Business White Paper

Anatomy of a Healthcare Data Breach

Prevention and remediation strategies

ClearDATA
SECURE • HEALTHCARE • CLOUD

Anatomy of a Healthcare Data Breach

Table of Contents

The statistics on healthcare data breaches is growing increasingly troublesome. According to the Identity Theft Resource Center, healthcare data breaches accounted for 44 percent of all breaches in 2013—the first time the healthcare sector topped this list. Perhaps the main reason for such a large proportion is because personal health information (PHI) is worth roughly 50 times more than credit card or Social Security numbers. The most profitable type of fraud stemming from identity theft is now Medicare fraud. The annual cost of health data breaches estimated at $5.6 Billion.

One in 10 Americans has been affected by a large health data breach, according to the HHS. Employee negligence is considered the biggest security risk based on the Ponemon Institute's Fourth Annual Benchmark Study on Patient Privacy and Data Security. Criminal attacks have risen 100 percent since the first study was released in 2010. What is even more surprising is that many healthcare organizations fail to detect these attacks and often remain compromised, according to a 2013 SAS-Norse study. Upgrades, enhancements, and overhauls of IT systems can open the door for data breaches if security issues aren't addressed in tandem.

Increased Risk

Personal health records have become high-value targets since they can be exploited for identity theft, fraud, and stolen prescriptions. The HIPAA Security Rule also requires business associates to appropriately safeguard electronic PHI.

Chris Bowen, chief privacy officer, ClearData, says healthcare data is potentially more susceptible than ever. "In healthcare, the shelf-life of a medical record is sometimes decades long," Bowen said. "Correcting your medical record after somebody uses it for fraudulent purposes is extraordinarily difficult for the patient – especially when you can tack on a debit card number, or fraudulent

treatment, and all kinds of serious things are on protected health information. We just don't think people understand that value."

According to a 2013 HIMSS Security Survey, internal employees inappropriately accessing patient information is an ongoing concern. Internal user monitoring technology can help alleviate this tendency. Physical safeguards remain a sticking point since many professionals prefer the portability of laptops and mobile devices. But their proliferation exacerbates the problem.

Mitigation Costs

According to a report by Meritalk, 19 percent of healthcare organizations experienced a security breach in 2013. The top causes were: malware/virus (58 percent), digital intrusion/theft (42 percent), and physical intrusion/theft (38 percent). The average cost per security breach for hospitals with over 100 beds averaged $810,189.

Depending on the nature of the breach, federal and state fines for a single disclosure of (PHI) could reach as high as $1.5 million. Other mitigation include: legal fees, credit monitoring fees, IT recovery fees, and costs associated with reputation damage.

An Industry Unprepared

Surprisingly, healthcare is still lagging behind other industries in security efforts and spending. Spending on electronic health records (EHRs) has been getting most of the attention and budget, while security and prevention often gets overlooked. In addition, changes in IT infrastructure or applications can have a trickle-down effect exposing new vulnerabilities, oversight, or mistakes. While some providers play catch-up, hackers are pouncing on the unprepared.

Healthcare organizations make particularly attractive targets because of payment data and detailed patient records used to collect reimbursements. In addition, healthcare providers typically have smaller IT budgets than private-sector companies. Although

the push to digital health records has increased health IT budgets, spending on EHRs and Meaningful Use has taken center stage. Prior to the HITECH Act, a surprising number of providers and practices were not encrypting healthcare data.

According to a Price Waterhouse Cooper survey, 74% of health providers believed their security activities were effective, but after an audit, only 22% actually met all advised security criteria. Lou Morentin, senior security risk consultant, ClearData, contends that the healthcare industry simply doesn't implement encryption safeguards as often as it should. "We're at that point now where not just mobile devices need to have drive encryption," Morentin said, "but your desktops, as well, because if somebody breaks into your clinic and steals a desktop, you've got a data breach. One of the easiest things to do is just encrypt all those drives, but yet very few people moving to get this done."

Patterns Are Emerging

To date, approximately 945 data-breach incidents have been reported where PHI was compromised. A few recent high-profile data breaches could shed additional light on how vulnerable PHI can be and what can be done to prevent breaches.

Community health systems

As recently as August 2014, Community Health Systems (CHS) suffered a criminal cyberattack affecting 4.5 million individuals, the second-largest HIPAA breach ever reported. The attacker was able to bypass security measures and implemented malware to copy and transfer data outside the company. CHS has implemented remediation efforts aimed at preventing similar attacks in the future. These efforts include implementing additional audit and surveillance technology to detect unauthorized intrusions, adopting advanced encryption technologies, and requiring users to change their access passwords. A closer look at the breach reveals that the Heartbleed bug contributed to the vulnerability of the data. Chris Bowen, CEO of ClearData, said he is surprised such a breach could occur with so much advanced warning about the bug.

