A Holistic Strategy for Preventing Internal Breaches in Patient Data Security

WHITE PAPER

caradigm

Privacy breaches have been escalating in the healthcare industry at an alarming rate. Last year alone, more than seven million patient health records were breached. Industry experts estimate the annual cost of those breaches to be over $5.6 billion.[1]

In order to protect patient privacy, hospitals have been focusing their efforts on external intrusion detection and hard drive encryption. But in doing so, they have been overlooking a far more insidious and growing problem: internal breaches by their own staff and extended care partners.

With the healthcare landscape shifting to integrated care and population health, hospitals are particularly vulnerable to internal breaches. In addition to a fluid workforce of new clinicians, interns and residents flowing in and out of the organization and roving from one workstation to another throughout the day, hospitals now need to share data outside their four walls in alliance with other providers and physician groups coordinating care as patients transition from hospital to clinic to home. The problem is compounded further by the accelerated consolidation of hospital entities through mergers and acquisitions. This confluence of factors is causing an exponential rise in the risk of unauthorized access and inappropriate use of confidential patient data.

To prevent compromising patient privacy and security, hospitals need to be looking at tools that can help them better identify and credential this widespread community of users and tightly control their access to an exploding volume of medical information. The balance is by necessity a delicate one. On the one hand, hospitals need to establish strong protocols to protect patient records and clinical applications from unauthorized use. On the other hand, caregivers need quick and easy access to their patients' records and clinical applications to expedite quality care. This puts hospitals under enormous pressure to institute simple, yet secure log-on procedures that enable efficient navigation between clinical applications and patient data.

This white paper presents hospitals with ways they can balance the need for extended care teams to have rapid access to complete patient data with the need to safeguard patients' privacy. This holistic strategy encompasses deploying IT tools to credential users and control their access to data, instituting best practices and elevating security initiatives to executive-level status in the organization to help foster a culture of security-conscience users.

UNDERSTANDING THE MAGNITUDE OF THE PROBLEM

While professional cyber criminals might be grabbing all the headlines, the dangers presented by internal threats are starting to raise serious concerns among hospitals and clinics. In a 2014 security report by KLAS Research[2], survey respondents listed unauthorized access and identity management as their number one concern. One provider was quoted as saying, "Many people think that people on the outside hack into the system, but that is not the case. People who are already on the inside and already have the appropriate access are given $1,000 by outside people to get 100 Social Security numbers."

Whether stolen or accidentally disclosed, it's evident that health data is valuable and makes a lucrative target. No wonder that almost 20 years after HIPAA was first enacted, the risk to patient privacy and security continues to escalate.

In a 2014 survey conducted by the Ponemon Institute, 90% of the surveyed providers admitted to having had at least one data breach in the past two years. That same survey also revealed a 137.7% increase in the number of patient records breached from 2012 to 2013.

While the root of those data breaches ran the gamut from external hacking to theft of laptops and phones, the U.S. Department of Health and Human Services noted that the second leading cause of HIPAA breaches reported in 2013 was due to unauthorized access and disclosure.

It's clear that the problem is pervasive and only going to get worse as the volume of patient data and the number of system and applications continue to grow and the boundaries between healthcare provider teams become more porous. This places a sense of urgency on hospitals to re-examine the way they share patient information and reframe their approach to data security to include ways to deliver faster access to the right data at the right time to the right people, with the ultimate goal being to improve care quality and outcomes.

RECOGNIZING THE CLINICAL AND FINANCIAL RISK

Failure to address the problem can be costly. For instance, in September 2012, FierceHealthIT reported that the Office of Civil Rights (OCR) levied $2 million in HIPAA fines for stolen laptops. In April 2014, the same publication reported that a Boston teaching hospital was fined $1.5 million for an electronic data breach of patient healthcare information. In July 2013, the OCR fined Wellpoint $1.73 million for neglecting to implement user verification technology that would have prevented over half a million individual patient files from being illegally accessed over the Internet.

Depending on the nature of the breach, federal and state fines for a single disclosure of personal information could reach as high as $1.5 million. Data security breaches can cost a hospital in other ways. Legal fees, credit monitoring services for patients whose data was compromised, IT recovery and other associated costs can be several times that of the initial fine. Violations of data privacy and security laws can lead to increased regulatory oversight as well. There is also the damage to a hospital's reputation and brand image which can create long-term financial consequences for the institution. Ponemon Institute interviewed more than 850 senior-level executives who estimate that the damage to a hospital's brand due to a security breach could run as much as $330 million, depending on the size of the institution.

