NELSON HARDIMAN
HEALTHCARE LAWYERS

HIPAA Security Breaches Raise Bar for HIPAA Compliance

With the U.S. Department of Health and Human Services Office fo

Rights (OCR) about to begin a second phase of audits of covered entities and business, healthcare organizations should be c checking that they are in compliance with the federal Health Insurance Portability and Accountability Act (HIPAA). That's certa good move, but is it enough to protect the privacy of your patients?

Healthcare Data Hacking is on the Rise

Data hacking from healthcare organizations increased an astounding 1,800 percent from 2008-2013, according to a new stud there is every reason to think 2014 and 2015 will continue the trend. Coming on the heels of the major breach at health insure Anthem, which compromised the data of potentially 80 million current and former customers, it is clear that computer savvy criminals are outpacing healthcare defenses by a huge margin.

The Brookings Institution reviewed Health and Human Services reports of data breaches where more than 500 patients were exposed and found that the number went from just 13 in 2008 to 256 in 2013.

The Brookings report notes that the healthcare sector is an increasingly attractive target for hackers, and another think tank, t Ponemon Institute, reports that about 40 percent of health organizations experienced criminal cyber-attacks in 2013. The num are high because hacking a healthcare organization promises a great return on investment.

A hacker can sell personally identifiable information and Social Security numbers, which often are compromised in healthcare hacks, on the black market for at least ten times what credit card information is worth. A set of complete health insurance credentials for an individual sold for a minimum $20 on underground markets in 2013, and that figure is likely higher today. Th up to 20 times more than hackers get for what most people assume is the hot ticket for fraud — a U.S. credit card number wit security code. Yet, the retail industry tends to secure credit card information much better than the healthcare industry protects personal information of patients. Hackers have recognized that disparity and are going after healthcare organizations with gus

The Actual and Hidden Costs of a HIPAA Violation

Once they breach the gates and make off with your data, a healthcare organization is facing trouble on many fronts. HIPAA penalties can be $10,000 per violation, with an annual maximum of $250,000 for repeat violations, when the breach is caused "willful neglect," the likely category for failing to secure a computer network. A willful neglect issue that is not corrected in the required time period can cost you $50,000 per violation, with an annual maximum of $1.5 million.

But that's only the beginning. Reporting the breach to the government and affected patients will result in significant publicity fo

your organization — none of it good – and that can directly affect your bottom line when patients choose to go elsewhere. The organization also will incur the cost of notifications, investigations, and remedial actions such as offering credit monitoring to t affected.

Those costs add up quickly, evidenced by the Ponemon Institute's finding that the average per-capita cost of handling a data breach is $359 in the healthcare industry, compared to $201 in other industries. In theory at least, that means Anthem could l more than $28 billion from its breach. Even if Anthem manages to pare that number down significantly, the financial cost will b tremendous.

Rethink Your HIPAA Compliance Program

When you are the target of focused efforts by criminals who are really good at what they do, even a solid HIPAA compliance program may not be enough to protect your data. Think of HIPAA compliance as merely the baseline to keep federal regulato bay, and then think seriously about how to defend against a purposeful attack on your data system. Remember, HIPAA is aim mostly at prohibiting willful or careless data breaches from within the healthcare organization rather than defending against ar outside attack.

Hackers are using increasingly sophisticated methods to probe healthcare networks for weaknesses, taking advantage of hov healthcare networks are now so complex that they challenge even the best IT professionals to secure them and monitor them closely for evidence of attack. In what Anthem called a "very sophisticated external cyber-attack," hackers managed to steal lo keys and passwords from more than one administrator, most likely with a phishing campaign that used malware attachments took advantage of a browser exploit.
The stolen information included names, birthdays, medical identifications, Social Security numbers, street addresses, e-mail addresses, employment information, and income data. Unfortunately, the data were not encrypted.

