Spotlight on HIPAA Enforcement: Ongoing Patterns of Non-Compliance

Serena Mosley-Day
Acting Senior Advisor
HIPAA Compliance and Enforcement
HHS Office for Civil Rights

March 27, 2018

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 CFR §§ 164.502(e), 164.504(e), and 164.308(b).

Case Example: Raleigh Orthopaedic

- North Carolina orthopedic practice
- Released PHI to a potential business partner without first executing a business associate agreement
  - Released x-ray films and related PHI of 17,300 patients
  - Entity promised to digitize the images
- $750,000 - April 14, 2016

Business Associate Agreements: Non-Compliant

- The HIPAA Omnibus Rule, issued in January 2013, changed the standards for BAAs
  - Modified BAA requirements
  - Must execute a BAA that includes the modified provisions
  - Compliance date: September 23, 2013

Case Example: Care New England

- Breach notification from Woman & Infants Hospital of Rhode Island
- Unencrypted backup tapes containing the ultrasound studies of approximately 14,000 individuals were missing
- Women & Infants Hospital (CE) provided OCR with a BAA with Care New England Health System effective March 15, 2005
- Document was not updated until August 28, 2015
- $400,000 - September 16, 2016

Risk Analysis: Incomplete or Inaccurate

- 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).

Case Example: Cancer Care

- August 2012 breach report - an unencrypted server backup media and laptop were stolen from an employee's car
- 55,000 patients affected
- Failed to conduct an enterprise-wide risk analysis
- No written policy addressing or controlling the removal of electronic media from its locations
- Had failed to address these deficiencies since 2005
- $750,000 - August 31, 2015

Risk Management: Insufficient

The Risk Management provision of the Security Rule requires a covered entity to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. See 45 CFR § 164.308(a)(1)(ii)(B)

Case Example: 21st Century Oncology

- On two occasions in 2015, the FBI notified 21CO that PHI was illegally obtained by an unauthorized third party and produced 21CO patient files purchased by an FBI informant
- 21CO determined that 2,213,597 individuals were affected
- Failure to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the ePHI
- Failure to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level
- Failure to implement procedures to review information system activity, such as audit logs
- Disclosed PHI to 3rd party vendors without BAAs
- May 25, 2017, 21CO filed for Chapter 11 bankruptcy protection
- $2.3 million - December 14, 2018

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).

Case Example: Memorial Healthcare System

- The login credentials of a former employee of an affiliated physician's office had been used to access MHS ePHI on a daily basis without detection from April 2011 to April 2012
- Affected 80,000 individuals.
- Failured to implement procedures to review, modify and/or terminate users' right of access.
- Failured to regularly review records of information system activity on applications that maintain ePHI by workforce users and users at affiliated physician practices, despite having identified this risk on several risk analyses conducted from 2007 to 2012
- $5.5 million - February 14, 2017.

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).

Case Example: St. Joseph Hospital

- Files containing PHI, were publicly accessible on the internet from February 1, 2011, until February 13, 2012
- The server storing the files included a file sharing application whose default settings allowed anyone with an internet connection to access them
- SJH did not examine or modify the server, resulting in unrestricted access to PHI for 2 years
- $2,140,500 - October 13, 2016

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).

Case Example: Filefax

- A company that was appointed as a receiver to liquidate Filefax's assets has paid a $100,000 monetary settlement to settle potential HIPAA violations.
- OCR determined that Filefax disclosed the PHI of 2,150 individuals between January 28, 2015 and February 14, 2015.
- Disclosed by leaving the PHI in an unlocked truck in the Filefax parking lot, OR by granting permission to an unauthorized person to remove the PHI from Filefax, and leaving the PHI unsecured outside the Filefax facility.

