503 SURVIVING A HIPAA BREACH INVESTIGATION

Presented by
Nicole Hughes Waid, Esq.
Mark J. Swearingen, Esq.
Celeste H. Davis, Esq.
Regional Manager

© FISHERBROYES LLP 2015

Surviving a HIPAA Breach Investigation: Enforcement

Presented by Nicole Hughes Waid
Enforcement Rule History
- HITECH Act Enforcement Interim Final Rule (October 29, 2009)
- HIPAA Enforcement Rule – Final Rule (February 16, 2006)
- Extension of Expiration Date of Interim Final Rule (September 14, 2005)
- HIPAA Enforcement Rule – Proposed Rule (April 18, 2005)
- Extension of Expiration Date of Interim Final Rule (September 15, 2004)
- Correction of Expiration Date of Interim Final Rule (April 28, 2003)

Enforcement Process

OCR is responsible for enforcing the HIPAA Privacy and Security Rules (45 C.F.R. Parts 160 and 164, Subparts A, C, and E). One of the ways that OCR carries out this responsibility is to investigate complaints.

OCR will notify the person who filed the complaint and the covered entity named in it.

If a complaint describes an action that could be a violation of the criminal provision of HIPAA (42 U.S.C. 1320d-6), OCR may refer the complaint to the Department of Justice for investigation.
Enforcement Process

- 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

- If the covered entity does not take action to resolve the matter in a way that is satisfactory, OCR may decide to impose civil money penalties (CMPs) on the covered entity

- If CMPs are imposed, the covered entity may request a hearing in which an HHS administrative law judge decides if the penalties are supported by the evidence in the case
  - Complainants do not receive a portion of CMPs collected from covered entities; the penalties are deposited in the U.S. Treasury

Enforcement Landscape

- The most common types of covered entities that have been required to take corrective action to achieve voluntary compliance are, in order of frequency:
  - Private Practices;
  - General Hospitals;
  - Outpatient Facilities;
  - Pharmacies; and
  - Health Plans (group health plans and health insurance issuers)

Enforcement Landscape

- Top five issues investigated with cases closed with corrective action
  - Impermissible uses and disclosures
  - Safeguards
  - Access
  - Minimum Necessary
  - Mitigation
Resolution Agreements

- Contract signed by HHS and a covered entity in which the covered entity agrees to perform certain obligations (e.g., staff training) and make reports to HHS, generally for a period of three years
- During the period, HHS monitors the covered entity’s compliance with its obligations
- Agreement likely would include the payment of a resolution amount

Civil Money Penalties

- When HHS has not been able to reach a satisfactory resolution through the covered entity’s demonstrated compliance or corrective action through other informal means, civil money penalties (CMPs) may be imposed for noncompliance against a covered entity
- To date, HHS has entered into 25 resolution agreements and issued CMPs to one covered entity

Enforcement Landscape

- August 2015 - $750,000 - Cancer Care Group, P.C. (CCG) agreed to settle potential HIPAA violations
  - In August 2012, the company reported the theft of a laptop bag from an employee’s car; the bag contained unencrypted backup media which contained names, addresses, DOBs, and SSNs of approximately 55,000 patients
  - Investigation revealed that CCG had not conducted an enterprise-wide risk analysis; and did not have a written policy specific to the removal of electronic media from the facility
  - CCG adopted a robust corrective action plan to in its HIPAA compliance program
July 2015 - $218,400 - St. Elizabeth’s Medical Center (“SEMC”) agreed to settle potential HIPAA violations:

- In November 2012, OCR received a complaint alleging employees used an internet-based document sharing application to store ePHI documents of at least 498 individuals without having analyzed the risks associated with the practice.
- Investigation revealed that SEMC failed to timely identify and respond to known security incident.
- Separately, in August 2014, SEMC notified HHS OHR regarding a breach of unsecured ePHI stored on a former employee’s personal laptop and USB drive, affecting 595 individuals.
- Settlement amount took into consideration the circumstances, size of entity, and type of PHI disclosed to determine CMP.

