HIPAA
Common Compliance Issues and Recent Enforcement Activities

OFFICE FOR CIVIL RIGHTS (OCR)
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

BARBARA STAMPUL
DEPUTY REGIONAL MANAGER
SOUTHEAST REGION

SEPTEMBER 25, 2019
What is the Office for Civil Rights (OCR)?

- U.S. Department of Health and Human Services
- As the Department's civil rights, conscience and religious freedom, and health privacy rights law enforcement agency, OCR investigates complaints, enforces rights, and promulgates regulations, develops policy and provides technical assistance and public education to ensure understanding of and compliance with non-discrimination and health information privacy laws.
- Enforces the HIPAA Privacy, Security, and Breach Notification Rules
• **Mission**

The mission of the Office for Civil Rights is to improve the health and well-being of people across the nation; to ensure that people have equal access to and the opportunity to participate in and receive services from HHS programs without facing unlawful discrimination; and to protect the privacy and security of health information in accordance with applicable law.

• **Vision**

Through investigations, voluntary dispute resolution, enforcement, technical assistance, policy development and information services, OCR will protect the civil rights of all individuals who are subject to discrimination in health and human services programs and protect the health information privacy rights of consumers.
Major Laws Enforced By OCR

- Title VI of the Civil Rights Act of 1964
- Section 504 of the Rehabilitation Act of 1973
- Title II of the Americans with Disabilities Act of 1990
- The Age Discrimination Act of 1975
- Section 1557 of the Affordable Care Act
- HIPAA Privacy, Security, and Breach Notification Rules
What do we do?

- Enforcement and Compliance Activities
  - Complaint Investigations
  - Compliance Reviews
  - Voluntary Resolution Agreements
  - Formal Enforcement
  - Audits
  - Outreach and Public Education
  - Policy Development
HIPAA: Who is Covered?

• Limited by law to:
  ○ “Covered Entities” (CEs):
  ○ Health care providers who transmit health information electronically in connection with a transaction for which there is a HIPAA standard
  ○ Health plans
  ○ Health care clearinghouses
  ○ Business Associates
HIPAA Complaints

Complaints Received by Calendar Year

<table>
<thead>
<tr>
<th>Year</th>
<th>Complaints</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>20,000</td>
</tr>
<tr>
<td>2014</td>
<td>17,643</td>
</tr>
<tr>
<td>2013</td>
<td>13,015</td>
</tr>
<tr>
<td>2012</td>
<td>12,825</td>
</tr>
<tr>
<td>2011</td>
<td>10,379</td>
</tr>
<tr>
<td>2010</td>
<td>8,987</td>
</tr>
<tr>
<td>2009</td>
<td>8,752</td>
</tr>
<tr>
<td>2008</td>
<td>7,536</td>
</tr>
<tr>
<td>2007</td>
<td>8,729</td>
</tr>
<tr>
<td>2006</td>
<td>8,221</td>
</tr>
<tr>
<td>2005</td>
<td>7,362</td>
</tr>
<tr>
<td>2004</td>
<td>6,866</td>
</tr>
<tr>
<td>2004 Partial 2013</td>
<td>6,534</td>
</tr>
<tr>
<td>Year</td>
<td>Issue 1</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>2015</td>
<td>Impermissible Uses &amp; Disclosures</td>
</tr>
<tr>
<td>2014</td>
<td>Impermissible Uses &amp; Disclosures</td>
</tr>
<tr>
<td>2013</td>
<td>Impermissible Uses &amp; Disclosures</td>
</tr>
<tr>
<td>2012</td>
<td>Impermissible Uses &amp; Disclosures</td>
</tr>
<tr>
<td>2011</td>
<td>Impermissible Uses &amp; Disclosures</td>
</tr>
<tr>
<td>2010</td>
<td>Impermissible Uses &amp; Disclosures</td>
</tr>
</tbody>
</table>
OCR Updates

- Policy Development
- Breach Notification
- Enforcement
Recent Security Rule Guidance Material

- **Cloud Service Provider**
  - OCR released guidance clarifying that a CSP is a business associate – and therefore required to comply with applicable HIPAA regulations – when the CSP creates, receives, maintains or transmits identifiable health information (referred to in HIPAA as electronic protected health information or ePHI) on behalf of a covered entity or business associate.