Impermissible Disclosure and Safeguards

- A covered entity or business associate may not use or disclose protected health information, except as permitted or required by the Privacy Rule. See 45 C.F.R. § 164.502(a)
- A covered entity must have in place appropriate administrative, technical, and physical safeguards that protect against uses and disclosures not permitted by the Privacy Rule, as well as that limit incidental uses or disclosures. See 45 CFR 164.530(c).

Case Example: St. Luke's-Roosevelt Hospital Center

- Institute operated by CE impermissibly faxed the complainant's PHI to the complainant's employer
- Institute for Advanced Medicine which provides comprehensive health services to persons living with HIV or AIDS and other chronic diseases.
- Disclosure included: HIV status, STDs, sexual orientation, and physical abuse.
- Similar incident 9 months prior; no changes made
- $387,000 – May 8, 2017

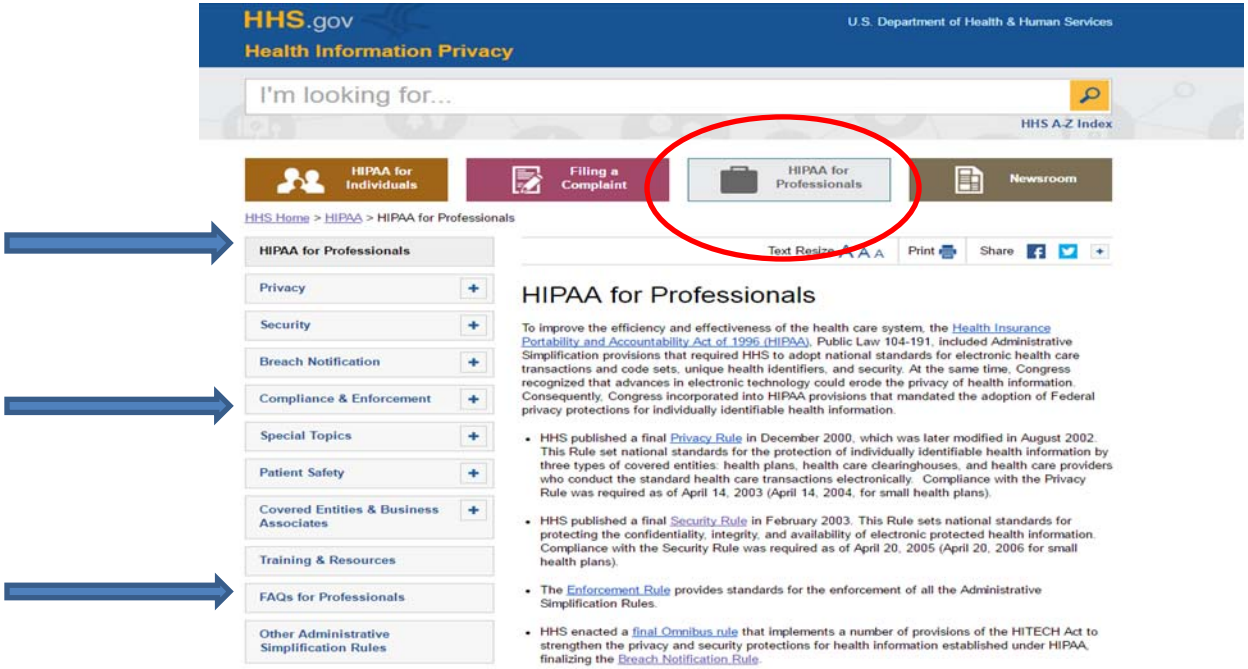
Corrective Actions May Include:

- Updating risk analysis and risk management plans
- Updating policies and procedures
- Evaluating vendor/contractor relationships and updating BAAs
- Training of workforce
- Implementing specific technical or other safeguards
- External monitoring

Some Best Practices

- Review vendor/contractor relationships to ensure required BAAs are in place 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

For More Information



- OCR's website at https://www.hhs.gov/hipaa
- Join our Privacy and Security listservs at https://www.hhs.gov/hipaa/for-professionals/list-serve/
- Find us on Twitter @hhsocr