Cyber Liability Tip Sheet

Cyber Attacks are on the Rise in Healthcare

In 2014, the FBI signaled an alarm to the healthcare industry, calling it “a rich new environment for cybercriminals to exploit.” Only in recent years has the healthcare industry begun the process of transitioning from paper to electronic systems. The rush to adopt the technology has left some healthcare organizations more focused on the clinical and workflow aspects of the electronic systems and less focused on data security. Meanwhile, cybercriminals have discovered new opportunities for financial gain from the virtual “treasure trove” of information contained in a medical record and medical devices.

Financial Impact of a Data Breach

According to the Poneman Institute’s 2015 Cost of Data Breach Study, the financial impact of a data breach continues to increase. In fact, in 2015, the financial impact hit a record high. Over the last ten years, there has been an 11% increase in the total cost of a data breach; the average cost per lost or stolen record for all industries is $217.00. The healthcare industry is substantially above the average at $398 per record stolen.

Primary Causes of Data Breach

Malicious or criminal attacks continue to be the primary cause of data breach.
Tips for Preventing/Mitigating Damages from a Data Breach

1. Software, hardware, and procedural methods to protect applications from external threats, such as firewalls
2. Application security
3. Database security
4. Endpoint protection
   i. Require endpoint devices to comply with specific criteria before they are granted access to network resources.
5. Administrative policies and procedures (For example, audit policies, facility access controls, contingency plans, security incident response and reporting, workforce clearance, termination procedures)
6. Workstation policies and procedures
   i. Mobile device policies
   ii. Retirement of devices that may contain PHI
7. Data protection/encryption
8. Maintain Business Associates Agreements (BAAs)
   i. HHS sample Business Associate Contract
9. Vulnerability management
10. Security risk assessment/management
   i. HealthIT.gov Security Risk Assessment tool
11. Identity and access management control
12. Mobile security and access controls
   i. HealthIT.gov offers a library of materials on mobile device management and security
13. Data breach detection solutions
14. Data governance
15. Malware analysis
16. Consider risk transfer (cyber liability insurance)
17. Training and awareness
18. Breach response plan

Teach Your Staff

Begin training staff (permanent, temporary, and contractors) during the orientation process, followed by regular ‘refresher’ training and briefings on healthcare privacy and security. Teach staff to identify suspicious emails, links, and emails and how to respond if they receive one of these.

- Suspicious emails - A suspicious email may tell the user that they should immediately review an overdue invoice or a similar tactic to entice the user to open the attachment.
- Suspicious links – A common tactic is to offer free software upgrades to commonly used software that contains malware.
- Suspicious websites – Attackers entice victims to visit the infected website and then run their malware once the victim downloads infected software from the website.

Respond Promptly to Mitigate Risks

Immediately notify your IT department, the FBI, and Mag Mutual if you believe you are a victim of a cyber attack. Early intervention may mitigate damages.

More Information of Cyber Security from HealthIT.gov


iii Ponemon Institute, 2015.

The content and information presented here is intended to be used for general information and is not legal advice. It does not create an attorney client relationship. Consult a licensed attorney to assist with specific situations that require legal advice or counseling.

6/17/2016