iatricSystems™

Three Simple Steps to Protect Patient Privacy

How Policies, Procedures, and Technology Ensure Patient Privacy Monitoring Compliance

Executive Overview

Healthcare institutions are at greater risk of falling short on patient privacy requirements than ever before. The movement to a complete electronic health record and constant changes to patient privacy regulations make compliance increasingly difficult. Since the HIPAA Privacy statue was first enacted in 1996, major regulations regarding patient privacy have followed — HITECH, ARRA Meaningful Use, and the Omnibus Rule.

Hospitals face severe penalties for patient privacy breaches, including financial, criminal, and harm to reputation. Complicating the matter are tighter regulations with the recent Omnibus Rule, increased audits from OCR, and the daily headlines that not all organizations entrusted with PHI protection are upholding their responsibility.

Hospitals need to move beyond random manual audits that review a very small percentage of the access events that occur every day in a healthcare setting — especially when the stakes are so high.

This paper introduces a simple three-step methodology — policy, procedures, and technology — to build a solid foundation to ensure patient privacy throughout your organization.

It examines:

- Challenges, current practices, and their consequences
- Three-step methodology for a successful patient privacy monitoring program
- Protecting PHI technology checklist

CIOs' Top Challenges Regarding Securing Patient Privacy Data

Healthcare today is the most regulated industry in America. It's also the biggest target for fraud and the theft of personal information, threats that continue to grow. The Ponemon Institute's Third Annual National Study on Medical Identity Theft estimated an average of 2 million Americans are victims of medical identity theft yearly, with an **estimated total cost to U.S. healthcare organizations of $41 billion.** As a result, we are likely to see more regulations as lawmakers and healthcare consumers wrestle with how to stem the leakage. These new regulations place a greater burden on IT organizations in an industry that is already stretched thin.

...an average of 2 million Americans are victims of medical identity theft yearly, with an estimated total cost to U.S. healthcare organizations of $41 billion.

HIPAA provides the underpinning for other privacy requirements like the Omnibus Rule and Meaningful Use:

- The new Omnibus Rule specifies that organizations are now presumed guilty for a breach until they prove their innocence with a 4-step risk assessment.
- Meaningful Use requires a risk analysis in accordance with HIPAA 45 CFR 164.308(a)(1), identified as the Security Management Process.

The new Omnibus Rule regulations around breach notification make it clear that hospitals have to provide more accurate and timely monitoring of access to patient records. With the cost of non-compliance and breaches rising sharply, privacy has become a business imperative.

To comply with the strict regulations and avoid steep penalties, healthcare organizations are faced with three key challenges to protect patient data:

Challenge 1: Log every access to patient data

HIPAA forces healthcare providers to log every access to patient data. However, electronic health records, advancements in data integration, and networking now generate massive amounts of data which is shared across many local and remote locations. This greatly increases the number of data access points and the challenge of protecting patient privacy. Patient privacy requirements span many systems that already exist as well as systems yet to be developed such as patient and physician portals and HIEs. Bringing these new systems live can come to a halt until IT has a solid patient privacy foundation in place.

Challenge 2: Audit massive volumes of access records

The second challenge relates to the sheer volume of data that needs to be audited. Imagine that a hospital wants to identify inappropriate access to patient data at their facility. On a daily basis, a 100-bed facility has an average of 52,000 patient access records. Manually

monitoring and reviewing these accesses every day to find which ones are inappropriate is clearly unfeasible.

Challenge 3: Correlating diverse data into one database

The third challenge is correlating the data from all the logs across all the disparate systems into one consolidated database. When a hospital can see all the accesses across all systems at one time, it can detect patterns and trends, and the magnitude of any privacy violations.

Current Practices and Their Consequences

The April 2012 HIMSS Analytics Report: Security of Patient Data, commissioned by Kroll Advisory Solutions, reveals that many hospitals today are not focused on patient privacy. The survey shows that healthcare organizations have not been allocating the appropriate resources or specific focus required to ensure all patient health information remains protected and secure. Here are some of the numbers from the report:

- 47% spend less than 3% of IT budget on information security
- 66% have an internal breach and disclosure auditing plan in place
- 11% reported a known case of medical identity theft
- 91% review audit logs and 84% of those manually review

So why have healthcare organizations not fully implemented preventive measures for a data breach? Why are healthcare organizations preforming random audits, and not taking advantage of creating better policies, processes, and seeking technology to reduce the cost of the manual effort?

