Healthcare Cybersecurity: Protecting Patients From Evolving Threats, Inside and Outside the Organization

Yolanda Sims, JD, MHA
Loss Prevention & Risk Management Advisor

Disclosure

• No conflicts to disclose.
• This presentation is intended to be a high-level educational seminar, and is not intended as legal advice. Legal advice is highly particularized and based on specific facts, circumstances, and the client’s needs, and the advice is given in the context of a specific attorney-client relationship that does not exist here. For specific questions relative to your practice and individualized needs, consult your attorney.
• KAMMCO is a professional liability company. One or more members of this audience may be insured by my employer.
Today’s Agenda

• Review security threat vectors that are most impactful in healthcare organizations.
• Identify risks related to cybersecurity incidents.
• Practical tips to protect against cybersecurity insider/outsider threats.
The ransomware attack, according to the hospital's news release, disrupted and affected the following services:

- No outpatient lab, respiratory therapy and radiology exams or procedures.
- No new inpatient admissions
- Some surgery cancellations
- Patients presenting to the emergency department and walk-in clinic will be triaged and transferred to an appropriate care facility if needed.
- Phone systems were operational.

• Data breaches cost the healthcare industry $6.5M or $429.00 per patient record.
• For the ninth consecutive year, the healthcare industry is the hardest hit financially by data breaches.
• The costs are directly related to legal, technical and regulatory functions such as patient notification, credit monitoring, and reputational damage.

Let’s Talk About Hackers!
THREAT: RANSOMWARE ATTACKS

What is Ransomware?

• Ransomware is a type of malware distinct from other malware.
• It denies you access to your information and files.
• It encrypts the data with a key known only to the hacker who deployed the malware.
• It is released when ransom is paid $$$$.
Disruption of Services

[Image of a hospital with a sign saying "Sorry We’re Closed"]

Google Ransomware War Map 9.20.19

https://www.google.com/maps/d/viewer?mid=1UE6Nko9iRG1t1ci_AeqqszxGzs&ll=39.802613835499116%2C‐107.45439572248102&z=4
Should You Pay the Ransom?

• Paying a ransom does not guarantee that the hacker will unencrypt or unlock the stolen or locked data.

• Law enforcement and government agencies such as the FBI, say don’t pay unless you really have to.

THREAT: Email Phishing Attacks
What is Email Phishing?

Email phishing is an attempt to trick you, a colleague or someone else in the workplace into giving out information using email.

Phishing attacks rely on human tendencies, which is why email is the most common initial point of compromise for significant security incidents.

Ex: Your employee receives a fraudulent email from a cyber-attacker disguised as an IT support person from your patient billing company. An employee clicks the link, which collects that employee’s login credentials and transmits information to the attackers.

Boost Your Phishing IQ: Use Critical Thinking Skills

Don’t take everything at face value. Before you open and click an email go through these questions:

• Is the email from someone I recognize?
• Am I expecting the email?
• Are the requests of the email reasonable?
• Is the email using emotional gauges like fear or urgency to entice an action?
Always Hover

- Before clicking any links in the email, hover your mouse over the link and the actual URL will appear.
- Double check to make sure the real URL is leading you to the right place.
- You don’t want to click a link to juspandoo.de/82359/index.html.
- Hackers will also try to spoof the URL to look like the legitimate address.
- Investigate to make sure the domain is the same as the sender of the email.

Email Phishing Don’ts

- Don’t copy and paste the link into the URL section of your browser to check it. That’s the same as clicking the link.
- Don’t forward a suspected malicious email to other people.
- Don’t open the malicious email on your mobile devices. They are not immune to malware and viruses.
- Don’t solely rely on antivirus software. Antivirus protects against known signatures, but are susceptible to new malware that goes undetected.
THREAT: Loss of Theft of Equipment or Data

Every day, mobile devices such as laptops, tablets, smartphones, and USB/thumb drives are lost or stolen.

The threat is far worse if the lost device was not appropriately safeguarded or password protected.

• Loss or malicious use of unsecured PHI may result in business disruption and compromised patient safety.

• May trigger regulatory obligations and notification to patients.

Ex: a physician stops for a coffee. As he leaves the table momentarily to pick up his coffee, a thief steals the laptop. He returns to find the laptop gone.
Do you know your organization’s policy on removing equipment from the workplace?
Ask the following:
• Can I travel with my equipment?
• Can I take my equipment offsite to work remotely?
• Are USB or other portable storage devices allowed?
• Is the information on my computer or device encrypted?
• Is there a secure VPN that I can use, along with secure, password-protected Wi-Fi to log into the network and work?

Vulnerabilities of Mobile Device

Bring Your Own Device ("BYOD")
• Hospital issued vs Employee owned
• Personal use on Hospital-owned devices
• PHI on devices? Remote Access?
• Policies regarding use
• Ability to remotely wipe
• Mobile Device Management Software
Insider Threats: Accidental or Intentional Data Loss

Human error is a significant initial point of compromise, which is why insider threats are so prevalent.

- An accidental insider threat is unintentional loss caused by honest mistakes or a degree of negligence.
- An intentional insider threat is malicious loss or theft with the objective of personal gain or inflicting harm to the organization or another individual.