The Anthem Healthcare Security Breach – a Cautionary Tale

Even though the Anthem breach is thought to be the largest healthcare data breach in history, it is typical of how hackers get healthcare systems and what they steal. Hackers are ruthless in probing for even the smallest way to get in, and with healthca providers they often find the weaknesses involve employee credentials and log-in information. That makes internal security ar diligent monitoring of the system more important than ever in healthcare. To Anthem's credit, the breach was recognized and stopped when a system administrator saw that his credentials were being used to access data.

An Example of a Healthcare Data Security Weak Spot

When it comes to internal weaknesses, it's hard to beat the lowly infusion pump. Any large healthcare organization probably h hundreds or thousands of these innocuous looking devices that don't seem to offer much risk to anyone. But to a healthcare hacker, that little machine can be the golden key to your entire network.

The fact that infusion pumps seem so unrelated to network security is what makes them attractive to hackers. They know that a hospital that makes a virtual Fort Knox of its computer system may overlook infusion pumps because they just don't seem li computers. But, oh, they are very much part of the computer network.
Today's infusion pump may look about the same as it did five or ten years ago, but it has changed significantly. Back then the pumps were hardly computerized at all, but now they are standalone computers tied into your system's wireless network, transmitting data about their status and metadata on patients, and receiving updates of drug libraries and firmware. The Natio Institute of Standards and Technology (NIST) recently issued a report warning of the security risk from infusion pumps, noting some networks even allow interaction between the pump and electronic health records. Infusion pump vendors also can log in remotely to troubleshoot and collect data on the pumps, leaving the organization vulnerable to whatever security weaknesses vendor may have.

Traditional security scan techniques can adversely affect the devices, so in-house IT security may be reluctant to monitor infu pumps for cyber-attacks. Additionally, the devices may fall under the responsibility of clinical device experts rather than netwo engineers. Manufacturers are reluctant to upgrades software when weaknesses are discovered because that may be conside significant change to the device, requiring further certification and Food and Drug Administration (FDA) 510(k) clearance. The has told manufacturers that such an update would not trigger re-certification, but infusion pump manufacturers still play it safe for them, that is. Not for healthcare organizations or their patients.

But wait, you haven't heard the worst security risk posed by infusion pumps. Amazingly, most infusion pumps from the same manufacturer have the same usernames and passwords. For both maintenance and clinical use, the same credentials will grant access to any pump in the hospital or health system. This makes it impossible to revoke access codes when an employee leaves the hospital, for instance, and a hacker can only has to steal one set of credentials to access any pump in the system. Solving this problem isn't easy, however. It is technically possible to assign a separate username and password to each pump, but that would create an unreasonable burden on the staff who must access multiple pumps throughout their shifts.

Some Tips to Prevent Security Breaches and Resulting HIPAA Violations

Still, with infusion pumps and all other aspects of a hospital network, you must be careful not to trade away security for easy access. Nelson Hardiman advises its healthcare clients to take these steps in addition to any efforts at ensuring HIPAA compliance:

• When negotiating contracts, insist that manufacturers provide software and firmware updates in response to the discovery o security weaknesses or a new method of attack from hackers. Healthcare device vendors are notoriously slow in providing the same type of security updates that are routine from software companies like Microsoft.

• Conduct frequent security training with employees, not just a one-time in-service that covers HIPAA and every other aspect data security. Employees need to be reminded of the risks from seeming innocent devices like infusion pumps and how to saf use them without encumbering their daily work. They also must be updated on any security improvements or new technology use.

• Consider hiring a "white hat" hacker to try breaching your system. Some expert hackers now work as consultants who will at to break into your computer network using the same devious methods they learned on the dark side. They will seek out the vulnerabilities that they know other hackers will look for and provide a report on how to secure those weak points. This type o can be far more effective than having a consultant assess your network security in a more academic way.

Securing your organization's computer network is a big job, and it must be addressed by more than just the IT department. Th professionals may be your front line in the effort, but they require support and guidance from the C-suite and key administrato you are to sleep well at night.

For more information/questions regarding any legal matters, please email info@nelsonhardiman.com or call 310.203.2800.