May 7, 2014 – New York-Presbyterian Hospital (NYP) agreed to pay $3.3 million and Columbia University agreed to pay $1.5 million in the largest HIPAA settlement with OIG HHS to date.

- The two hospitals participate in a joint compliance arrangement where they operate a shared network of data and shared firewall.
- The two hospitals learned of the breach after an individual found information about his partner, a former patient at NYP, on the internet.

Both NYP and Columbia reported the breach to Office of Civil Rights (OCR) at the HHS:

- OCR’s investigation found that the breach occurred when a Columbia physician attempted to deactivate a personally-owned computer server on the network containing NYP patients’ electronic protected health information.
- The investigation also found that neither organization made efforts before the breach to ensure that the server was secure.
- In addition, neither hospital conducted an accurate risk analysis that identified all systems that access the patients’ electronic records.
HIPAA Criminal Prosecution 2014

- Georgia women sentenced to 27 years in prison and ordered to make restitution of $493,000 for using identities of nursing home residents to obtain fraudulent income tax refunds
  - The defendant, an employee of Macon Management Health & Rehabilitation Center, netted $460,000 in the scheme
  - Impact on Macon Management is largely dependent upon strength of its compliance program
  - Potential civil fines could reach up to $50,000 per incident

2015 Health Care Hacks

- Excellus Blue Cross Blue Shield – Reported nearly 10.5 million of its customers had been exposed in a sophisticated attack on its information technology systems (September)
- Anthem – the nation’s second-largest health insurance company, reported they were a target of a very sophisticated external cyber attack involving approximately 80 million people (February)
- Premera Blue Cross and Blue Shield of Alaska and affiliate brands Vivacity and Connexion Insurance Solutions – discovered the hack on the same day as Anthem, reported approximately 11 million customers were exposed (March)
- Both Premera and Anthem described the attacks against their systems as “very sophisticated,” and some believe the attacks may be linked to a state-sponsored attack out of China.

HIPAA COMPLIANCE

STEP 1 RISK ASSESSMENT
STEP 2 BUSINESS ASSOCIATE AGREEMENTS
STEP 3 POLICIES AND PROCEDURES
STEP 4 TRAINING
STEP 5 BREACH PLAN
STEP 6 CONTINGENCY PLAN
STEP 7 DOCUMENTATION
STEP 8 PREPARE FOR OCR AUDIT
Breach Investigation – Defense Counsel View

Presented by Mark J. Swearingen

- The investigation begins
  - Starts with an initial information request letter
  - Time is of the essence.
  - Form/gather team to respond to data request and prepare submission
  - This is the opportunity for the entity to tell OCR its story.
  - First impression... lay a strong foundation
  - Be prepared to provide documentation in support of statements made in the submission.
  - OCR likely will request additional information at least once.
  - Can be a long process
Breach Investigation – Defense Counsel View

- Breach Investigations are all about the DC
  - DC: What does it stand for?
    - OCR is headquartered in DC.
    - OCR provides resources and guidance that certainly are helpful to HIPAA compliance.
    - However, if DC headquarters is discussing your breach, you likely are heading toward a Resolution Agreement and Corrective Action Plan.
    - You don’t want this DC!
  - 3 DC’s that you do want:
    - Demonstrate you Care
    - Do Cooperate
    - Don’t get Cute

Breach Investigation – Defense Counsel View

- Demonstrate that you Care about HIPAA compliance.
  - Make good faith efforts at breach response and remediation
  - Conduct a prompt, accurate and thorough investigation
    - Activate breach response team and confirm leader
      - C-Suite, legal, compliance, privacy/security, IT, PR
    - Notify law enforcement, if necessary
    - Remediate harm, to the extent possible
    - Engage outside resources as needed for forensics, IT consulting and/or legal determinations.

