals/security-risk-assessment-tool
On-Going HI PAA Compliance

- Update policies and procedures
- Conduct on-going staff training
- Perform periodic security risk assessments
- Establish process to detect and report breaches
- Document corrective actions
- Monitor BAs
HI PAA and HI TECH

- HI PAA established national standards for the privacy and security of PHI
- HI TECH established breach notification requirements to facilitate transparency for individuals whose information may be at risk
HI TECH

• If unsecured PHI is impermissibly used or disclosed, security officer must perform risk assessment to determine whether there has been a “breach”

• If there is a breach, certain notification requirements (to the affected individuals, HHS and sometimes the media) apply

• “Unsecured PHI” is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals by encryption or destruction
### Most Common Issues/CEs

<table>
<thead>
<tr>
<th>Compliance Issues</th>
<th>CEs Most Often Required to Take Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Impermissible uses and disclosures of PHI</td>
<td>1. Private practices</td>
</tr>
<tr>
<td>2. Lack of safeguards of PHI</td>
<td>2. General hospitals</td>
</tr>
<tr>
<td>3. Lack of patient access to their PHI</td>
<td>3. Outpatient facilities</td>
</tr>
<tr>
<td>4. Use or disclosure of more than the minimum necessary PHI</td>
<td>4. Pharmacies</td>
</tr>
<tr>
<td>5. Lack of administrative safeguards of electronic PHI</td>
<td>5. Health plans (group health plans and health insurance issuers)</td>
</tr>
</tbody>
</table>
OCR Audit Programs

- HITECH requires HHS’s Office for Civil Rights (OCR) to conduct periodic audits of CEs and BAs compliance with the HIPAA Rules
  - Pilot Audit Program
    - Phase 1
    - Audited CEs only
    - Commenced and completed in 2012
  - Audit Program
    - Phase 2
    - Auditing CEs and BAs
    - Commenced in 2016
Phase 2—Audit Program

• OCR has implemented Phase 2 of the audit program which will:
  – audit both CEs and BAs
  – be comprised of 200 to 250 audits in all

• OCR’s audit schedule:
  – Summer 2016 CEs desk audits
  – Fall 2016 BAs desk audits
  – Early 2017 onsite audits of both CEs and BAs
Phase 2—Auditee Selection

- OCR is identifying pools of CEs and BAs
  - Any CE or BA is eligible for audit
  - Each category of CE will be represented
    - Specific selection criteria (e.g., public or private and size of entity)
    - Division within categories (e.g., health plans divided into group health plans and issuers)
  - Auditees will be randomly selected
- BA auditees will be selected from business associate listings provided by CEs
Phase 2—Desk Audits

- On July 11, 2016, 167 CEs received notice via e-mail of their selection to participate in the desk audits
  - E-mails came from OSOCRAudit@hhs.gov
  - Responses due July 22, 2016
- CEs required to submit documentation electronically
Phase 2—OCR Requests

- CEs given 10 business days to provide requested information which includes:
  - HIPAA Policies and Procedures (P&P) and Notice of Privacy Practices (NPP)
    - Entities must provide only the specified documents, not “compendiums” of all P&Ps
  - Business associate Listing with contact information
    - Auditees must identify and provide detailed information regarding all of their BAs
    - A sample business associate listing template is available at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/batemplate/index.html
## Phase 2—Desk Audit Standards

<table>
<thead>
<tr>
<th>Rule</th>
<th>Controls</th>
</tr>
</thead>
</table>
| **Security Rule**         | Security Management Process -- Risk Analysis
|                           | [§164.308(a)(1)(ii)(A)]                                   |
|                           | [§164.308(a)(1)(ii)(B)]                                   |
| **Breach Notification Rule** | Timeliness of Notification
|                           | [§164.404(b)]                                             |
|                           | Content of Notification
|                           | [§164.404(c)(1)]                                          |
| **Privacy Rule**          | Notice of Privacy Practices & Content Requirements
|                           | [§164.520(a)(1) & (b)(1)]                                 |
|                           | Provision of Notice – Electronic Notice
|                           | [§164.520(c)(3)]                                          |
|                           | Right to Access
|                           | [§164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)] |
Phase 2—Audit Protocol

- Audit protocol last updated April 2016 and is available at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html


- 2016 OCR HIPAA Desk Audits—Audited Entity Questions and Answers is available at http://www.hhs.gov/sites/default/files/Phase2AuditOpeningMeetingWebinarQ%26A.pdf
Phase 2—OCR Reports

