For the healthcare sector, 2016 was a frenetic year with an onslaught of ransomware attacks, hacking attacks and data breaches along with a record number of HIPAA enforcement actions. The healthcare sector saw 310 cyber-related incidents in 2016 with 16.1 million individuals affected by those data breaches.

Several factors drive the motivation for attacks on the healthcare sector. Healthcare records have valuable personal information that can be used by cyber criminals in a variety of malicious ways. With access to healthcare information and other personal data, attackers can access healthcare services on behalf of the individual, file fraudulent claims, or use the victim's identity to commit other crimes.

5 Steps to Mitigate Your Risks

Healthcare entities that implement the following best practices and are able to demonstrate they have made business decisions with privacy and data security in mind fare much better in the midst of an investigation.

5X MORE RANSOMWARE ATTACKS

[2]2015-2016 KASPERSKY LABS ANALYSIS

1. Conduct a Risk Assessment

Risk assessments and analysis are the foundation to mitigating the risks above and preventing an unpleasant experience with the U.S. Department of Health and Human Services Office for Civil Rights ("OCR"). Failure to conduct a risk analysis is the most common HIPAA violation found during the OCR's investigations. Analyzing the organization's risks is the starting point to determining a proper information security program and appropriate risk mitigation measures.

[1] http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

[2] Kaspersky Lab official blog article, "Ransomware's History and Evolution in Facts and Figures", released June 3, 2016 (accessed January 27, 2017)

2. Train Employees

Employee training is another key element of HIPAA compliance and mitigating associated privacy and security risks. HIPAA Rules require that the organization's workforce is properly trained on the HIPAA Privacy, Security, and Breach Notification Rules. Additionally, employees that have access to protected health information ("PHI") need to be trained on the specific privacy and security policies and procedures. Healthcare regulators will typically request to see an organization's training reports during an investigation or audit. They want to see documentation that employee training took place to address privacy and security risks.

In addition, employees should also be trained on email security and malware. All office and professional medical staff should be trained on data security practices to maintain a high degree of suspiciousness, check return email addresses, make sure their equipment is current on all updates and anti-malware software, and to never be afraid to report suspected incidents.

3. Implement Policies & Procedures

HIPAA's Privacy and Security Rules require healthcare organizations to have data security policies and procedures addressing a multitude of risks. Inadequate policies and procedures are a frequent violation cited in HIPAA enforcement actions.

Having appropriate policies and procedures in place is the first step towards compliance. Enforcing those policies and procedures is the next step. These policies must be reviewed no less than annually and when needed based on risk, law changes, technology, and environment.

4. Manage Vendors Appropriately

Vendor risks have become one of the top data security concerns for healthcare organizations. As OCR holds business associates and covered entities liable for HIPAA compliance when it comes to vendor relationships, it is important for healthcare organizations to have a vendor managment program in place to maintain control of their business associates processing PHI. Business associate agreements should have appropriate data security provisions that hold business associates to the same standards as the covered entity and requires them to push down the same requirements to their vendors.

5. Prepare an Incident Response Plan

The best way to handle a data breach is to be prepared well in advance.

When responding to a data breach, critical decisions must be made in a condensed time frame. Notification deadlines apply to all healthcare organizations, most notably is the 60 notification deadline to OCR and affected individuals. Any mistakes can be costly and have a lasting impact.

Having a game plan – incident response plan – in place, and a response team that has rehearsed the plan, can minimize harm to the organization and those affected. That includes having established relationships in place, if only with an external breach management team which has relationships with forensic analysts, mail houses, and regulators.

Having a game plan – incident response plan – in place, and a response team that has rehearsed the plan, can minimize harm to the organization and those affected. That includes having established relationships in place, if only with an external breach management team which has relationships with forensic analysts, mail houses, and regulators.

Top 10 Actions to Take Right NOW!

As the best practices above may take time to implement, following are 10 simple steps that healthcare providers can take now to reduce their vulnerabilities to cyberattacks:

1

Never email patient information

2

Don't fax patient data unless there is no other choice.

3

Keep devices updated with all software updates.

4

Eliminate patient SSNs except where you absolutely need them for government insurance programs.

5

Encrypt all laptops.

6

Ensure all users have their own access accounts.

7

Do NOT share passwords or post them somewhere easily found.

8

Change the default passwords on all equipment and software.

9

Lock machines when you walk away.

10

Implement two-factor authentication on all accounts including email.