Hot Topics in HIPAA Enforcement

HCCA Regional Conference – Dallas
February 17, 2017

Jamie Sorley, JD, MBA, CIPP/US
Supervisor, Southwest Region

Erica Broussard, RN, JD
Investigator, Southwest Region

Topics

- Overview of OCR
- Enforcement Statistics and Process
- Recent Enforcement Actions
- Recently Issued Guidance
- Filing a Breach Notification Report
Overview of OCR

Overview

Headquarters - Washington, DC
- Policy and regulations
- Guidance materials
- Centralized Case Management Operations and Customer Response Center

Regional Offices - Boston, New York City, Philadelphia, Atlanta, Denver, Dallas, Kansas City, San Francisco, Los Angeles, Chicago, Seattle
- Investigations
- Technical Assistance
- Outreach
Numbers at a Glance

Between April 2003 and December 31, 2016:

- OCR has received 146,345 complaints
  - 24,774 Investigated and resolved through CE or BA taking corrective action
- 11,133 resulted in finding of no violation
- 17,905 cases OCR intervened early and provided technical assistance
- 41 cases resulted in civil money penalties or settlements
  - Total $48,679,700

Breach Highlights

September 2009 through December 31, 2016

- Approximately 1,795 reports involving a breach of PHI affecting 500 or more individuals
  - Individuals affected are approximately 171,166,753
- Approximately 247,824 reports of breaches of PHI affecting fewer than 500 individuals
Breach Highlights

500+ Breaches by Type of Breach as of December 31, 2016

- Theft: 43%
- Unauthorized Access/ Disclosure: 26%
- Loss: 8%
- Hacking/ IT: 14%
- Other: 5%
- Improper Disposal: 3%
- Unknown: 1%

Breach Highlights

500+ Breaches by Location of Breach as of December 31, 2016

- EMR: 5%
- Email: 9%
- Network Server: 15%
- Portable Electronic Device: 10%
- Laptop: 18%
- Desktop Computer: 11%
- Paper Records: 22%
- Other: 10%

DHHS Office for Civil Rights
Audit Program: Phase 2

Purpose: Support Improved Compliance

- Identify best practices; uncover risks & vulnerabilities; detect areas for technical assistance; encourage consistent attention to compliance
- Intended to be non-punitive, but OCR can open up compliance review (for example, if significant concerns are raised during an audit or an entity fails to respond)
- Learn from this next phase in structuring permanent audit program
- Develop tools and guidance for industry self-evaluation and breach prevention

Program Status

- Desk audits underway
  - 166 Covered Entities
  - 48 Business Associates
- Business Associate selection pool largely drawn from over 20,000 entities identified by audited CEs
- On-site audits of both CEs and BAs in 2017, after completion of the desk audit process, to evaluate against a comprehensive selection of controls in protocols
- A desk audit subject may be subject to on-site audit
Compliance Challenges

Lack of Business Associate Agreements

HIPAA generally requires that covered entities and business associates enter into agreements with their business associates to ensure that the business associates will appropriately safeguard protected health information. See 45 C.F.R. § 164.308(b). Examples of Potential Business Associates:

- A collections agency providing debt collection services to a health care provider which involves access to protected health information.
- An independent medical transcriptionist that provides transcription services to a physician.
- A subcontractor providing remote backup services of PHI data for an IT contractor-business associate of a health care provider.
Incomplete or Inaccurate Risk Analysis

- 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 [organization]. See 45 C.F.R. § 164.308(a)(1)(ii)(A).

- Organizations frequently underestimate the proliferation of ePHI within their environments. When conducting a risk analysis, an organization must identify all of the ePHI created, maintained, received or transmitted by the organization.

- Examples: Applications like EHR, billing systems; documents and spreadsheets; database systems and web servers; fax servers, backup servers; etc.; Cloud based servers; Medical Devices Messaging Apps (email, texting, ftp); Media

Failure to Manage Identified Risk

- The Risk Management Standard requires the “[implementation of] security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [the Security Rule].” See 45 C.F.R. § 164.308(a)(1)(ii)(B).

- Investigations conducted by OCR regarding several instances of breaches uncovered that risks attributable to a reported breach had been previously identified as part of a risk analysis, but that the breaching organization failed to act on its risk analysis and implement appropriate security measures.