• Following an OCR HIPAA audit:
  – OCR issues draft audit report
    • Auditee can respond
  – OCR issues final audit report
    • Includes auditee’s response to draft report
  – OCR will determine whether to open separate compliance review if there are numerous compliance issues
OCR Enforcement

HIPAA Privacy & Security Rule Complaint Process

Complaint → Intake & Review → Possible Privacy or Security Rule Violation → Investigation → Accepted by DOJ

Resolution:
- The violation did not occur after April 14, 2003
- Entity is not covered by the Privacy Rule
- Complaint was not filed within 180 days and an extension was not granted
- The incident described in the complaint does not violate the Privacy Rule

OCR finds no violation
OCR obtains voluntary compliance, corrective action, or other agreement
OCR issues formal finding of violation

Flowchart courtesy of http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/index.html
Civil Penalties

- Pre-HITECH penalties maxed at $25,000 per year for identical violations
- Current tiered penalty structure based on intent:

<table>
<thead>
<tr>
<th>Violation category</th>
<th>Amount of penalty per violation</th>
<th>Max penalty for all violations of identical provision per year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100 – $50,000</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000 – $50,000</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>Willful Neglect, Timely Corrected</td>
<td>$10,000 – $50,000</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>Willful Neglect, Not Timely Corrected</td>
<td>$50,000</td>
<td>$1.5 million</td>
</tr>
</tbody>
</table>
## OCR Resolution Agreements/ CMPs

<table>
<thead>
<tr>
<th>Entity</th>
<th>CE or BA</th>
<th>Incident(s)</th>
<th>Resolution or CMP</th>
</tr>
</thead>
<tbody>
<tr>
<td>University of Mississippi Medical Center (7/16)</td>
<td>CE</td>
<td>Missing laptop</td>
<td>$2.75m and adopt corrective action plan</td>
</tr>
<tr>
<td>Oregon Health &amp; Science University (7/16)</td>
<td>CE</td>
<td>Two unencrypted laptops/ stolen unencrypted thumb drive</td>
<td>$2.70m and adopt corrective action plan</td>
</tr>
<tr>
<td>Catholic Health Care Services of the Archdiocese of</td>
<td>BA</td>
<td>Theft of mobile device</td>
<td>$650,000 and adopt corrective action plan</td>
</tr>
<tr>
<td>Philadelphia (6/16)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Raleigh Orthopaedic Clinic, P.A. (4/16)</td>
<td>CE</td>
<td>Failed to execute BAA</td>
<td>$750,000 and adopt robust corrective action plan</td>
</tr>
<tr>
<td>Lincare, Inc. (2/16)</td>
<td>CE</td>
<td>Employee left behind documents with PHI</td>
<td>$239,800 in CMPs</td>
</tr>
</tbody>
</table>
Tips for Cybersecurity

• Establish a security culture
• Protect mobile devices
• Maintain good computer habits
• Use a firewall and security tools
• Install and maintain anti-virus software
• Plan for the unexpected
• Control access to PHI
• Use strong passwords and change them regularly
• Limit network access
• Control physical access
Preparing for a HIPAA Audit

- Routinely review P&Ps to confirm that they are relevant and up-to-date
  - Amend or develop new P&Ps, as necessary
- Review security risk assessment, consider when to perform a new one
- Prepare business associate listing
- Conduct on-going HIPAA staff training
- Document and retain records of steps taken to comply with the HIPAA Rules
- Consider performing a self-audit using OCR’s audit protocol as a guide
- When in doubt about the HIPAA Rules, consult your privacy/security officer
- Monitor spam/junk email for notice of HIPAA audit from OSOCRAudit@hhs.gov

Website Resources
http://blog.ifebp.org/index.php/hipaa-phase-2-audits-include-business-associates
2017 Educational Programs
Health and Welfare

63rd Annual Employee Benefits Conference
October 22-25, 2017
Las Vegas, Nevada
www.ifebp.org/usannual

Certificate Series
February 27-March 4, 2017
Lake Buena Vista (Orlando), Florida
July 24-29, 2017
Denver, Colorado
www.ifebp.org/certificateseries

Health Care Management Conference
May 1-3, 2017
New Orleans, Louisiana
www.ifebp.org/healthcare

Certificate of Achievement in Public Plan Policy (CAPPP®)
Part I and Part II, June 13-16, 2017
San Jose, California
Part II Only, October 21-22, 2017
Las Vegas, Nevada
www.ifebp.org/cappp

Related Reading
Visit one of the on-site Bookstore locations or see www.ifebp.org/bookstore for more books.

Self-Funding Health Benefit Plans
Item #7563
www.ifebp.org/SelfFunding