Health IT Security In 2017
What You Need To Know In 15 Minutes Or Less

Health TechNet Presentation January 27, 2017

David F. Katz, Leader, Privacy and Data Management Practice Group

Nelson Mullins®
Nelson Mullins Riley & Scarborough LLP

David Katz, Leader, Privacy and Data Management Team

david.katz@nelsonmullins.com 404.322.6122 | @KatzFDavid

Nelson Mullins.
Nelson Mullins Riley & Scarborough LLP

Privacy Rule

The HIPAA Privacy Rule: located at 45 CFR Part 160 and Subparts A and E of Part 164.

- Establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.
- Requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.
- Gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

Security Rule

The HIPAA Security Rule: The Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164.

- Establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity.
- The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

Specifically, covered entities must:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.

Overview Top 10 Health Care Data Breaches 2016

Premier Healthcare, LLC	205,748	Unencrypted laptop stolen
Central Ohio Urology Group, Inc.	300,000	Unauthorized post to open internet
California Correction Health Care Services	400,000	Unencrypted laptop stolen
Radiology Regional Center, PA	483,000	Lee Co., PA's Solid Waste Div. left them on the street
Peachtree Orthopaedic Clinic	531,000	Result of "cyber attack"
Bon Secours Health System Incorporated	651,971	Vendor error
Valley Anesthesiology and Pain Consultants	882,590	Unauthorized access
21st Century Oncology	2,213,597	"Inappropriate" access by an unauthorized third party
Newkirk Productions, Inc.	3,466,120	Unauthorized access
Banner Health	3,620,000	"Cyber attack" on card holder data

Underlying Themes To 2016

- Insecure Networks/ User Accounts / Unauthorized Access / Ransomware
- Mobility / Theft / Lack of Encryption
- Disposal / Loss
- Lack of Security Controls, Compliance or Culture

OCR In 2016

13 OCR HIPAA Settlements Total 23.5 million

- Focus of OCR: Regulatory Risk Assessments and Business Associate Agreements

Highlights:

- University of Mass Amherst: $650,000 malware infection.
- Care New England Health System $400,000 no BAA in place.
- Advocate Health Care Network $5.55 million 3 data breach reports in less than 3 weeks.
- University of Mississippi Medical Center $2.75 million found to no have adequate risk management security measures.
- Oregon Health & Science University $2.7 million OHSU storing data using non-business associate internet-based services provider Google.

Risk Assessments

The Administrative Safeguards provisions in the Security Rule require covered entities to perform risk analysis as part of their security management processes.

- A risk analysis process includes, but is not limited to, the following activities:
  - Evaluate the likelihood and impact of potential risks to e-PHI;
  - Implement appropriate security measures to address the risks identified in the risk analysis;
  - Document the chosen security measures and, where required, the rationale for adopting those measures; and
  - Maintain continuous, reasonable, and appropriate security protections.

Focus 2017

- Healthcare Security and Application to New Technologies:
  - IOT poised to hit $117 Billion. Marketresearch.com
  - Philips and Qualcomm in partnership to develop IT Ecosystem. Forbes
- Threats:
  - DDOS Attacks and October 21, 2016 / Outages and Performance / Disruption / Collateral Damage
- Truths about Healthcare Security:
  - You are going to have a breach sooner or later
  - Threats are going to come from sources we have not previously seen to date
  - No security can be static because the threats are constantly changing

Focus 2017

- Audit Controls:
  - OCR January 2017 Newsletters 45 C.F.R. 164.312(b)
- HIPAA Security Rule requires Covered Entities and Business Associates to implement hardware, software and/or procedural mechanism that record and examine activity in information systems that contain or use e-PHI.
- Questions that Covered Entities and Business Associates should consider:
  - What audit control mechanism are reasonable and appropriate to implement so as to record and examine activity in information systems that contain or use e-PHI.
  - What are the audit control capabilities of information systems with e-PHI?
  - Are changes or upgrades of an information system's audit capabilities necessary?

Focus 2017

- Vendor Audit and Review
  - Leverage Next Generation Security Systems
- Deployment and Policy Adoption together with Testing New Systems
- Digital Devices, Interconnected Technology, Controls for Threats, the User Experience and Business Benefit
- Robust Incident Response:
  - See DHS refreshed version of National Cyber Incident response plan www.us-cert.gov/ncirp