FEATURE Privacy

Proactive Compliance

Protecting Patient Privacy in an Ever-Changing Environment

By James Lawson and Michael 'Mac' H. McMillan

ABSTRACT

Healthcare institutions are at greater risk of falling short on patient privacy compliance than ever before. The movement to a complete electronic health record and constant changes to patient privacy regulations are key challenges. It can be difficult to maintain compliance due to these changing regulations, manual processes and limited resources. Hospitals face severe penalties for breaches, including financial, criminal, and harm to reputation. This article will review the changes to HIPAA mandated by ARRA and HITECH, including breach notification rules, penalties, Meaningful Use Stage 2 rules, and the OCR HIPAA Audits that started in 2011. It will review how hospitals can maintain compliance with patient privacy laws by implementing an automated auditing system, and will discuss breach incident tracking best practices. It will cover how to proactively review the thousands of patient records that are accessed daily, and how to catch breaches for reasons of human error, snooping, for profit, identity theft, and more. Multiple examples of patient privacy breaches from healthcare institutions will describe the effective methods for protecting patient privacy.

KEYWORDS

Patient privacy, ePHI, HITECH, Meaningful Use, HIPAA, audits, CMS, security breach, ARRA.

TECHNOLOGY ADVANCEMENTS in healthcare go both ways. They enhance the sharing of patient health information as well as the quality and efficiency of healthcare. At the same time, however, those advances make patient health information more vulnerable to inappropriate access and use.

In the interview that follows, James Lawson, VP Strategic Integration, Iatric Systems, and Mac McMillan, Chairman and CEO of CynergisTek, Inc., provide their combined insight into the effect technology is having on the privacy and security of patient health information and what hospitals should be doing about it.

Q. What are the top challenges facing healthcare organizations in relation to protecting patient privacy?

Healthcare today is the most regulated industry in America. It's also the biggest target for fraud and the theft of patient information, a threat that continues to grow. As a result we are likely to see more regulations as lawmakers and consumers wrestle with how to stem the leakage. These new regulations place a greater burden on an IT organization and industry that is already stretched thin. Regulations around breach notification and accounting for disclosures laser-focus the need for more accurate and timely access moni-

THERE ARE MANY THREATS to patient privacy. Most hospitals have done a good job of trying to protect hospital data from outside hackers. Surprisingly, the real threat is internal.

toring. More importantly, the cost of noncompliance and breach is rising sharply, making privacy a business imperative.

In this environment, healthcare organizations are faced with these specific challenges.

First, HIPAA forces healthcare providers to log every access to patient data. On top of that, technology advancements in data integration and networking now generate massive amounts of data sharing across many local and remote locations. This increases the challenge of protecting patient privacy.

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 needs to monitor and review an average of 52,000 patient access records. Think of every access to Electronic Protected Health Information (ePHI) as one red M&M candy in a jar. Now, of those 52,000 red M&Ms, there are 5 that are filled with cinnamon, not chocolate. They all look the same from the outside. One would have to bite into every one to find the cinnamon. This is just like looking at audit records. A hospital would have to manually review 52,000 accesses, every day, to find which ones are inappropriate. It's clearly unfeasible.

The third challenge is correlating the data from all the logs across all the disparate systems into one consolidated database. Seeing a single event of inappropriate access is just a clue in a mystery. When a hospital can see all the accesses at one time, it can easily see that someone is snooping.

Q. What are the most common threats to patient privacy?

We see it in the news every day. Hundreds of privacy breaches are reported, affecting millions of patients. There could be many causes for a breach. It could be due to theft of laptops or mobile devices that house patient data. It could be theft by someone who is authorized to access patient data but did so inappropriately, or incidents of patient data being accessed inappropriately by third parties. Whatever the reason, breaches continue an upward climb, costing hospitals millions.

There are many threats to patient privacy. Most hospitals have done a good job of trying to protect hospital data from outside hackers. Surprisingly, the real threat is internal.

That's 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 creates problems.

The two top internal threats are organizational complacency and human error or inadvertent activity. Organizations that don't implement diligent processes for monitoring what users are doing are setting themselves up for failure and embarrassment.

Others fall into three general categories. The first falls under flat-out snooping — such as an employee looking at the records of a neighbor or prominent person. Snooping is not that straightforward. An employee looking up his or her own information is a violation if they do not have a release at their facility saying that it's okay. If an employee who has been snooping knows he can lose his job over it, he will stop. The second inappropriate access falls into the for-profit category, such as getting data with the intent to sell the information. The third is red flags, which are all about identity theft.