- **Ransomware**
  - OCR recently released guidance on ransomware. The new guidance reinforces activities required by HIPAA that can help organizations prevent, detect, contain, and respond to threats.
  - Includes guidance on security incident procedures, prevention techniques, and assessing whether a HIPAA breach has occurred
Ransomware

Prevention:
• Know your threats and vulnerabilities by conducting a thorough risk analysis
  • Mitigate and remediate identified risks
• Update antivirus and malware software—early detection and response is key!
• Train users to identify and report
  • Social engineering, increase in CPU activity, files missing, suspicious network activity, etc.
• Limit technical access—including vendors
• Frequent backups to ensure continuity
• Routinely test contingency plans

Response:
Activate Security Incident Procedures (NIST SP 800-61, Rev.2) to include:
• Identifying and analyzing scope of damage—what is affected, is it still going, etc.
• Containing impact and propagation
• Eradicating the malware and remediating cause of intrusion

Recovery:
• Restore lost data and continue operations
• Consider notifying local FBI or U.S. Secret Service field office
• Review any other required actions (under HIPAA, per contractual relationship, etc.)
Common Breaches & Compliance Issues

- Lack of Business Associate agreements
- Insufficient Risk Analysis and failure to manage identified risks
- Failure to Manage Identified Risk
- Lack of transmission security (i.e. Encryption)
- Lack of appropriate auditing and review of user activity
- Failure to patch/update software (antivirus, malware)
- Insider threat (bad actors)
- Improper disposal (paper and electronic PHI)
- Failure to regularly train workforce
- Failure to restrict access to minimum necessary
- Improper Disposal
- Insufficient Data Backup and Contingency Planning
- Compliance with Individual’s Right to Access medical records
CE/BA must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the entity. See 45 C.F.R. § 164.308(a)(1)(ii)(A).

Organizations frequently underestimate the proliferation of ePHI within their environments. Identify all ePHI created, maintained, received or transmitted. Be sure to consider:

- Applications (EHR, PM, billing systems; documents and spreadsheets; database systems and web servers; fax servers, backup servers; etc.)
- Computers (servers, workstations, laptops, virtual and cloud based systems, etc.)
- Medical Devices (tomography, radiology, DXA, EKG, ultrasounds, spirometry, etc.)
- Messaging Apps (email, texting, ftp, etc.)
- Mobile and Other Devices (tablets, smartphones, copiers, digital cameras, etc.)
- Media (tapes, CDs/DVDs, USB drives, memory cards, etc.)
Risk Analysis Guidance

Corrective Action after a Breach

- Update risk analysis and management plan
- Review and revise policies and procedures
- Re-training workforce
- Sanctions as appropriate
- Implementation of specific technical or other safeguards
- Mitigation
- CAPs may include monitoring
Enforcement

Investigations involve analyzing:
- Underlying cause of the breach
- Actions taken to respond to the breach, including compliance with notification requirements
- Actions taken to prevent future incidents
- Compliance prior to the breach

Enforcement action is warranted in cases where entities are unreceptive to OCR’s technical assistance or systemic noncompliance is evident
BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY
What is a Breach?

• **Definition of a Breach: See § 164.402**
  • A breach means the acquisition, access, use or disclosure of protected health information ... which compromises the security or privacy of the protected health information.

• **OCR Discretion: A breach of PHI is presumed a breach unless a CE or BA demonstrates a low probability of compromise based on a risk assessment.**

• **Low probability of Compromise- 4 factor test**
  • Examples: Burglarized storage unit vs. Landlord-Tenant dispute
Breach Notification Requirements

- Covered entity must notify affected individuals, HHS, and in some cases, the media, of breach
- Business associate must notify covered entity of breach
- Notification to be provided without unreasonable delay (but no later than 60 calendar days) after discovery of breach
  - Annual reporting to HHS of smaller breaches (affecting less than 500 individuals) permitted
- OCR posts breaches affecting 500+ individuals on OCR website
500+ Breaches by Type of Breach

- **Sept 23, 2009 through July 31, 2019**
  - Theft: 32%
  - Unauthorized Access/Disclosure: 28%
  - Hacking/IT: 26%
  - Improper Disposal: 3%
  - Other: 3%
  - Unknown: 1%

- **Jan 1, 2019 through July 31, 2019**
  - Theft: 9%
  - Unauthorized Access/Disclosure: 28%
  - Hacking/IT: 59%
  - Improper Disposal: 1%
  - Loss: 2%
  - Other: 3%
  - Unknown: 1%
500+ Breaches by Location as of Breach

**Sept 23, 2019 through July 31, 2019**
- Email: 17%
- Network Server: 17%
- Portable Electronic Device: 5%
- Paper Records: 21%
- Desktop Computer: 13%
- Other: 10%
- EMR: 6%

