St. Louis Medical News
Your Primary Source for Professional Healthcare News
April 2012 >> $5

*the*PracticeSpecialist

BY RON PRESENT

Cyber Threats – Are You Protected Against an Electronic Security Breach?

By RON PRESENT

With all the news and chatter surrounding electronic health records and meaningful use, healthcare providers are becoming more dependent upon their systems and data to manage their patients and businesses. While the changing information system infrastructure needs offer significant opportunities and benefits, they also carry many new and significant risks, including cyber security risks that providers, managers, payors and patients need to be aware of.

To protect your practice from cyber security threats, it's time to start thinking like a hacker. What sensitive, confidential or HIPAA data do you collect, store or transfer that could be compromised? And how vulnerable is that data to attack?

The risk is significant for practices that do not make cyber security a priority. Failing to put security measures and infrastructure in place can cripple not only a practice's bottom line, but also create a public reputation and regulatory nightmare. Within a healthcare provider's data base are oftentimes stored patients' social security numbers, financial account data, birth dates, addresses and phone numbers which make that information valuable to cyber criminals and identify thieves.

The types of organizations being targeted are becoming more varied, says Tony Munns, Member, Risk Advisory Services, Brown Smith Wallace LLC. "Several years ago, the primary targets were financial services and similar organizations, but we are now finding that other companies with a high dependence upon technology are becoming targets for attack with particular focus on healthcare operations," says Munns. "The size of the practice doesn't seem to matter, as hackers often choose their targets based on ease of attack and availability of data although smaller providers are identified to be an easier target because of typically more limited resources."

According to Pamela Lewis Dolan from the American Medical News, "The Top Cyber Security Trends for 2012, as compiled by Kroll's Cyber Security and Information Assurance, reported that small practices are more susceptible to security vulnerabilities because they are "the path of least resistance." Many rely on outdated technology. Basic security protections, such as proper use of encryption, often are overlooked as practices focus on meeting regulatory requirements, such as those related to meaningful use."

What cyber security challenges are healthcare providers facing?

While healthcare providers are not purposely exposing themselves to cyber security risks, many smaller practices have traditionally limited resources to understand and address their vulnerabilities. Today, providers are doing more with less at a time when the number and severity of attacks are on the rise. The greatest challenge is that this is a complex area that is constantly changing, requiring expertise and resources that often aren't readily available. Providers often focus on keeping systems up and running, while information security drops down the priority list.

What impact will practices face because of these issues?

There are many potential impacts if sensitive information is not adequately protected, including direct costs such as fines, investigation, notification and legal fees, and indirect costs, including lost business opportunities due to reputational harm. The impact can also depend on applicable laws and regulations, such as:

• HIPAA — The Health Insurance Portability & Accountability Act, which addresses the protection of personally identifiable health information; and

• PCI DSS — The Payment Card Industry Data Security Standards, which is aimed at protecting payment (credit, debit) card security which is of great significance as more and more providers are accepting payment through credit cards.

It is critical today for providers to establish security measures and an infrastructure that protects data so that if security is breached, there is a record of compliance with laws and regulations. Across the board, there is an emphasis on urging all providers to get their house in order on matters of cyber security.

How do cyber security breaches occur?

There are generally two basic types of security incidents. First, there are unintentional situations, such as an employee losing a laptop computer containing protected data. In these cases, data security is generally not top of mind, as no one plans on these incidents.

The other security threats are very much intentional. There are cyber criminals who make money by hacking into systems and mining data. Once a system is compromised, the attacker can siphon off data or steal money directly, for example by initiating bank account transfers or payments to fictitious vendors.

What can providers do to protect their interests?

The key is to identify security risks and put an appropriate security program in place. A security program should include a comprehensive security policy with assigned responsibility, risk assessment, security control framework, independent assessment and employee awareness. And, for when all else fails, there should be a response program, which should be tailored to meet regulatory requirements and be regularly tested.

Even if you are a small provider with limited resources, you are held to the same standards as large providers with "armies" of technology experts. Reach out to an expert and conduct a security risk assessment and begin developing a plan to protect information from cyber threats. When — not if — a security breach occurs, you want to be prepared with a plan to protect you and your patients' interests.

Ron Present, CALA, CNHA, is the healthcare services practice leader for Brown Smith Wallace LLC, one of the Midwest region's most prominent locally owned full-service public accounting firms. INSIDE Public Accounting has recognized Brown Smith Wallace nationally as a Top 5 Fastest Growing Firm in the $20-30 million net revenue category. Email him at RPresent@bswllc.com.