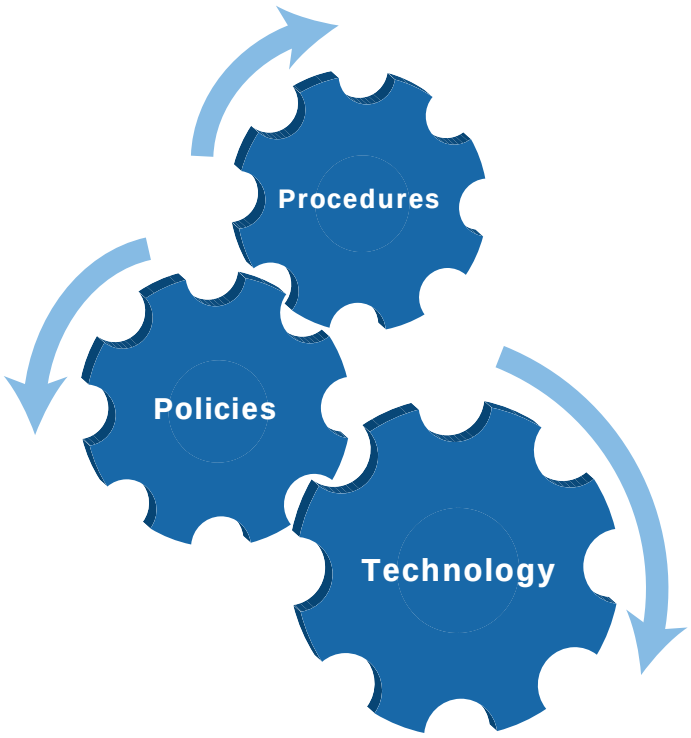
The problem stems from a lack of understanding about privacy violations and the potential consequences. If healthcare leaders really understood how much PHI access is going on in their facilities, understood the privacy expectation of their patients, and fully understood the ramifications, they would reallocate their resources. In addition, healthcare organizations don't have appropriate staff in place to maintain the privacy program. In many cases, patient privacy is the second or third job for employees, who do not understand their responsibilities and requirements that are based on state and federal guidelines.

This lack of preparedness can have severe consequences. The HITECH mandate and the new Omnibus Rule require hospitals to notify patients within 60 days if their PHI has been accessed inappropriately. Some states have even tighter reporting requirements. Penalties for an organization that fails to comply can add up to $1.5 million per year. The rules apply whether the breach is a careless mistake, active snooping, theft for profit, or identify theft. Ignorance of the law or of the breach is no longer a defensible position. In fact, it may be identified as "willful neglect" and if so, carry with it the most severe civil, and possibly criminal penalties.

The early results of the first random audits confirm that user activity monitoring is the number one deficiency. In the first round of audits, which included 20 healthcare organizations of various sizes and types, there were 46 deficiencies noted in user activity monitoring. Literally every organization audited had at least one deficiency noted in this area. Very few organizations were found to be using technology effectively to address this standard, and few were auditing all of their systems with PHI. The risks are huge.

Three-Step Methodology for a Solid Foundation

There are three elements of any patient privacy compliance program that reduce the risk of a data breach and provide a solid foundation for securing patient privacy — **Policies, Procedures, and Technology**.



Policies

Policies reflect the principles that are accepted by your healthcare organization regarding patient privacy, and establish a culture and expectation for all stakeholders. Typically, a privacy policy is formed by a committee that includes the compliance officer, patient privacy officer, security officer, CIO, CFO, and Human Resources. There are some models that can be used to help create the policy, such as the HITRUST Common Security Framework.

Procedures

The next part of the process is to develop, document, implement, and communicate procedures to enforce the conditions set forth in the privacy policy. Organizations that don't establish diligent procedures for monitoring what users are doing are setting themselves up for failure and embarrassment.

Technology is now available that can automate patient privacy monitoring, allowing hospitals to move beyond the limitations of manual and random audits.

Surprisingly, the real threat is internal. One reason is because our healthcare practice model encourages open access, to all caregivers, to all patient information. This makes sense for the people who work in the emergency department. We surely do not want to limit their access to patient records, especially when it can help with patient care. So, in essence, we are allowing healthcare personnel to access everything that is appropriate but not look at everything. This is what complicates the enforcement of patient privacy procedures — we need to allow caregivers entree to all information, and then check the audit logs to ensure that they accessed the right information.

Technology

Procedures must be augmented by technology to perform tasks that cannot be addressed manually.

Technology is now available that can automate patient privacy monitoring, allowing hospitals to move beyond the limitations of manual and random audits.

Technology such as iatricSystems Security Audit Manager™ can transform privacy protection into a proactive, 100%, near real-time review of all user interaction with patient information. For hospitals, it means comprehensive and immediate breach detection and notification.

Once automation is implemented via technology, healthcare organizations can then investigate and track a breach, report on any unauthorized access to the patient's medical records, and put practices in place so the breach doesn't happen again. An automated solution that can integrate and correlate access to PHI that is located in multiple healthcare systems is the easiest and most effective way to streamline these processes and procedures to ensure compliance. With the Omnibus Rule and OCR HIPAA audits it is even more critical to have practices in place to not only prove that a hospital is monitoring access to patient records, but that it can do something about it when a breach is detected.