With this many internal threats to patient privacy, it's necessary that hospitals audit all access to patient data proactively.

Q. Why is it necessary for audits to be proactive?

This is a simple concept, but difficult for healthcare organizations to do. Basically, proactive audits detect potential violations as they occur. Immediately catching and addressing these issues, as they happen, is the best way to prevent ongoing problems.

Let's take an example of identity theft, where credit card, Social Security, and drivers license information is being stolen. Catching an unidentified access the first time it happens, versus two years later, can make a big impact. If the first time a hospital hears about a breach is from a patient with a complaint, it might turn out that the hospital doesn't have one violation, but thousands. Any breach 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. This notification comes with a large fine and significantly harms a hospital's reputation. Proactive audits reduce the negative impact on the hospital and prevent ongoing problems.

Also, if individuals know that access is being monitored and that they will be caught and punished if they inappropriately access patient data, they won't do it. It's human nature. In fact, I worked at a hospital once that had a policy to immediately fire an employee if he is caught accessing patient data he isn't permitted to see. The hospital did it, too.

The word "proactive" goes hand-in-hand with receiving information in a timely manner. In the example involving identity theft, the bad guys are trying to steal an "identity." Having an automated monitoring process in place can alert the hospital if there are inappropriate changes to the data, such as gender changes, significant weight changes, or blood type changes. This can be addressed immediately and helps the hospital catch identity theft as it is occurring.

Q. Why has there been an increase in focus on this issue?

The most obvious issue is the changing regulations with the American Recovery and Reinvestment Act of 2009 — the HITECH Act and Meaningful Use. Those that do not comply risk severe penalties, including fines, law suits, and action by the attorney general just to name a few. But the most important driver is the threat of damage to the hospital's reputation.

The media has turned patient privacy into a big story. The last place a hospital wants to see its name is on HHS.gov or the 10 o'clock news.

The other reason for the increase in focus is extreme competition. We have seen a transition from one hospital per town to 20 facilities per town — all located a half a block from each other. If a hospital has a breach, a patient can easily choose to go to a different hospital around the corner.

In addition to patient privacy breaches, the media has a passion for celebrity information. Ironically, this is causing even more privacy breaches. Most of the information on the news centers around an inappropriate release of information about a celebrity or prominent person. Unfortunately, health information is now newsworthy.

And last of all, if the media, competition, and changing regulations are not enough, there are the governing audits. Today, there is an enormous potential for a hospital to be audited by the OCR and CMS, especially if it has attested for Meaningful Use.

Q. With all these pressures, why is access to patient data so difficult to monitor?

Hospitals are called on to do more with less. They need to excel in performance even in the face of declining hospital revenues. Hospitals are shifting to procedure-based, outcomes-based reimbursement, while continuing to improve the quality of care. Implementing a successful patient privacy program requires a huge commitment. Failing to implement one has a huge cost.

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. Here are some of the numbers from the report:

- 60% spend less than 3% of IT budget on information security
- 10% have an internal breach and disclosure auditing plan in place
- 1/3 reported a known case of medical identity theft
- 94% review audit logs
- 75% of those manually review

There is indeed a gap in handling patient privacy, and this problem stems from a lack of education. If the healthcare organization, specifically the CIO, really understood how much ePHI access is going on in their facilities, and really understood the ramifications, they would re-allocate their resources. In addition, healthcare organizations don't have appropriate staff in place to maintain the privacy program. This includes having employees who do not understand their responsibilities based on state/federal guidelines.

Healthcare organizations need to have documentation showing audit policies and procedures, and they need to have a reactive incident plan. If an incident happens, it's critical that the healthcare organization document what it is going to do. It's too late when the media calls and asks about a VIP breach. If a hospital has a reactive plan in place, has tested it to the best of their abilities, and has validated every incident that should be caught, that hospital can protect itself from risk.

The best-of-breed technology used in hospitals today can also be a barrier to the monitoring patient data access.

Q. Why do you say that the use of best-of-breed applications makes it harder to protect ePHI?

We have found that healthcare organizations that do not have an HIS that incorporates many applications, such as MEDITECH or Epic, typically have many disparate healthcare systems in their ED, surgery, laboratory, HR, radiology, and pharmacy departments.

Even though these systems provide the best assistance to hospital personnel, they tend to make it difficult for those hospitals to conduct comprehensive and correlated audit reviews.