Breach Investigation – Defense Counsel View

- Demonstrate that you Care about HIPAA compliance.
  - Show that basic HIPAA requirements are being met, to the extent possible:
    - Policies and procedures
    - Risk analysis/management
    - Workforce training
    - Sanctions
  - Show that HIPAA is part of the culture, not just a binder on a shelf.
Breach Investigation – Defense Counsel View

- Do cooperate in all aspects of the investigation.
  - OCR appreciates honest, open dialogue throughout the process
  - Provide timely and thorough responses to all information requests
    - OCR generally grants reasonable extensions
  - Update periodically, as necessary
  - Produce what OCR requests in a convenient form
    - Confirm with assigned investigator
  - Take advantage of opportunities to communicate with OCR
    - Writing
    - Telephone
    - In person

Breach Investigation – Defense Counsel View

- Don’t get cute in any aspect of the investigation or response.
  - Opportunities to get cute:
    - Whether the breach requires notification
    - Number of individuals affected
    - Timing of notifications
    - What policies and procedures already were in place
    - Effective date of new policies and procedures
    - Selective documentation
  - There is a fine line between being cute and being dishonest
  - Objective, factual analysis can go a long way.
    - OCR regional offices will be more likely to advance your cause to OCR headquarters.

Breach Investigation – Defense Counsel View

- Specific tasks for legal counsel:
  - Guide the overall investigative response.
    - Serve as the primary contact?
  - Determine applicable breach notification laws.
  - Engage forensics and other third parties to protect under attorney-client privilege.
  - Review the entity’s policies and procedures, making changes as appropriate.
  - Assess third-party relationships for privacy/security risks and seek contractual protections.
  - Determine whether entity has adequate liability insurance coverage.
Contact

Mark J. Swearingen
317.977.1458
mswearingen@hallrender.com

HIPAA Compliance and Enforcement:
Helpful Hints from OCR

Presented by
Celeste H. Davis, Esq.
Regional Manager
U.S. Department of Health and Human Services
Office for Civil Rights - Midwest Region

• These power point slides and Ms. Davis’ remarks, are intended to be purely informational and informal in nature. Nothing in the slides or in the speaker’s statements are intended to represent or reflect the official interpretation or position of the U.S. Department of Health and Human Services, Office for Civil Rights.
OCR Investigation Basics

Types of OCR Inquiries

Complaint Investigations
• 45 C.F.R. §160.306

Compliance Reviews
• 45 C.F.R. §160.308

Information OCR Often Seeks
• Policies and procedures – document and implement
• Comprehensive risk analysis – an ongoing process that includes all PHI
• Workforce training – document training materials and who received training when
• Incident Response – identify and respond, mitigate, and sanction
• Evidence of Sanctions (if applicable)
• Business Associate Agreement (if applicable)

Key Compliance Considerations
• CEs and BAs must undertake a careful risk analysis to understand the threats and vulnerabilities to individuals’ data, and have appropriate safeguards in place to protect this information.
• Take caution when implementing changes to information systems, especially when those changes involve updates to Web-based applications or portals that are used to provide access to consumers’ health data using the Internet.
• Senior leadership helps define the culture of an organization and is responsible for knowing and complying with the HIPAA privacy and security requirements.
HIPAA Data Breach Response Key Elements

#1: Have a Plan

- The Security Rule requires a covered entity or business associate to implement policies and procedures to address security incidents (45 C.F.R. 164.308(a)(6)(i)).
- When developing security incident procedures, consider:
  - What is considered a “security incident”?
  - How will incidents be documented and reported?
  - To whom should incidents be reported?
  - What are reasonable and appropriate responses to certain types of incidents?
- OCR may request evidence that a covered entity or business associate has complied with its security incident procedures.