Hospitals that are using enterprise HIS such as MEDITECH and Epic still require technology to automate the process. Most hospitals have multiple facilities, additional best-of-breed applications, as well as information about employees stored in Human Resource Systems. Information Systems can run simple reports that can assist with conducting random audits, but your hospital is still exposed due to not seeing all the accesses across all systems at one time, to detect patterns and trends.

Protecting PHI Technology Checklist

When you are evaluating technology for a successful patient privacy monitoring program, use this checklist to make sure the system you select offers these critical capabilities.

Top investments for 2013 include an audit log or log management, a data loss prevention system, and a mobile device management system.

Healthcare Organizations Are Taking Action

The Information Security Media Group recently published a handbook entitled *Healthcare Information Security Today, 2013 Outlook: Update on Safeguarding Patient Information*. The report shows that the top priorities include improving regulatory compliance, boosting security education, and preventing and detecting breaches. Top investments for 2013 include an audit log or log management, a data loss prevention system, and a mobile device management system.

Technology Requirements to Protect PHI
1. Provides central monitoring of all accesses to patient records. This process saves time by using a system that automatically aggregates audit logs from across the entire organization and provides single search queries and proactive auditing.
2. Catches and resolves single and recurring breaches in real time. It is important to proactively audit all accesses to patient records and spot inappropriate activity as it happens. This type of monitoring reduces violations, helps prevent recurring breaches, and allows you to document and share audit findings with your security team for quick resolution.
3. Documents breach investigations and their resolution. A centralized and automated system provides the information required to document all investigations and their resolutions to fulfill notification requirements.
4. Provides reporting per state and federal guidelines. Hospitals are required to report breaches. They need to create a comprehensive, centralized environment to review documented findings and provide insight into areas requiring additional security measures and/or employee education.
5. Documents the release of medical records. With so many ways that a HIPAA violation can occur when releasing medical records, it is important to develop a plan to document and track their release.
6. Accounts for all disclosures. The HITECH rule requires all hospitals and business associates to account for all electronic disclosures of PHI. In addition, the accounting must produce disclosures made for three years prior to the date of the request. The accounting requirement only applies to disclosures (that is, releases of PHI outside the covered entity) and not to uses (which are understood to be within the covered entity). This process should be tracked and documented in a central repository.
7. Meets Meaningful Use patient privacy requirements. Under the HIPAA Security Rule, hospitals are required to implement policies and procedures to prevent, detect, contain, and correct security violations under HIPAA 45 CFR 164.308(a)(1).

As the security update reveals, healthcare organizations are now investing in technology to improve their regulatory compliance. Perhaps the catalyst was the Omnibus Rule, and the deadline that looms in September of 2013? Or it could be the threat of OCR Audits?

Regardless of the catalyst, for those organizations willing to create privacy policies and procedures, and invest in the right patient privacy monitoring technologies, there is light at the end of the tunnel.

How three hospitals saved time and money protecting patient data

If your hospital is like most, your patient data is accessed hundreds, if not thousands, of times every day. With the ever-increasing patient privacy breach regulations, monitoring this access can no longer be done manually.

We invite you to read how three hospitals — each with a different healthcare information system — are automating their monitoring to catch all inappropriate access to patient data:

- A hospital with Siemens, McKesson, and Picis enhances protection of patient data
- An Epic hospital simplifies the auditing process and makes it proactive

Read these case studies and learn why automating access to patient data is now a must at your hospital and how easily it can be accomplished.

Protect Patient Privacy and Your Hospital with Three Simple Steps

Protected Health Information (PHI) is not just data — it's the personal history of an individual, and represents a bond of trust between the patient and the hospital entrusted with their data. A hospital's ability to maintain that trust is vital to its image, reputation, financial success, and longevity. It is not only the 'hard' costs associated with a breach that you need to consider, but also the cost when intangible assets are compromised.

Healthcare organizations can head off the consequences of a data breach by investing in a solid foundation and methodology for their privacy and security programs. Start by defining effective privacy policies, create procedures to enact the policies, and add technology that automates the procedures and makes their enforcement possible. A solution that enables you to protect the personal data of your patients and stay in compliance with strict regulatory requirements is now within reach.

About iatricSystems

iatricSystems is a healthcare technology company dedicated to helping healthcare organizations enhance their IT investments. We do so with our diverse healthcare experience, an extensive partner network, and our proven capabilities in patient privacy, analytics, EHR optimization, and interoperability. For more than 25 years, iatricSystems has delivered solutions to more than 1,300 healthcare organizations. For more information, contact info@iatric.com or visit http://www.iatric.com/securityauditmanager. Connect with iatricSystems on Twitter, Facebook, and LinkedIn.

Ph: 978-805-4100 Fax: 978-805-4101 info@iatric.com iatric.com