Business White Paper

Healthcare IT In The Cloud: Predicting Threats, Protecting Patient Data

ClearDATA
SECURE • HEALTHCARE • CLOUD

Healthcare IT In The Cloud: Predicting Threats, Protecting Patient Data

Table of Contents

Evolving criminal and unscrupulous internal threats to healthcare data networks continue to plant seeds of fear and uncertainty in the minds of healthcare IT professionals. Those fears are well-founded; a recent Information Week survey found that 91 percent of small healthcare practices in North America say they have suffered a data breach. Equally disturbing is the finding that 70 percent of respondents aren't confident that their budget meets risk management, compliance, and governance requirements. The Ponemon Institute's third annual Benchmark Study of Patient Privacy and Data Security found that six out of 10 healthcare organizations' security systems aren't mature enough to detect or react to data breaches.

Breach Avoidance: The Motivation For Protection

The figures don't present healthcare providers with very good odds of avoiding a breach, and breaches don't often come without significant cost. If state and federal investigations conclude that the organization has in fact violated the laws governing PHI (protected health information), the provider must deal with corrective action plans, formal resolutions, or both. Information Week reports that 80 percent of federal investigations end up generating some type of corrective action plan. These corrective action plans and formal resolutions can run well into the millions of dollars. According to the aforementioned Information Week study, the average cost is around $7 million.

What's more, data breaches are rarely isolated incidents. According to the Ponemon report cited above, 94 percent of respondents had at least one data breach in the last two years, and nearly half of the respondents have experienced more than five data breaches. It's healthcare's own epidemic to cure.

Where Are The Threats, How Are They Mitigated?

To know where healthcare IT security is going - and what it needs to protect in 2016 and beyond - it's instructive to take a look at where we've been. In general, compromised credentials remain the leading source of intrusion across industries, according to Verizon's 2015 Data Breach Investigations Report. While the volume of spyware/keylogger attacks are dwindling, phishing and RAM scraping incidents are expanding at a rapid pace. Specific to healthcare, the top three sources of unauthorized data access are:

- **Miscellaneous errors.** Within healthcare, the largest source of unauthorized data disclosure - accounting for 32 percent of incidents - is attributed to "miscellaneous errors." Chief among them are misdelivery of information, capacity shortages, and publishing errors committed by administrative personnel.

  While these mistakes are often innocuous and hard to control, there are protocols for dealing with them. Providers should have a VERIS (Vocabulary for Event Recording and Incident Sharing) system in place for the recording of incidents that could expose them to risk. It's important to track how often human error creates data risk exposure and create controls and management processes aimed at avoiding such errors. That tracking should be granular enough to identify root causes of systemic issues, such as training, poor process control, or the unintended consequences of automation.

- **Insider misuse.** Insider misuse caused 26 percent of the healthcare industry's 2014 data breach incidents, placing it firmly in the top three industries affected by individuals abusing the access with which they have been entrusted. This is a difficult issue to address, as it requires a combination of process and access control, and its detection is usually reactive.

  Providers should identify core areas of protection and specific activities to track, then deploy password protection and identity verification, fraud detection capabilities, and auditing activities at a regular cadence. Standard practice should involve forensic examination of suspect user devices and server access, especially upon the departure of employees, which will help inform best practices for avoidance of the insider misuse threat.

- **Physical theft and loss.** The good news is that the healthcare industry is proving progress on what the report identified at its biggest weakness in 2014, when a whopping 46 percent of data loss was attributed to physical theft and loss. This year, that figure stands at 16 percent. Most of this theft occurred within the victim's work area (55 percent of incidents), and employee-owned vehicles (22 percent of incidents).

  To minimize the risk of physical device theft and loss in healthcare, security leaders should work with their procurement departments to log device access and usage, and track the volume and type of devices lost. With these metrics in hand, data security professionals can effectively analyze the threat presented by the theft of a specific device and take corrective action. When devices are lost or stolen, time to reporting is of the essence to safeguarding data. Policy should dictate immediate reporting of missing provider property. Further, security providers should employ full-disk encryption, password protection, USB port lockdown, and remote wiping to as countermeasures to lost or stolen property.

As a matter of best practice, we've compiled a list of important steps toward ensuring the security of data in healthcare, steps that are critical regardless of whether providers are handling data on-premise, in the cloud, or both.

- Limit employees' Internet activity to job-specific tasks, and train thoroughly on safe use of Internet resources.
- Keep anti-virus software up-to-date on all end user devices and servers handling business data, whether company or employee-owned.
- Perform frequent and granular vulnerability assessments of applications, networks, data centers, devices, access points, and third-party/supplier/partner integration points.
- Mandate strong authentication protocols for every end user, including two-factor authentication via a combination of passwords, tokens, or PINs.

- Employ firewalls at every point of data access.
- Encrypt and certify every piece of sensitive information, especially that on mobile devices. According to the Ponemon Institute, more than 43 percent of employees admit to having lost a portable device.

Data Security In The Cloud

These baseline risks and the guidance offered to avoid them are inherent in any healthcare IT infrastructure, whether or not that infrastructure involves cloud services. As it relates specifically to the recent adoption of cloud services for healthcare data storage and retrieval, we've witnessed and acknowledged a fair amount of skepticism of cloud security. We've also ascertained that this skepticism is unfounded.

Mark Kadrich, Chief Information Security and Privacy Officer at San Diego Health Connect and author of Endpoint Security, puts it plainly. "I can think of ten really significant breaches within last six months, and none of them had anything to do with the cloud," he says. "As is the case with on-premise server, device, and network security, cloud security is dependent on who's implementing it." Kadrich says the mechanics of data security are the same regardless of the storage and retrieval medium; demonstrable software insurance and protocols including key management and encryption are critical in any sensitive data storage and retrieval infrastructure. "When these tools are wielded by individuals who are specialized in their knowledge and focused on it, the tendency is to be more secure," says Kadrich. "If the OS has holes and the apps have holes and the network has holes, the notion that they will be more secure when the data is held on premise is false." In fact, asserts Kadrich, many cloud data solution providers are more security-centric than their on-premise counterparts, as the leading among them have invested heavily in security specialists assigned to deal with end users' security concerns.

Future-Proofing For HIT Security

Preparing for future data security threats begins with awareness. The aforementioned Verizon report found that 99.9% of the known vulnerabilities exploited by hackers in 2014 had been compromised more than a year after the associated CVE (common vulnerabilities and exposures) was published. In other words, the weakness was known, but left unaddressed. As we look to the future, it becomes clear that unaddressed known threats are more a management and policy issue than they are a technology issue. That's why so many providers are hiring chief security officers, or outsourcing the role to their network and IT partners. Only when a designated point entity is tasked with addressing and obviating for known vulnerabilities can a concerted effort be made to deploy and maintain the patches, updates, and policies that protect healthcare data - whether that data resides on premise or in the cloud.

**For more information, call (800) 804-6052
or visit www.ClearDATA.com**

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