Access to ePHI takes place in many different systems, and, to complicate the issue, access can be happening at locations that are remote from the hospital. Without looking inside the entire log of all activity and seeing patterns, the audit team cannot understand what the audit logs are telling them.

Q. How big is the risk to hospitals that are unable to demonstrate compliance with these regulations?

The passage of the HITECH Act has imposed a historic level of privacy and security requirements on healthcare providers. These mandates require hospitals to notify patients, within 60 days, if their PHI has been accessed inappropriately. Some states have even tighter reporting requirements. Penalties imposed on hospitals for failure to comply can add up to as much as $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 the past two years, breach notification has seen a 60-fold increase in audits conducted by the OCR. Breach notification has highlighted significant failures to secure health records, with the number of breaches reported increasing by 32% from

2010 to 2011 at an estimated cost to the healthcare industry of $6.5 billion.

More recently, the early results of the first random audits confirm that user activity monitoring is a huge deficiency for most healthcare entities. In the first round of audits, which included 20 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 ePHI. The risks are huge.

Q. What steps can hospitals take to pass these audits and meet the many regulations related to patient privacy?

The privacy of digitized patient information needs to move away from the limiting random manual audits that review a very small percentage of the overall access events that occur every day in healthcare settings. Through advancements in Electronic Health Records mandated by HITECH, the automation of logging and monitoring, and the introduction of Privacy Monitors and security information and event management (SIEM) into the enterprise, healthcare can transform privacy protection into a proactive, 100%, near-real-time review of user interaction with patient information.

Once automation is implemented, hospitals 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 multiple patient care systems is the easiest and most effective way to streamline these processes to ensure compliance. With the 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 hospitals have processes in place to do something about it when a breach is identified.

During the past decade, we have found that a successful patient privacy program contains the following attributes.

1. Some kind of centralized monitoring system that can track employee access to patient records
2. The ability to catch and resolve single and recurring breaches as they happen
3. A process for documenting breach investigation and resolutions, and how to meet reporting requirements
4. An employee education program that presents the hospital's policies, the laws, and the consequences of inappropriate access
5. A process in place that meets Meaningful Use requirements

Protecting patient privacy goes hand-in-hand with providing high-quality medical care. It's interesting to realize that, in the name of improving patient care, hospitals readily share treatment and technology information with other healthcare providers. Yet, when it comes to sharing how they are using technology to ensure the privacy of patient data, there is no sharing going on. When hospitals are sharing information and technology with other providers to improve healthcare outcomes, we urge them to bring the privacy of that patient data into the discussion. It's up to each healthcare organization to do everything possible in this ever-changing and highly regulated environment to protect patient privacy. **JHIM**

James Lawson has more than 14 years of experience in the healthcare industry and is a systems integration and application security expert. As VP Strategic Integration, at Iatric Systems, James has many responsibilities, including management of the programming, implementation, and support of Iatric Systems Security Audit Manager. Before joining Iatric Systems, James was the principal of HCT Consulting, assisting HIM departments (among other areas) across the nation.

Michael 'Mac' McMillan is cofounder and CEO of CynergisTek, Inc., a firm specializing in the areas of information security and regulatory compliance in the healthcare sector. Mr. McMillan brings over 30 years of combined intelligence, risk management and security consulting experience. His philosophy for security is grounded in understanding the complicated nexus between people, processes and technology. He has focused on developing appropriate solutions based on business purpose and knowledge and a common-sense application of technology and controls. He has worked in the healthcare industry since his retirement from the federal government in 2000 and has contributed to HFMA, HCCA, AHIA, AHIMA, and HIMSS. He is the former Chair of HIMSS Information Systems Security Working Group. In 2009 he joined the HIMSS Privacy & Security Steering Committee and was selected as its Chair in 2010. He contributes frequently to healthcare periodicals and was a contributing author and editor for the HIMSS book, Information Security in Healthcare: Managing Risk. Prior to CynergisTek, he was the National Practice Director for Information Security Services at CTG Healthcare Solutions. Before that, he spent more than 20 years in the federal government and served as Director of Security at two defense agencies. Mr. McMillan holds a Master of Arts degree in National Security and Strategic Studies from the U.S. Naval War College in Newport, Rhode Island and a Bachelor of Science degree in Education from Texas A&M University in College Station, Texas. He was a 1993-4 Excellence in Government Fellow and is a graduate of the Senior Officials in National Security program from the John F. Kennedy School of Government, Harvard University. He was awarded both the Department of Defense Silver and Gold Medals for Exceptional Meritorious Service.