Cyber Hot Topics Webinar Series:

Data Security Strategies Suited to Small Physician Practices

May 17, 2017
11:30AM – 12:15PM CST

Presented by: Amy S. Leopard, Judd A. Harwood, and Jordan A. Stivers

Presenters

Amy S Leopard
Nashville

Judd A. Harwood
Birmingham

Jordan A. Stivers
Nashville

Bradley

Welcome from the Bradley Cybersecurity and Privacy Team

Breach Incident Response

- 17 attorneys in 4 offices
  - Healthcare
  - IP
  - Financial Services and Banking
  - Litigation
  - Government Contracts
  - Insurance coverage issues

Health Information and Technology (HIT)

- Compliance Training and HIPAA audits
- Operational and Regulatory Guidance
- Contracting
  - Data Sharing
  - Outsourcing/ IT Procurement
  - Vendor Management
- Due Diligence

Next Webinar August 16, 2017 11:00 CST
HIPAA Comes of Age

Bradley

Agenda

- The threat landscape
- Technical controls
- Administrative controls

Bradley

The Threat Landscape

Bradley

The Threat is Real

- Healthcare has become one of the most highly targeted industries for cyber attacks.
- Sensitivity of healthcare information + lack of cybersecurity sophistication makes healthcare an attractive target.
- You can change your credit card information if it is compromised, but you cannot change your health information, date of birth, etc.
- Healthcare providers need their patients' healthcare information to provide care, and are more likely to pay to get it back.

Most Common Types of Security Incidents

- Phishing attacks
  - *Ex. An employee receives an email with a link, clicks on it, and malware is installed on the computer*
- Ransomware
  - *Ex. An image pops up on your screen that says "Your data has been locked and encrypted, you must pay $_____ within 48 hours to unlock it or it will be permanently destroyed."*
- Misdirected information
  - *Ex. A patient's file is accidentally sent to the wrong email address.*
- Lost or stolen laptop or smartphone
  - *Ex. An employee's laptop containing patient information is stolen from his car.*

Bradley

Why would a small physician practice be the target of a cyberattack?

- Most small clinics and physician practices do not have dedicated IT or privacy personnel.
- Cybersecurity and privacy concerns are treated as secondary to providing medical care to patients.
- Cybersecurity can be confusing and overwhelming, and providers do not know where to begin.
- Hackers know this, and view clinics and physician practices as an easy target.

Why cybersecurity should be a priority

- If your information is compromised, it may affect the care you are able to provide to patients.
- You have a legal obligation to protect patient information (HIPAA, state data security laws).
- The cost of responding to a data breach can be very expensive.
- Legal reporting requirements.
- Potential loss of patient trust.

Technical Controls

Bradley

Firewalls

- A firewall is a system designed to prevent unauthorized access to or from a private network.
- Its job is to inspect all messages coming into the system from the outside and decide, according to pre-determined criteria, whether the message should be allowed in.
- Software v. hardware firewalls
- Software firewalls are generally more appropriate for small clinics and physician practices.

Install and maintain anti-virus software

- A primary way that attackers compromise computers in a small practice setting is through viruses and other malicious code that exploits vulnerabilities on the machine.
- Keep anti-virus software up-to-date to protect against the newest viruses and malware.
- Symptoms of an infected computer system.

Choose a secure EMR system

- Some features to look for when choosing an EMR vendor:
  - “Software as a service” or web-based offering (ePHI will be stored at the vendor’s secure data centers rather than on your computers)
  - Continuous updates to the software
  - Certified for Meaningful Use

Practice good computer habits

- Configuration Management:
  - Uninstall any software application that is not essential to running the practice (e.g., games, instant messaging, photo-sharing tools)
  - Do not simply accept the default configuration
  - Disable remote file sharing and remote printing within the operating system configuration
- Keep all software up-to-date

Practice good computer habits

- Operating system maintenance:
  - Delete user accounts for former employees
  - “Sanitize” computers and other devices before disposal
  - Old files are deleted/destroyed
  - Uninstall all outdated or unused software

- Wireless networks – set to encrypted mode, do not allow visitors to access the wireless network

Encryption

- If you maintain any patient information on office computers, it needs to be encrypted.
  - Windows – BitLocker
  - Mac - FileVault
- If you send patient information via email, it needs to be encrypted.
  - Outlook
  - Apple Mail
  - Gmail

Bradley

Mobile devices

- Increased risk associated with accessing patient information from a mobile device.
- The notorious “stolen laptop” – do not leave laptops or other mobile devices in view of others.
- Protections:
  - Password or other user authentication
  - Encryption
  - Personal firewalls for mobile devices
  - Do not send health information over public Wi-Fi networks

Administrative Controls

Bradley

Establish a culture of security

- Many security incidents are the result of human error
- Passwords
  - Pick a good one
  - Do not share
  - Do not write it down
- Lock your computer when you are away from your desk
- Access control – limit access to those who need it to do their job
- Limit physical access, and do not remove hard copy files from the practice setting

Bradley

Policies, procedures & training

- Policies and procedures need to be finalized, implemented, and actually practiced.
  - *Recent OCR settlement for failure to finalize and implement polices and procedures.*
- Draft procedures with usability in mind.
- Regularly train employees on the policies and procedures, and designate someone responsible for answering questions about policies and procedures.
- Creative ways to reinforce privacy and security principles during daily tasks.

Questions?

aleopard@Bradley.com

jharwood@Bradley.com

jstivers@Bradley.com

Bradley

Sources

- "How Can You Protect and Secure Health Information When Using a Mobile Device?" https://www.healthit.gov/providers-professionals/how-can-you-protect-and-secure-health-information-when-using-mobile-device
- "Top 10 Tips for Cybersecurity in Health Care" https://www.healthit.gov/providers-professionals-newsroom/top-10-tips-cybersecurity-health-care
- "The Physician's Guide to Protecting Patient Information" September 11, 2014. Capterra Medical Software Blog. http://blog.capterra.com/physicians-guide-protecting-patient-information/
- "HIPAA Compliance on a Small Practice Budget" Cam Roberson, February 4, 2015. Medical Practice Insider. http://www.medicalpracticeinsider.com/best-practices/hipaa-compliance-small-practice-budget
- "Quick, Low-Cost HIPAA Compliance Solutions for Small Practices" Tammy Worth, January 13, 2016. Renal & Urology News - http://www.renalandurologynews.com/hipaa-compliance/quick-low-cost-hipaa-compliance-solutions-for-small-practices/article/464950/
- "Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices" https://www.hhs.gov/sites/default/files/small-practice-security-guide-1.pdf
- "HITRUST Announces HITRUST CSF Roadmap Including a New Simplified Program for Small Healthcare Organization and NIST Cybersecurity Framework Certification" May 1, 2017. https://hitrustalliance.net/hitrust-csf-roadmap-including-new-simplified-program-small-healthcare-organizations-nist-cybersecurity-framework-certification/

Bradley