#1: Have a Plan (Cont’d)

- The Breach Notification Rule requires a covered entity or business associate to implement policies and procedures to address the timely reporting of breaches (45 C.F.R. 164.414(a)).
- When developing breach notification procedures, consider:
  - To whom should workforce members report potential breaches?
  - Who is responsible for completing a risk assessment to determine whether the incident is a reportable breach?
  - Who is ultimately responsible for ensuring that timely notifications are submitted?
  - Ensure that all relevant workforce members are periodically trained on breach response plan as a whole.
#2: Mitigate

- The Privacy Rule requires a covered entity to mitigate, to the extent practicable, harmful effects of uses or disclosures that violate its privacy policies or the Privacy Rule (45 C.F.R. § 164.530(f)).
- The Security Rule requires a covered entity or business associate to mitigate, to the extent practicable, harmful effects of security incidents (45 C.F.R. 164.308(a)(6)(ii)).
- Mitigation examples:
  - Retrieve or otherwise limit the further distribution of impermissibly used or disclosed information;
  - Promptly notifying the affected individual of the violation if the individual needs to take self-protective measures to ameliorate or avoid the harm, as in the case of potential identity theft.

#3: Document

- The Security Rule requires a covered entity or business associate to document security incidents and their outcomes (45 C.F.R. 164.308(a)(6)(ii)).
- Additionally, consider documenting, in detail:
  - Root cause analysis of incident
  - Actions taken to mitigate harm to affected individuals
  - Corrective action measures taken, and if certain actions were not taken, the rationale for not taking them
- Important to retain documentation related to:
  - Internal investigation into incident
  - Risk assessments and submission of notifications pursuant to Breach Notification Rule
  - Implementation of corrective action measures

#4: Determine If the Breach Must Be Reported Under the Breach Notification Rule

- Breach involves only unsecured PHI
  - Encrypted (per NIST Standard) or “unreadable, unreadable, or indecipherable” PHI is considered “secured” PHI
- Breach excludes:
  - Any unintentional acquisition, access, or use of PHI made in good faith and within the scope of authority, or any inadvertent disclosure of PHI by an authorized person to another authorized person at the same entity, provided that the PHI is not further used or disclosed in a manner not permitted under the Privacy and Security Rules
  - A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information
• Breach is presumed, unless the covered entity or business associate demonstrates that there is a low probability that the PHI has been compromised (LoProCo), based on a risk assessment of at least the following:
  • The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
  • The unauthorized person who used the PHI or to whom the disclosure was made;
  • Whether the PHI was actually acquired or viewed; and
  • The extent to which the risk to the PHI has been mitigated

• Breaches affecting 500 or more individuals
  • Notices to OCR, affected individuals, and the media must be made without unreasonable delay and no later than 60 days following the discovery of a breach
• Breaches affecting under 500 individuals
  • Notices to affected individuals must be made without unreasonable delay and in no case later than 60 days following the discovery of a breach
  • Notices to OCR must be submitted no later than 60 days after the end of the calendar year

500 + HIPAA Breaches by Since February 27, 2015
BREACH HIGHLIGHTS

September 2009 through February 27, 2015

- Approximately 1,144 reports involving a breach of PHI affecting 500 or more individuals
  - Theft and Loss are 60% of large breaches
  - Laptops and other portable storage devices account for 32% of large breaches
  - Paper records are 22% of large breaches
- Approximately 157,000+ reports of breaches of PHI affecting less than 500 individuals

LESSONS LEARNED

Appropriate Safeguards Prevent Breaches

- Evaluate the risk to e-PHI when at rest on removable media, mobile devices and computer hard drives
- Take reasonable and appropriate measures to safeguard e-PHI
  - Store all e-PHI to a network
  - Encrypt data stored on portable/movable devices & media
  - Employ a remote device wipe to remove data when lost or stolen
  - Consider appropriate data backup
  - Train workforce members on how to effectively safeguard data and timely report security incidents
Platform for users to influence guidance:
http://hipaaQsportal.hhs.gov/

HIT Developer Portal

- OCR launching platform for mobile health developers; purpose is to understand concerns of developers new to health care industry and HIPAA standards
  - Users can submit questions, comment on other submissions, vote on relevancy of topic.
  - Will consider comments as we develop our priorities for additional guidance and technical assistance

http://hipaaQsportal.hhs.gov/

QUESTIONS?