Then, of course, there's the cost to the individual patient. The value of something like a Social Security number has an unlimited shelf life. Any patient experiencing a breach of their medical records could be at risk indefinitely.

Clearly the stakes are high. The problem is widespread. Complacency is no longer an option.

GETTING A REALITY CHECK ON PREPAREDNESS

Many healthcare organizations think that the systems they already have in place are doing an effective job in protection against security breaches, but closer examination often tells a different story. In a survey conducted by PricewaterhouseCoopers (PwC)[3], 74% of the healthcare provider respondents believed their security activities were effective. After an audit, however, PwC found that security strategies had not kept pace with the growing sophistication of information privacy and security risks.

According to PwC, only 20 percent of hospitals with 200 beds or more have a full provisioning system to manage user identity and control data access. Yet, 56% of healthcare providers consider themselves frontrunners in security. PwC assessed the number of true leaders to be around 22%.

Where does your organization lie on the preparedness spectrum? To determine that, you need to look at the data control factors that might be compromising compliance and therefore increasing your privacy and security risk. According to a 2014 Ponemon Institute benchmark study[4], employee negligence was a top security concern, while 40% of the surveyed providers also cited the insecurity of mobile devices as a primary security worry.

For instance, in reviewing security protocols you may find that the rise in unsecured mobile devices allowed access to patient records is increasing the opportunity for data breaches. What is the policy on allowing clinicians to connect their own devices to the hospital network? Do you permit access from remote and mobile devices? If so, can you track and audit which patient records and clinical applications are being accessed remotely and by whom?

Risk assessment needs to be an ongoing process. Are the hospital's privacy and security initiatives reviewed regularly to ensure that they comply with current data security laws and company policies about who should be granted access to what specific data? In light of the most recent HIPAA Omnibus Rules, you could be subject to a random compliance audit by the Office of Civil Rights even if you haven't had a history of privacy breaches. Perhaps more importantly, are your privacy and security policies evolving as fast as your risks of privacy breaches are growing? Regulatory requirements consistently lag years behind technology advances that might leave your systems vulnerable to inadvertent data disclosures. So it is imperative that the hospital keeps up to date on the latest trends and adjust their data security protocols accordingly.

TAKING STEPS TO CLOSE THE SECURITY GAPS

To foil both internal and external threats, data security measures need to be front and center in any hospital activity involving access to patient information, including sharing of data with external providers and partners. To that end, there are a number of steps hospitals can take to weave security policies and practices into the fabric of the organization.

- **Hire a Chief Information Security Officer (CISO)**. Visibility connotes importance. Elevating security to an executive level position establishes the mindset that data security is a priority rather than an afterthought. It also ensures that data security plays an integral role in shaping strategic operations going forward.

  What are some criteria to look for in a CISO? Today's CISO needs to be both tactical and strategic – understand changing technology but be business-driven in their approach to data security. They should focus on both data security and IT risk, work in partnership with the hospital's CIO and be a good communicator in order to build relationships and gain influence in the boardroom. A CISO needs to be metrics-minded and business savvy to objectively weigh the range of risk factors and costs associated with various business decisions against the possible rewards. They need people skills and the passion to transform the corporate culture into one that strives for security excellence. They also need the financial acumen to calculate a reasonable budget and the creativity to stretch those funds as far as possible to protect critical business initiatives.

- **Implement best practices in data security.** No matter how strong a hospital's privacy and security policies and controls are, you never really know how adequate those defenses are unless you continually verify that they are sound, uncompromised and applied consistently across the organization. While there are many best practices worth employing, PricewaterhouseCoopers cites three critical lines of defense to combat attacks on your data: assign ownership at the management level for assessing, controlling and mitigating risks; establish a working group to implement risk management practices and help risk owners report risk-related information up and down the organization chain; and create an internal audit team to provide objective assurance to the board and executive management on how effectively the hospital is assessing, validating and managing privacy and data security risks. Without this internal audit component, the hospital runs the risk of its security and privacy practices becoming inadequate or even obsolete.