**Jan 1, 2019 through July 31, 2019**
- Email: 42%
- Network Server: 24%
- Laptop: 4%
- Portable Electronic Device: 1%
- Paper Records: 11%
- Desktop Computer: 8%
- Other: 6%
- EMR: 4%
Breach Investigations

- OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
  - Public can search and sort posted breaches
- OCR opens investigations into breaches affecting 500+ individuals, and into number of smaller breaches
- Investigations involve looking at:
  - Underlying cause of the breach
  - Actions taken to respond to the breach (including compliance with breach notification requirements) and prevent future incidents
  - Entity’s compliance prior to breach
Breach Statistics

Breaches Affecting 500 or More Individuals
Reports Received Involving the Theft of PHI

Calendar Years 2014 - 2018

<table>
<thead>
<tr>
<th>Year</th>
<th>Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>121</td>
</tr>
<tr>
<td>2015</td>
<td>80</td>
</tr>
<tr>
<td>2016</td>
<td>62</td>
</tr>
<tr>
<td>2017</td>
<td>56</td>
</tr>
<tr>
<td>2018</td>
<td>40</td>
</tr>
</tbody>
</table>
Breach Statistics

**Breaches Affecting 500 or More Individuals**

**Reports Received Involving Hacking/IT Incidents**

**Calendar Years 2014 - 2018**

- **2014**: 39
- **2015**: 56
- **2016**: 113
- **2017**: 150
- **2018**: 149
Breaches Affecting 500 or More Individuals
Reports Received of Breaches of Laptop Computers

Calendar Years 2014 - 2018

- 2014: 44
- 2015: 38
- 2016: 25
- 2017: 21
- 2018: 19
Breach Statistics

Breaches Affecting 500 or more Individuals
Reports Received of Breaches of Network Servers

Calendars Years 2014 - 2018

- 2014: 56
- 2015: 41
- 2016: 84
- 2017: 88
- 2018: 59
Breach Statistics

BREACHES AFFECTING 500 OR MORE INDIVIDUALS
REPORTS RECEIVED OF BREACHES INVOLVING EMAIL ACCOUNTS

CALENDAR YEARS 2014 - 2018

- 2014: 39
- 2015: 37
- 2016: 46
- 2017: 86
- 2018: 105
Breach Statistics

BREACHES INVOLVING 500 OR MORE INDIVIDUALS
REPORTS RECEIVED INVOLVING BREACHES OF ELECTRONIC MEDICAL RECORDS

CALENDAR YEARS 2014 - 2018

<table>
<thead>
<tr>
<th>Year</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>16</td>
</tr>
<tr>
<td>2015</td>
<td>19</td>
</tr>
<tr>
<td>2016</td>
<td>30</td>
</tr>
<tr>
<td>2017</td>
<td>31</td>
</tr>
<tr>
<td>2018</td>
<td>21</td>
</tr>
</tbody>
</table>
Breach Review Observations

• In most cases, entities able to demonstrate satisfactory compliance through voluntary cooperation and corrective action

• In some cases though, nature or scope of indicated noncompliance warrants additional enforcement action

• Resolution Agreements/Corrective Action Plans
  o 62 settlement agreements that include detailed corrective action plans and monetary settlement amounts

• 4 civil money penalties

As of July 31, 2019
## Recent Enforcement Activities

<table>
<thead>
<tr>
<th>Date</th>
<th>Facility</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/2018</td>
<td>Boston Medical Center</td>
<td>$100,000</td>
</tr>
<tr>
<td>9/2018</td>
<td>Brigham and Women's Hospital</td>
<td>$384,000</td>
</tr>
<tr>
<td>9/2018</td>
<td>Massachusetts General Hospital</td>
<td>$515,000</td>
</tr>
<tr>
<td>10/2018</td>
<td>Anthem</td>
<td>$16,000,000</td>
</tr>
<tr>
<td>11/2018</td>
<td>Allergy Associates of Hartford</td>
<td>$125,000</td>
</tr>
<tr>
<td>12/2018</td>
<td>Advanced Care Hospitalists</td>
<td>$500,000</td>
</tr>
<tr>
<td>12/2018</td>
<td>Pagosa Springs Medical Center</td>
<td>$111,400</td>
</tr>
<tr>
<td>12/2018</td>
<td>Cottage Health</td>
<td>$3,000,000</td>
</tr>
<tr>
<td>5/2019</td>
<td>Tennessee Medical Imaging</td>
<td>$3,000,000</td>
</tr>
<tr>
<td>5/2019</td>
<td>Medical Informatics Engineering</td>
<td>$100,000</td>
</tr>
</tbody>
</table>
Recent Enforcement Activities

Other recent cases involve ePHI viewable on the web, failure to manage identified risks, and malware attacks.

