THE CHANGING LANDSCAPE OF HEALTHCARE: A WHITE PAPER

THE IMPACT OF THE FINAL RULE ON HEALTHCARE ORGANIZATIONS AND TECHNOLOGY

EXECUTIVE SUMMARY

Since the Health Insurance Portability and Accountability Act of 1996 (HIPAA) went into effect, the landscape of healthcare has changed for all entities.

Since 1996, there have been significant advances in technology – sophisticated wireless networks, smartphones and tablets. HIPAA Privacy Rules had to be updated along with these advancements to address security and privacy concerns related to protected health information (PHI).

And on Jan. 17, 2013, the U.S. Department of Health and Human Services (HHS) addressed these concerns by announcing a new Final Omnibus Rule "to strengthen the privacy and security protections for health information established under HIPAA."[1] Specifically, the Final Rule "provides the public with increased protection and control of personal health information."[1] The Final Rule applies to business associates, including subcontractors, or those entities or individuals that maintain PHI on behalf of a covered entity.[2] For organizations and business associates not in compliance (no matter the size), there is a maximum fine of $1.5 million. The new privacy and security rules increased damages for civil penalties, and the criminal penalties remain the same; however, OCR is now taking a more proactive and strict approach to HIPAA violations and prosecutions.

From private practices to healthcare systems, organizations must take appropriate steps to make sure they are HIPAA compliant and follow the guidelines of the Final Rule.

HIPAA PRIVACY RULE AND THE FINAL RULE

When instituted, HIPAA's Privacy Rule was a set of standards to "address the use and disclosure of individual's health information – called "protected health information" by organizations subject to the Privacy Rule."[2] One of the main objectives of the Privacy Rule was to protect PHI while promoting effective workflows within an organization.

Currently, there are more than 5,000 hospitals, approximately 1 million healthcare providers and hundreds of thousands of business associates in the U.S. All are affected by the Final Rule, which addresses minimum necessary use and disclosure, sales of PHI and disclosure of child immunization proof to school, to name a few. Additionally, the Final Rule expands individual patients' rights as well. For instance, a patient can request a copy of their electronic medical records in an electronic form, and the provider has an obligation under the regulations to fulfill that request.

What does this mean for involved parties? All entities must evaluate whether they are compliant or non-compliant. "One of the key challenges most organizations face is that they are not sure how to comply with some of these regulations like HIPAA…" explains Ali Pabrai, MSEE, CISSP, chief executive of ecfirst, home of the HIPAA Academy and a company that offers training, certification and consulting in the areas of cyber security and compliance. "The most critical first step is to conduct a very comprehensive risk analysis exercise, inclusive of a technical vulnerability assessment, which establishes a baseline of what areas of the regulation comply with [the Final Rule], and what areas do not comply or have deficiencies," he says.

In fact, Pabrai suggests organizations put together a risk assessment/analysis policy, which would be completed on a fixed schedule. For instance, a practice would perform one in the beginning of the year, and if they find 50 issues, they can address those issues throughout the year. The next year, the practice would evaluate those previous issues as well as address new or updated regulatory requirements and vulnerabilities.

PENALTIES FOR NON-COMPLIANCE

With the onset of the Final Rule, a primary care physician (PCP), a 25-bed critical access hospital and a 26-hospital health system, are held to the same standards as well as to the same financial penalties. As Pabrai points out – each will choose their own way to comply, but "it comes down to three elements: a combination of reasonable and appropriate policies, procedures and capabilities (i.e., security controls)."

Prior to 2008, Pabrai explains, HIPAA was not really enforced. "Now there are seven-figure fines, and this has put a lot of pressure on the industry to take this much more seriously, more than they have done in the past," he says. "There is still a long way to go. Healthcare organizations are rich in identity information and generally poor at protecting it."

In any case, the cost for an organization to become compliant is much less than the penalties for non-compliancy. These fines range from $100 to a few hundred thousand dollars. In addition, the Final Rule now extends to business associates, who can be penalized for breach of contract. There are four factors used to determine whether a breach has occurred: the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; the unauthorized person who used the PHI or to whom the disclosure was made; whether the PHI was actually acquired or viewed; and the extent to which the risk to the PHI has been mitigated.

SECURING TECHNOLOGY

For companies like Konica Minolta Business Solutions U.S.A., it is imperative that their multi-functional peripherals (MFP - copier, printer, fax) are protected against outside threats, especially since these devices have become more intelligent. "[The devices] are capable of storing information, are connected to a network and are capable of transmitting information," says Pabrai. Organizations have to review these technologies very carefully to ensure sensitive information is appropriately protected, he explains.

Furthermore, organizations rely on wireless infrastructures, which can be easily compromised.

And with the increase use of smart phones, tablet devices and iPads, there is a risk these devices will be lost or stolen. "A person can afford to lose a $500 iPad," Pabrai says, "but an organization cannot afford to lose a $500 iPad with 1,000 patient records that were not encrypted."

However, when Pabrai's company conducts HIPAA assessments and

audits, he also hears another perspective. Nurses and doctors rely on these devices to share photos of a patient's condition. This is an invaluable process to all parties, if the resulting outcome can be a faster diagnosis. However, the caveat is protecting the patient information, which can be easily compromised if such information is exchanged as a text message or an email without the appropriate encryption.