SUGGESTED READING

There are also a number of industry publications offering insights on data security:

Fortifying your defenses: The role of internal audit in assuring data security and privacy, *PricewaterhouseCoopers*

Health Information Privacy and Security: a 10 Step Plan, *HealthIT.gov*

HIPAA Audits: a 5 Step Survival Guide for Healthcare Providers, *HIT Consultant*

- **Institute tighter provisioning.** While the CIO focuses on hardening systems with advanced encryption and intrusion detection technology, the CISO should be focusing on strategies that can facilitate the sharing of critical data among care providers without introducing new vulnerabilities to the system. One component of that strategy should be deployment of an identity management solution that can assist the hospital in protecting patient health information from unauthorized access. These role-based provisioning software programs are used to automatically create, modify or terminate an individual's access to clinical and business applications throughout the lifecycle of a user's identity within the organization. Be sure to select programs that are uniquely designed for the healthcare industry where users may or may not be direct employees of the hospital yet require access to clinical applications or patient data – such as medical students, community physicians and agency nurses. In addition, you should choose a solution that easily facilitates zero-day provisioning so that users have immediate access to the information and applications they need from their very first day on the case.

  Provisioning software not only enforces corporate role policies through certification and remediation workflows. In the world of integrated care and population health, where the borders between healthcare providers' systems need to be porous, identity and access management become the new security perimeter. Their presence limits the hospital's exposure to privacy breaches by ensuring each user is properly credentialed to access only those systems and data stores for which they're authorized.

- **Integrate single sign-on (SSO) and context management technology.** In a fast-paced hospital environment shared workstations provide a fertile ground for compromising the privacy of patient medical records. Deploying software tools that integrate SSO with context management can help minimize the exposure time while helping clinicians quickly access pertinent patient data as they travel throughout the halls of the hospital. To ensure transparency for HIPAA compliance, be sure to choose an SSO solution with context management capabilities that automatically produces audit logs that identify who has looked at which patients, in which applications, when and where.

  SSO and context management software can help protect patient privacy and system security by one-tap logon/offs, and also include configurable timeout rules that quickly close out records and applications. The best SSO applications are designed to integrate with strong authentication technologies like smartcards and biometrics to further enhance data security. Context management adds another level of security by linking role-based access with patient-centric navigation. This helps the hospital reduce the risk of medical error by automatically tuning different applications to the same patient using the medical record number. With the tap of a badge the clinician can unlock a workstation, automatically launch their personal settings, view an authorized set of applications and primary electronic health records, sign orders and then lock the device. As they move from one workstation to another throughout the day, the authorized applications, settings and records will follow suit. It's the perfect marriage of security and workflow efficiency.

ABOUT CARADIGM

Caradigm is a healthcare analytics and population health company dedicated to helping organizations improve patient care, reduce costs and manage risk through the strategic, timely and compliant use of data generated across the healthcare continuum.

REAPING THE BENEFITS OF TIGHTER DATA SECURITY

It's clear that being non-compliant with data privacy and security laws can be expensive, not only in financial terms but in the loss of public goodwill as well. On the flip side of the coin, implementing strong data security measures like identity and access management, SSO and context management can do more for the hospital than simply deter hackers and snooping employees from capitalizing on privileged information. They address the complexity of today's integrated care and population health programs by providing the foundation for efficiently sharing critical medical data among a patient's network of health providers to ensure quality care while minimizing clinical and financial risk.

Adopting a holistic strategy for preventing data breaches—one that raises security to an executive-level initiative, adopts industry best practices, deploys hospital-centric provisioning, SSO and context management tools—can transform a good hospital into a model of excellence for the healthcare industry.

[1] 2014 Ponemon Institute "Fourth Annual Benchmark Study on Patient Privacy & Data Security"

[2] "Security and Privacy Perception 2014: High Stakes, Big Challenges," KLAS Research

[3] PricewaterhouseCoopers "2014 Global State of Information Security Survey"

[4] 2014 Ponemon Institute "Fourth Annual Benchmark Study on Patient Privacy & Data Security"

caradigm

www.caradigm.com
+1-425-201-2500
500 108th Ave NE, Suite 300
Bellevue, WA 98004