Trust: The Real Reason for a Patient Privacy Program

Protect your hospital's reputation and reduce privacy breaches

By James Lawson

Implementing a successful patient privacy program requires a significant commitment. Hospitals face severe penalties for breaches, including financial, criminal and reputational. Hospitals can maintain compliance by implementing a comprehensive privacy program along with best practices for breach incident tracking. Learn how to proactively review the thousands of patient records accessed daily, and to detect inappropriate behavior resulting from human error, prying, financial gain, identity theft and more.

James Lawson is the Senior VP of Software Solutions at Iatric Systems. His responsibilities include management of the programming, implementation and support of Security Audit Manager. He has over 15 years-experience in the healthcare industry and is an integration expert, working to bridge the gap between hospitals and security requirements. You may reach him at (978) 805-3169 or James.Lawson@iatric.com.

Healthcare institutions are at a greater risk of falling short on patient privacy compliance than ever before.

Now HIPAA regulations require organizations to map where their Protected Health Information (PHI) is located. As such, the requirements and enforcement under HITECH and HITECH Omnibus regulations are becoming more specific. These regulations also place increased emphasis on the definition and notification of a breach occurrence. Hospitals and business associates now have the added burden of proof to demonstrate that there is a low probability that PHI has been compromised.

Hospitals need to do better

HIPAA, Meaningful Use, HITECH Omnibus, and a growing number of medical identity theft cases have put patient privacy in the spotlight. In addition, with the HITECH Omnibus ruling, there is now a growing likelihood that healthcare organizations with their business associates will face security and privacy scrutiny under the audit program launched by the Office of Civil Rights (OCR).

Leon Rodriguez, director of the HHS Office for OCR, notes that some of the largest breaches reported to the agency have involved business associates:

"This final Omnibus Rule marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented," he said. "These changes not only greatly enhance a patient's privacy rights and protections, but also strengthen the ability of my office to vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a healthcare provider, or one of their business associates."

Early results of the random OCR audits confirm that effective monitoring for patient privacy violations is a major weakness for most healthcare organizations. Audits of 20 various sizes and types of organizations revealed 46 deficiencies in user

activity monitoring. Each organization audited had at least one deficiency.

A similar trend has been seen in audits that are more recent. Very few of the organizations were using technology effectively to address this standard, and only a few were auditing all systems that contained electronic PHI (ePHI).

With these pressures, why do most healthcare organizations still monitor access to patient information randomly, and not take advantage of technology to assess risks and automate the process?

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 healthcare organizations have not been allocating the appropriate resources required to ensure all PHI remains protected and secure. Here are some of the numbers from the report:

- One in three have reported a known case of medical identity theft
- 60% spend less than 3% of the IT budget on information security
- 10% have an internal breach and disclosure auditing plan in place
- 94% review audit logs and 75% of those review manually

The true cost of noncompliance

Most healthcare organizations have firsthand knowledge that the majority of breaches are perpetrated or enabled by insiders. However, due to the sheer volume of data that needs to be audited, organizations can only review a small percentage of patient records. This results in an enormous risk that inappropriate behavior that could cause a severe breach will go undetected.

According to Meditech, a typical 100-bed facility generates 52,000 patient access records daily. Furthermore, information about PHI access does not reside in one place. Trying to find inappropriate activity manually throughout a healthcare organization is a huge task.

Why do most healthcare organizations still monitor access to patient information randomly, and not take advantage of technology?

All this contributes to the healthcare industry suffering from the highest number of fraud cases in the U.S. Most healthcare organizations are neither efficient nor effective, leaving themselves open to a tremendous amount of risk. The most notable risk can be damage to the hospital's reputation and loss of trust from the community and patients they serve.

Today, violations in protecting health information are more newsworthy than ever. For the unfortunate hospital that has not instituted a comprehensive patient privacy program, inappropriate behavior and privacy breaches will inevitably occur.

Breaches of unsecured PHI involving 500 or more individuals must be reported by notifying the U.S. Department of Health & Human Services, as required by section 13402(e)(4) of the HITECH Act. Financial penalties may be assessed and hospitals will be listed on the OCR's infamous Wall of Shame.

The new reality

Penalties imposed on hospitals and business associates for failure to comply with HIPAA/HITECH can be as much as $1.5 million per violation depending on the level of negligence.

The rules apply whether the breach is a careless mistake, active snooping, theft or identify theft.

Ignorance of the law or of the breach is no longer a defensible position. OCR is required to investigate every complaint of a HIPAA violation to determine if the violation is due to willful neglect; and to impose a civil monetary penalty for any HIPAA violations determined to be due to willful neglect.

The new Omnibus Rule, which became effective on March 26, 2013, has clarified the reporting and definition of breach. It replaces the previous version of the HIPAA Breach Notification Rule.