"There are some attacks that are very sophisticated, very targeted, but the bulk of them are based on missing the basic checklist of things you've got to do," Bowen said.

"An active monitoring program could have helped mitigate the loss once the attackers gained access to the core infrastructure," Morentin said. "The Heartbleed bug once identified should have been patched as soon as Juniper released a patch however, many device manufacturers took some time to develop and test a patch that could be used. A System Information and Event Monitoring (SEIM) properly configured could have triggered an alert once an anomaly was detected."

Advocate Medical Group

Another recent data breach highlights the increased susceptibility of mobile devices, including laptops. In July 2013, Advocate Medical Group had four password-protected laptops stolen that contained 4.5 million medical records and patient health information, which was not encrypted. Advocate took aggressive steps to reduce the possibility of another break in, including the addition of 24/7 security personnel as well as accelerated deployment of enhanced technical safeguards. An Advocate senior vice president admitted that the data should never have been on laptops and instead should have been maintained on a secure network.

Sometimes, the simplest solution actually is the best solution. In this case, the data should have been encrypted and, as the Advocate vice president said, it should never have been on a mobile device. "Over and over these breaches could significantly be minimized by adopting an encryption policy and procedure," said Morentin. "A recent analysis of breaches showed over 60% of the breaches could have been prevented by encryption of the devices."

Morentin said practices and hospitals need to train their staff to never download PHI to mobile devices. He also suggests that policies and procedures should tie in to strong sanctions for violations.

"Cloud access to data could help to mitigate this kind of breach as well because the data is viewed through a secure browser connection (SSL) without the need to work the data on local machines," said Morentin.

Cogent healthcare

A summer 2013 data breach impacted Cogent Healthcare when a transcription partner stored provider data on an unsecure site, exposing patient data to potential identity theft. Apparently the site had its firewall down, and Google even subsequently indexed some of the patient data. More than 32,000 patients were affected. Cogent terminated its relationship with the transcription company and took possession of the hardware in use. Some of the steps providers can take to assure their business associates and partners maintain data security is to secure data through encryption and maintain the chain of custody concerning PHI.

"The business partner should have a Business Associate Agreement in place with random due diligent inspections to assure the BA is following the rule and regulations," Morentin said. "The final Onmibus Rule puts all business associates (BA's) in the same level of responsibility and safeguards as covered entities."

Morentin suggested periodic inspections of the BA's environment and auditing of their operations to ensure compliance with regulations. Again, Morentin said, policies and procedures should be tied into strong sanctions for all staff to safeguard company assets and applications to track assets and monitor their use.

"There are asset tracking applications to aid in the management of all company assets," said Morentin. "Applications like Lab Tech can help to monitor these devices."

Best Practices and Cloud Options

Industry best practices suggest an active learning approach to data breach prevention (including real-time surveillance of emerging threats) is perhaps the best way to better prioritize strategies and prevention. Near constant vigilance is becoming increasingly

important. Managed security solutions that cloud providers offer have shown tactical success against cyberthreats.

Industry groups such as The Advisory Board recommend a multipronged approach that includes audits, upgrades, and the use of cloud-services from organizations that specialize in robust security. It is also critical to prepare for a breach in advance. In other words, prevention and preparation are important. If a breach does occur, it is imperative that a crisis team be in place to move quickly and accept responsibility. A crisis team should be comprised of a multidisciplinary group including executive leadership, legal/compliance/privacy, information technology, communications and customer relations. Initial steps should be to end the compromise or remedy the risk control deficiency, restore the affected system and determine the cause of the incident and the appropriate mitigation and protection to be utilized.

Bowen was also quick to caution that just because a vendor or business associate is involved, it doesn't absolve the covered entity or provider. "It's a shared responsibility if you're hosting some data offsite, or if you are working with any type of vendor," Bowen said. "You can't just off-load data storage and management to a vendor or cloud provider. Those who think they can do so are fooling themselves."

For greater security options, it might be wise to consider a long-term cloud storage solution that is HIPAA-compliant. While recent breaches of public cloud services have cast some doubt on cloud-based storage, healthcare cloud data providers employ greater security measures for added protection. A long-term cloud computing solution could also be used as an alternative to on-site redundant archiving. In addition, a cloud-based Data Loss Prevention (DLP) solution can identify specific information that needs protecting and help make decisions on how to secure the information.

About Us

ClearDATA is the nation's fastest growing healthcare cloud computing company. More than 310,000 healthcare professionals rely on ClearDATA's HIPAA compliant cloud computing HealthDATA platform and infrastructure to store, manage, protect and share their patient data and critical applications.

For more information

1600 W. Broadway Road, Tempe AZ
(800) 804-6052
www.cleardata.com

ClearDATA
SECURE • HEALTHCARE • CLOUD