Ex: An attacker impersonating a staff member of a physical therapy center contacts a hospital employee and asks to verify patient data. Pretending to be hospital staff, the imposter acquires the entire patient health record.
Insider Threats vs. Outsider Threats

**Insider Threats**: Employees, contractors, or partners can commit fraud, espionage or theft of intellectual property.
- Insider threats are successful with the use of ransomware, malware, business email compromise, phishing scams etc.

**Outsider Threats**: Cyberterrorists, hackers
- Data breach, denial of service attacks, cybersquatting etc.

**THREAT: Medical Device Attacks**
Medical Device Attacks

IT experts are concerned that recent trends will convince cybercriminals to target medical devices such as pacemakers or Intensive Care Unit (ICU) respirators.

- Know your organization’s protocols in case of a potential shutdown or attack against medical devices.
- That means asking: 1) How do we notify patients if medical devices are compromised? 2) How do patients notify us if they suspect their medical device is compromised?
- Engage vendors or manufacturers of medical devices to understand vulnerabilities, risks and appropriate protection and response measures.

What is the Real Cost of a Data Breach?

Detection and Escalation
- Forensics and investigative services, crisis team management

Notification Costs
- Letters, emails and outbound calls to notify the person their information has been compromised

Post Data Breach Response
- Credit monitoring, legal expenditures, regulatory fines

Lost Business Cost
- Cost of business interruption, revenue loss and reputation loss
The HIPAA Security Rule & Meaningful Use incentives require physicians to conduct a security risk analysis.

Covered Entities have an obligation to implement administrative, technical and physical safeguards to protect the confidentiality, integrity and availability of protect health information.

OCR is increasing their enforcement efforts in this area. No organization, big or small is exempt. If you fail to comply, you may be the next covered entity listed on the OCR Breach Portal (“wall of shame”).
Common HIPAA Violations Revealed in OCR Investigations

- Impermissible uses and disclosures of PHI
- Lack of safeguards of PHI
  - Encryption
  - Ability to remotely wipe a hard drive
- Use or Disclosure of more than the minimum necessary rule
- Lack of administrative safeguards

HHS “Wall of Shame”
The Three P’s

Policy: THE WHAT
- Timely
- Relevant
- Defend against the current threat landscape.

Procedures: THE WHO
- You must be able to demonstrate that you have procedures in place based on the policies.

Practice: THE PROOF
- Evidence that you practice those procedures.

Cyber Hygiene: Practical Tips to Mitigate Cyber Threats
Tip 1: Establish a Cybersecurity Policy

Define all cybersecurity roles and responsibilities throughout the organization.

• This includes who will establish policy and who will implement and conduct security practices.

Tip 2: Conduct Security Risk Assessments

Use security risk assessment results to take actions and further enhance your cybersecurity efforts.

• First, start with a GAP analysis.
  • Identify threats and vulnerabilities and their potential impact.
  • Maintain a complete, accurate and current asset inventory profile to ensure you know where PHI resides.
  • Including laptops, USB drives and mobile devices.
Tip 3: Conduct Phishing Tests and Simulated Attacks

Do you know your phishing click rate at your practice or facility?
• Routinely launch “fake phishing scams”, use click bait to test your workforce’s awareness.
• Raise the collective phishing IQ of everyone.
• Train workers to trust their instincts and use common sense.

Tip 4: Monitor the Monitors

• Limit access to people who need it to perform their job duties, but be wise, snooping still exists.
• Security settings should monitor for unauthorized access or access attempts at every level.
Tip 5: Encryption, Encryption, Encryption

Extensive encryption is a huge cost saving measure.

Tip 6: Workforce Training

Provide security awareness training and education for all staff.

- Define the mechanisms that will be used to train workforce on cybersecurity practices, threats and mitigations.
- Ensure that education includes common cyberattacks, lost/stolen devices and methods for reporting suspicious behavior on their computers.
- The user base should be all users and a dedicated cybersecurity department or individual.
### Tip 7: Pay Attention to Third Party Vendors, Contractors and Consultants

- Look at risks that involve third party partners.
- Always review their business associate agreements on an annual basis.

### Tip 8: Protect Yourself from Ransomware

Backup your data and use the 3-2-1 backup rule
- Have 3 copies of your data, 2 copies on different media types and 1 copy offsite.

Patch/Update your software
- Develop a regular patch update program and make someone responsible for implementing it.

Use Anti-Virus Software
- Use from a reputable source and keep it updated.
Tip 9: Have An Incident Response Team & Test Your Incident Response Plan

• Companies that do both, save considerably more money than those that do not.
• Create a ransomware recovery playbook.
• Conduct several table tops or demonstrations throughout the year.
• Cyber threats are ever evolving, extensive training will help ensure you are ready to respond when it happens.

TIP 10: Stay Ready!
Final Takeaways

1. Adopt a security framework
   - NIST, HHS, HIMSS
2. Develop cybersecurity plans and policies
   - HHS guidance is a great starting point
3. Insure against remaining threats
   - Purchase cybersecurity coverage

Any Questions?

Yolanda Sims, JD, MHA
Loss Prevention & Risk Management Advisor
ysims@kammco.com
800.232.2259
References


Chase, M and Mohs, A. Thinking Inside the Box: How to Identify and Tackle Insider Cyber Threats. Baird Holm LLC Aug. 12, 2019


2019 HIMSS Cybersecurity Survey