Resolution Agreements:
https://www.hhs.gov/hipaa/
Some Good Practices:

- Review all vendor and contractor relationships to ensure BAAs are in place as appropriate and address breach/security incident obligations
- Risk analysis and risk management should be integrated into business processes; conducted regularly and when new technologies and business operations are planned
- Dispose of PHI on media and paper that has been identified for disposal in a timely manner
- Incorporate lessons learned from incidents into the overall security management process
- Provide training specific to organization and job responsibilities and on regular basis; reinforce workforce members’ critical role in protecting privacy and security
UPDATES
In April 2019, OCR issued new FAQs addressing the applicability of HIPAA to the use of software applications (apps) by individuals to receive health information from their providers.

- Provides guidance for covered entities, EHR developers and app developers.
- Reiterates the importance of HIPAA’s right to access for individuals.

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access-right-health-apps-apis/index.html
## Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties (Announced April 26, 2019)

<table>
<thead>
<tr>
<th>Culpability</th>
<th>Low/violation</th>
<th>High/violation</th>
<th>Annual limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Knowledge</td>
<td>$100</td>
<td>$50,000</td>
<td>$25,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000</td>
<td>$50,000</td>
<td>$100,000</td>
</tr>
<tr>
<td>Willful – Corrected</td>
<td>$10,000</td>
<td>$50,000</td>
<td>$250,000</td>
</tr>
<tr>
<td>Willful – Not corrected</td>
<td>$50,000</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

Direct Liability of Business Associates

Business associates are directly liable for HIPAA violations as follows:

- Failure to provide the Secretary with records and compliance reports; cooperate with complaint investigations and compliance reviews; and permit access by the Secretary to information, including protected health information (PHI), pertinent to determining compliance.

- Taking any retaliatory action against any individual or other person for filing a HIPAA complaint, participating in an investigation or other enforcement process, or opposing an act or practice that is unlawful under the HIPAA Rules.

- Failure to comply with the requirements of the Security Rule.

- Failure to provide breach notification to a covered entity or another business associate.

- Impermissible uses and disclosures of PHI.
Direct Liability of Business Associates (Continued)

- Failure to disclose a copy of electronic PHI (ePHI) to either the covered entity, the individual, or the individual’s designee (whichever is specified in the business associate agreement) to satisfy a covered entity’s obligations regarding the form and format, and the time and manner of access under 45 C.F.R. §§ 164.524(c)(2)(ii) and 3(ii), respectively.

- Failure to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

- Failure, in certain circumstances, to provide an accounting of disclosures.

- Failure to enter into business associate agreements with subcontractors that create or receive PHI on their behalf, and failure to comply with the implementation specifications for such agreements.

- Failure to take reasonable steps to address a material breach or violation of the subcontractor’s business associate agreement.

Notably, OCR lacks the authority to enforce the “reasonable, cost-based fee” limitation in 45 C.F.R. § 164.524(c)(4) against business associates because the HITECH Act does not apply the fee limitation provision to business associates. A covered entity that engages the services of a business associate to fulfill an individual’s request for access to their PHI is responsible for ensuring that, where applicable, no more than the reasonable, cost-based fee permitted under HIPAA is charged. If the fee charged is in excess of the fee limitation, OCR can take enforcement action against only the covered entity.

RESOURCES

— HIPAA Regulation

— Supplements to the HIPAA Regulation
  • HIPAA Security Information Series: (educational papers)
    — Administrative, Physical, and Technical Safeguards
    — Basics of Risk Analysis and Risk Management
  • Additional Security Guidance Material:
    — Remote use, mobile device, and ransomware
  • Cybersecurity Newsletters
    — Risk Analyses v. Gap Analyses, workstation security, software vulnerability and patching, guidance on disposing of electronic devices and media, considerations for securing electronic media and devices
    — Sign up for OCR Listserv: http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

— Join us on Twitter @hhsocr

— OCR Hotline: (800) 368-1019 or (800) 537-7697 (TDD).
**Additional Resources**

https://www.hhs.gov/hipaa

**Privacy and Security Toolkit:**
https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/index.html

www.healthit.gov
Questions?