Data Security and Patient Safety—Two Sides of the Same Coin!

Iliana L. Peters, JD, LLM, CISSP
October 12, 2018

Agenda

- Risk Analysis
- Vendors/Business Associates
- Transmission Security
- Insider Threat
- Ransomware
- Training
- Enforcement Cases
- Questions

SURVEY

- Is a gap analysis sufficient for HIPAA Security Rule compliance?

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.
- When identifying ePHI, 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.)
- April 24, 2017: CardioNet
  - $2,500,000
  - $2.5 million settlement shows that not understanding HIPAA [illegible] creates risk

HHS Risk Analysis Guidance

- http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html
- https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment
- https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-april-2018.pdf

FTC Resources

- https://www.ftc.gov/
- https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf
- https://www.ftc.gov/news-events/press-releases/2018/02/ftc-recommends-steps-improve-mobile-device-security-update
- https://www.ftc.gov/news-events/press-releases/2018/02/ftc-report-finds-some-small-business-web-hosting-services-could

SURVEY

- Are your cloud vendors business associates?

Business Associate Agreements

- The HIPAA Rules generally require 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).
- April 20, 2017: Center for Children's Digestive Health
  - $37,000
  - No Business Associate Agreement? $31K Mistake
- February 13, 2018: Filefax, Inc.
  - $100,000
  - Consequences for HIPAA violations don't stop when a business closes

Vendor Cyber Risk Management

- FTC Guidance: https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series
- NIST Guidance: https://www.nist.gov/cyberframework
- HHS Cloud Guidance: https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
- HHS Business Associate Guidance: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html?language=es
- Remote Access Issues

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).
- February 16, 2017: Memorial Healthcare System (MHS)
  - $5.5 Million
  - https://www.hhs.gov/about/news/2017/02/16/hipaa-settlement-shines-light-on-the-importance-of-audit-controls.html

Transmission Security

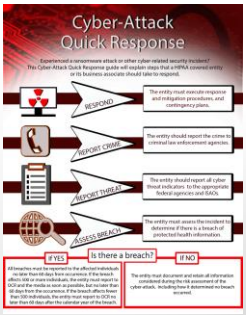
- When electronically transmitting ePHI, a mechanism to encrypt the ePHI must be implemented whenever deemed appropriate. See 45 C.F.R. § 164.312(e)(2)(ii).
- Applications for which encryption should be considered when transmitting ePHI may include:
  - Email
  - Texting
  - Application sessions
  - File transmissions (e.g., ftp)
  - Remote backups
  - Remote access and support sessions (e.g., VPN)
- June 10, 2015: St. Elizabeth's Medical Center (SEMC)
  - $218,400
  - https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/semc/index.html

SURVEY

- Does HHS presume that a ransomware incident is a breach under HIPAA?

Ransomware Attacks

- Phishing and Ransomware
  - Security Awareness and Training and Security Reminders
  - Be Prepared
  - Practice!



Software Patching

- 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.)

Training

- Most settlements include a training requirement
  - https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html
- OCR Published a Monthly Cybersecurity Newsletter
  - https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/cybersecurity-newsletter-archive/index.html
- OCR YouTube Page
  - https://www.youtube.com/user/USGovHHSOCR

Recent FTC Enforcement Actions

- June 6, 2018
  - U.S. Court of Appeals, 11th Circuit Ruling in LabMD, Inc.
  - http://media.ca11.uscourts.gov/opinions/pub/files/201616270.pdf
- Feb 27, 2018:
  - PayPal Settles FTC Charges that Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated Gramm-Leach-Bliley Act
- Nov 29, 2017:
  - FTC Gives Final Approval to Settlements with Companies that Falsely Claimed Participation in Privacy Shield
- Nov 8, 2017:
  - FTC Gives Final Approval to Settlement with Online Tax Preparation Service
- Aug 15, 2017:
  - Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims

Questions?

- Feel free to contact me for more information:
  - Iliana Peters: ipeters@polsinelli.com