- In some instances, encryption was included as part of a remediation plan; however, activities to implement encryption were not carried out or were not implemented within a reasonable timeframe as established in a remediation plan.
Lack of Transmission Security

- When electronically transmitting ePHI, a mechanism to encrypt the ePHI must be implemented whenever deemed appropriate. See 45 C.F.R. § 164.312(e)(2)(ii).
- Applications for which encryption should be considered when transmitting ePHI may include:
  - Email
  - Texting
  - Application sessions
  - File transmissions (e.g., ftp)
  - Remote backups
  - Remote access and support sessions (e.g., VPN)

Lack of Appropriate Auditing

- The HIPAA Rules require the “[implementation] of hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.” See 45 C.F.R. § 164.312(b).
- Once audit mechanisms are put into place on appropriate information systems, procedures must be implemented to “regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.” See 45 C.F.R. § 164.308(a)(1)(ii)(D).
- Activities which could warrant additional investigation:
  - Access to PHI during non-business hours or during time off
  - Access to an abnormally high number of records containing PHI
  - Access to PHI of persons for which media interest exists
  - Access to PHI of employees
No Patching of Software

- The use of unpatched or unsupported software on systems which access ePHI could introduce additional risk into an environment.
- Continued use of such systems must be included within an organization's risk analysis and appropriate mitigation strategies implemented to reduce risk to a reasonable and appropriate level.
- In addition to operating systems, EMR/PM systems, and office productivity software, software which should be monitored for patches and vendor end-of-life for support include:
  - Router and firewall firmware
  - Anti-virus and anti-malware software
  - Multimedia and runtime environments (e.g., Adobe Flash, Java, etc.)

Insider Threat

- Organizations must “[i]mplement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information … and to prevent those workforce members who do not have access … from obtaining access to electronic protected health information,” as part of its Workforce Security plan. See 45 C.F.R. § 164.308(a)(3).
- Appropriate workforce screening procedures could be included as part of an organization's Workforce Clearance process (e.g., background and OIG LEIE checks). See 45 C.F.R. § 164.308(a)(3)(ii)(B).
- Termination Procedures should be in place to ensure that access to PHI is revoked as part of an organization's workforce exit or separation process. See 45 C.F.R. § 164.308(a)(3)(ii)(C).
Disposal

• When an organization disposes of electronic media which may contain ePHI, it must implement policies and procedures to ensure that proper and secure disposal processes are used. See 45 C.F.R. § 164.310(d)(2)(i).

• The implemented disposal procedures must ensure that “[e]lectronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800–88: Guidelines for Media Sanitization, such that the PHI cannot be retrieved.”

• Electronic media and devices identified for disposal should be disposed of in a timely manner to avoid accidental improper disposal.

• Organizations must ensure that all electronic devices and media containing PHI are disposed of securely; including non-computer devices such as copier systems and medical devices.

Insufficient Backup and Contingency Planning

• Organizations must ensure that adequate contingency plans (including data backup and disaster recovery plans) are in place and would be effective when implemented in the event of an actual disaster or emergency situation. See 45 C.F.R. § 164.308(a)(7).

• Leveraging the resources of cloud vendors may aid an organization with its contingency planning regarding certain applications or computer systems, but may not encompass all that is required for an effective contingency plan.

• As reasonable and appropriate, organizations must periodically test their contingency plans and revise such plans as necessary when the results of the contingency exercise identify deficiencies. See 164.308(a)(7)(ii)(D).
Recent Enforcement Actions

Enforcement Process

- [https://www.hhs.gov/hipaa/for-professionals/special-topics/enforcement-rule/index.html](https://www.hhs.gov/hipaa/for-professionals/special-topics/enforcement-rule/index.html)

- OCR reviews the information, or evidence, that it gathers in each case. If the evidence indicates that the covered entity was not in compliance, OCR will attempt to resolve the case with the covered entity by obtaining:
  - Voluntary compliance;
  - Corrective action; and/or
  - Resolution agreement.
Enforcement Process

- Letter of Opportunity with Resolution Agreement and Corrective Action Plan
- Notice of Proposed Determination
  - Entity may request a hearing before ALJ
- Notice of Final Determination

Recent Enforcement Actions


**Children's Medical Center of Dallas**
- Multiple lost or stolen mobile devices with unsecured ePHI
- Failure to timely implement appropriate risk management
- $3,200,000 Civil Money Penalty

**MAPFRE Life Insurance Company of Puerto Rico**
- Stolen USB storage device containing the ePHI of 2,209
- Lack of appropriate risk analysis and management, including lack of encryption
- $2,200,000 Settlement with Corrective Action Plan
Recent Enforcement Actions

Presence Health
- Missing paper operating room schedules affecting 836 individuals
- Following discovery of the breach, CE did not timely notify affected individuals, media or OCR
- $475,000 Settlement with Corrective Action Plan
  - Revise policies and procedures
  - Provide additional training to staff

The New York and Presbyterian Hospital
- Patients complained of impermissible disclosure of PHI to ABC film crew
- Did not obtain patient authorization
- $2,200,000 Resolution Agreement/Corrective Action Plan

Recent Enforcement Actions

University of Missouri Medical Center
- Breach report - stolen laptop with unsecured PHI
- Use of generic username and password on network drive
- Identified risks to PHI as early as 2005 but did not significantly manage
- $2,750,000 Resolution Agreement and Corrective Action Plan
  - Conduct risk analysis and develop risk management plan
  - Implement unique user identification
  - Update policies and procedures