OCR is required to investigate every complaint of a HIPAA violation. Penalties can be as much as $1.5 million per violation.

The new rule states that an acquisition, access, use or disclosure of PHI that is not permitted under the Privacy Rule is presumed to be a breach unless a covered entity or business associate can demonstrate a low probability that the PHI has been compromised based on a four-factor risk assessment. Covered entities and business associates must comply by September 23, 2013.

Under this expanded view, there is no time to waste for companies to determine whether they are a business associate. With this ruling, business associates can be:

- A Health Information Organization, E-prescribing Gateway, or other person that provides PHI-related data transmission services to a covered entity and requires routine access to such PHI
- A person who offers a personal health record to one or more individuals on behalf of a covered entity

Expectations of the Office of Civil Rights

The Omnibus Rule, recent audit results, and the OCR Audit Protocol have all contributed to the growing list of the OCR expectations. They include:

1. All systems with PHI should be logging (collecting audit logs).
2. The audit process and audit logs should be protected from tampering.
3. A documented audit plan and written policies should exist to comply with the HIPAA Security Rule.
4. Workflow templates for tasks that involve patient data should be created to prevent a breach from occurring (e.g., transporting devices, replacing hard drives, updating computers, proactively monitoring all PHI, etc.).
5. The audit approach should be broad enough to cover all users.
6. The audit process should be enabled through automation.
7. Organizations, particularly large entities, should have procedures and processes for following up and resolving the identified issues.
8. Training is necessary—include the entire workforce and business associates.

These are not trivial expectations. To meet them, healthcare organizations need to re-evaluate their current approach. Conducting a yearly risk assessment is crucial, but this alone is not going to meet OCR's expectations.

Healthcare organizations need to implement a culture change—review, implement and/or update policies and procedures, including business associate agreements. Most importantly, they need to continue to educate their staff. Changes in legislation can affect them personally. How many employees in your organization truly understand how the choices they make can affect them personally and financially?

Protect your reputation and reduce privacy breaches

To reduce breaches, all patient access data must be correlated across disparate systems into one consolidated database. Seeing a single event of inappropriate access in one system is just a clue in a mystery, but when an organization can see all activity, the true picture of the behavior can quickly be revealed.

Capturing access to PHI centrally allows automated processes to look for inappropriate behavior. Privacy officers can then investigate, document, and report on any unauthorized access to medical records and put practices in place to prevent repeat behavior.

Consider medical identify theft, for example. An automated monitoring process can alert the privacy officer if there are changes to patient data collected in admissions compared to a previous visit (gender changes, significant height/weight changes or blood type changes). Catching the

problem as it is happening, versus months or years later, can make a big impact on reducing privacy breaches.

The most notable risk can be damage to the hospital's reputation and loss of trust from the community and patients they serve.

Continually monitoring access to PHI and being proactive in terms of finding inappropriate behavior will satisfy the HIPAA term "reasonable effort."

A successful patient privacy program includes the following attributes:

1. *Centralized monitoring* – Employee and business associate access to patient records is monitored using a system that automatically aggregates audit logs from across the entire organization and that provides single search queries and proactive auditing to save time.

2. *Catch and resolve* – It is important to proactively audit all access 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. *Document* – A centralized and automated system provides the information required to document all investigations and their resolutions to fulfill notification requirements.

4. *Reporting* – 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. *Release of medical records* – With so many ways that a HIPAA violation can occur when releasing medical records, it is important to develop a process to document and track the release of medical records.

6. *Accounting of 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. *Protect your reputation* – Patients have a choice of which hospital to use. They won't choose the one featured on the nine o'clock news for breaching patient privacy. If patients cannot trust the hospital's ability to keep their health information private, they will not trust the hospital's ability to take care of their medical needs.

8. *Meaningful Use privacy requirements* – Under the HIPAA Security Rule, hospitals are required to implement policies and procedures to prevent, detect, contain and correct security violations (45 CFR 16308).

9. *Access risk* – Performing annual security risk assessments is not enough to protect patient privacy and address the HIPAA/HITECH requirement. Instead, take a more proactive approach across the entire organization. Review existing security of PHI, identify threats and vulnerabilities, assess risks for likelihood and impact, mitigate security risks, and document and monitor results.

10. *Review organizational requirements* – Regularly review and update breach notification and associated policies and business associate agreements.

It's really about trust

Protecting patient privacy goes hand-in-hand with providing high-quality medical care. Implementing a comprehensive patient privacy program is not just about preventing fines. It is about maintaining the trust and confidence of the patients you serve. If a hospital incurs a privacy breach, patients may well choose to go to a different hospital.

Trust is hard to earn and even harder to rebuild when it is lost. Federal and state governments have instituted regulations to ensure patient privacy is protected, but it is up to each healthcare provider to embrace and implement change across their organization.

Your patients are depending on you. **NP**