University of Massachusetts Amherst (UMass)
- 1,670 individuals affected by malware incident
- Failed to include each business component in hybrid entity designation
- $650,000 Settlement with Corrective Action Plan
  - Conduct comprehensive risk analysis and implement risk management plan
  - Revise policies
  - Provide additional training to staff
Recent Enforcement Actions

**Complete P.T., Pool and Land Physical Therapy**
- Complaint that CE posted patient testimonials with PHI on website without authorization
- $25,000 Resolution Agreement with Corrective Action Plan
  - Revise policies
  - Staff training

**Oregon Health & Science Center**
- Breach reports – 2 stolen laptops and unencrypted thumb drive
- Storage of EPHI on cloud server without a BAA
- $2,700,000 Resolution Agreement with Corrective Action Plan
  - Conduct risk analysis and risk management
  - Encryption program
  - Revise policies and staff training

**Advocate Health Care**
- 3 breach reports
  - Lost/stolen computers with unsecured PHI of approx. 4 million
  - Unauthorized third party access to BA's network
  - $5,550,000 Resolution Agreement with Corrective Action Plan
    - Modify existing risk analysis
    - Develop and implement risk management plan
    - Process for evaluating environmental and operational changes
    - Revise policies and training

**Care New England Health System**
- Breach report – unencrypted back-up tapes missing from 2 facilities
- Outdated Business Associate Agreement
- $400,000 Resolution Agreement with Corrective Action Plan
  - Revise policies and training
Recent Guidance

• Disclosures - Same sex Marriage:

• Understanding Some of HIPAA's Permitted Uses and Disclosures:
  https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/permitted-uses/index.html

• Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals:
Recent Guidance

- Ransomware guidance: http://www.hhs.gov/hipaa/for-professionals/security/guidance/

Recent Guidance

- Access Fees - Individuals’ Right under HIPAA to Access their Health Information 45 CFR § 164.524 - https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html
- Difference between “designation” and "authorization"
  - Authorization – when an individual gives permission for the CE to disclose PHI
  - Designation – when an individual directs the CE to transmit the PHI about the individual directly to another person or entity identified by the individual
  - Why is this important? Access fee limitations apply for designated requests but not authorized requests
Cybersecurity Newsletters

February 2016  Ransomware, “Tech Support” Scam, New BBB Scam Tracker
March 2016  Keeping PHI safe, Malware and Medical Devices
April 2016  New Cyber Threats and Attacks on the Healthcare Sector
May 2016  Is Your Business Associate Prepared for a Security Incident
June 2016  What’s in Your Third-Party Application Software
September 2016  Cyber Threat Information Sharing
October 2016  Mining More than Gold (FTP)
November 2016  What Type of Authentication is Right for you?
December 2016  Understanding DoS and DDoS Attacks
January 2017  Audit Controls


Policy Development – What’s Coming

- Guidance on text messaging
- Social media guidance
- PMI and research authorizations
- ANPRM to solicit views on ways in which an individual who is harmed by an offense punishable under HIPAA may receive a percentage of any CMP or monetary settlement collected
Calculating Access Fees

• Possible methods
  1) Actual allowable costs for each request
  2) Average allowable labor costs
  3) For electronic copies, flat rate of $6.50 (inclusive of all labor, supplies, and postage)

Calculating Access Fees

• Hypothetical 1
  • An attorney requests PHI on behalf of her client.
  • The attorney includes an authorization form signed by her client.
  • The CE charges a $350 fee.
  • The attorney claims the CE should charge a reasonable, cost-based fee.
  • Does the CE have to charge a reasonable, cost-based fee?

• Hypothetical 2
  • An attorney sends a written request to a CE that is signed by her client.
  • The letter clearly identifies that the attorney is designated by her client to receive PHI and that the client is requesting the PHI sent to the attorney’s office.
  • The CE charges a $350 fee.
  • The attorney claims the CE should charge a reasonable, cost-based fee.
  • Does the CE have to charge a reasonable, cost-based fee?
Calculating Access Fees

Answers

Hypothetical 1

• In this case, the attorney is authorized, but is not designated. Thus, CE would not have to charge a reasonable, cost-based fee.

Hypothetical 2

• Yes, here the attorney is designated via a written, signed request that clearly identifies the designated person (the attorney) and the address where the PHI should be sent.

Other Access Considerations

• Requiring a Written Request
  • A covered entity may require individuals to request access in writing, provided the covered entity informs individuals of this requirement. See 45 CFR 164.524(b)(1).

• Verification
  • The Privacy Rule requires a covered entity to take reasonable steps to verify the identity of an individual making a request for access. See 45 CFR 164.514(h).

• Unreasonable Measures
  • While the Privacy Rule allows covered entities to require that individuals request access in writing and requires verification of the identity of the person requesting access, a covered entity may not impose unreasonable measures on an individual requesting access that serve as barriers to or unreasonably delay the individual from obtaining access.
Breach Notification


Questions?

Jamie.sorley@hhs.gov
Erica.broussard@hhs.gov