Companies developing and manufacturing MFPs must complete a risk assessment before releasing new products, programs and devices. Konica Minolta has taken a proactive approach to assessments by undergoing extensive compliance testing through ISO. In 2010, the company released "HIPAA Security Compliance for Konica Minolta bizhub MFPs," a white paper that examined how a healthcare facility could configure security settings in MFPs to satisfy HIPAA Security requirements.

The Federal Register published the Final Rule, comments and clarifications, and now it is explicit that MFPs come under the purview of the privacy and security rule per the following excerpt from the Federal Register: "…we clarify that protected health information stored, whether intentionally or not, in photocopier, facsimile, and other devices is subject to the Privacy and Security Rules. Although such devices are not generally relied upon for storage and access to stored information, covered entities and business associates should be aware of the capabilities of these devices to store protected health information and must ensure any protected health information stored on such devices is appropriately protected and secured from inappropriate access, such as by monitoring or restricting physical access to a photocopier or a fax machine that is used for copying or sending protected health information. Further, before removal of the device from the covered entity or business associate, such as at the end of the lease term for a photocopier machine, proper safeguards should be followed to remove the electronic protected health information from the media."[4]

Pabrai also suggests giving customers the option and flexibility to determine how they want to protect their patient information on these devices. There are a number of technology options available, such as proximity card, biometric or password authentication.

PRACTICE PERSPECTIVES

PRA Behavioral LLC, an outpatient psychiatric practice based in Illinois, could be the gold standard of Final Rule compliance. With three offices, PRA Behavioral maintains a staff consisting of psychiatrists, psychologists and supporting personnel. Since it is an outpatient facility, the staff communicates with outside vendors, schools and PCPs on a regular basis. And to protect their patients, there is full information transparency with patients. "We don't want to assume anything," explains Paula M. Comm, MA, LCPC, practice administrator. "And that's one of the safest ways to enact the law. You make sure your patient has full control over what is being disclosed."

Unlike similar practices, PRA Behavioral goes beyond HIPAA's privacy rules, including not sending emails with patient information and not communicating with PCPs if a patient was referred to the practice by the PCP, unless a release of information has been signed by the patient. PRA Behavioral has many other safeguards in place to protect patients and the facility. For instance, there are two levels of usernames/passwords to access computers, and there is also a level-based access control security system within its prescription application. Levels range from zero to four. The level depends on the individual's job function. For example, physicians are a level four; they have the most freedom, explains Comm. Scanners at the practice are a level zero. Additionally, PRA patient forms are specific to ensure the staff knows what individuals the patient wants information released to, and what numbers the staff can use to contact patients for reminder calls or questions regarding treatment. When information is released, PRA wants to make sure only to release the requested information, which has received final consent from the patient. This meets the Minimum Necessary Standard (164.502) provision of HIPAA.

In September 2011, Comm began conversations with Konica Minolta about transitioning to electronic medical records. "When we had to go electronic, I was so overwhelmed with the concept of how [we] were going to do this," says Comm, "and how were we going to keep our flow because [we] were so paper heavy." The venture proved complicated as it required a lot of rework with the billing software and scheduling software companies.

Konica Minolta worked with RxNT, an ePrescribing technology vendor, and Synergistic Office Solutions, Inc. (SOS), a scheduling and billing software company, respectively, to create an intuitive, seamless and secure process. Now, documents are scanned into Konica Minolta MFPs using one ID number, which is shared with RxNT and SOS. The document then is attached to the appropriate record. Comm explains that her staff follows up to confirm files are attached to correct records. Implementation and equipment fixes were finalized in March 2012.

For healthcare practices that need to assess compliancy, Comm recommends documenting all interactions and notifying patients immediately if there is an infringement. This is critical given the breach notification provisions made permanent in the Final Rule legislation. And similar to PRA Behavioral, PCPs and other healthcare facilities "have to make sure good machines and systems are in place to guarantee people are given informed consent."

CONCLUSION

In discussions with clients, Pabrai imparts the following advice: "HIPAA is a journey with no destination." Compliance must become the fabric of the organization—a process completed annually with a planned methodology in place. Ultimately, non-compliance is a costly decision with major implications to the organization as well as the constituents it is supposed to support and protect.

ABOUT KONICA MINOLTA BUSINESS SOLUTIONS U.S.A., INC.

Konica Minolta Business Solutions U.S.A. is dedicated to helping healthcare facilities protect its most valuable asset – protected health information.

By understanding the current challenges faced by facilities, Konica Minolta aims to create solutions that safeguard patient information as well as reduce operational costs. Konica Minolta Business Solutions focuses on complete business solutions including multifunctional products (MFPs), managed print services, and industry-specific solutions, services and supplies for healthcare systems.

Whether an organization wants to improve overall efficiencies, replace paper storage with a fully electronic system or institute a more private and secure system, Konica Minolta's solutions address all these concerns.

Konica Minolta's EnvisionIT Healthcare strategy places a strong focus on partnering with our customers to offer practical solutions to their real world problems and challenges. EnvisionIT delivers award winning MFP technology, best-of-breed software solutions and managed IT services in a single package customized specifically for our healthcare customers.

References
1. New rule protects patient privacy, secures health information. www.HHS.gov. January 17, 2013. http://www.hhs.gov/news/press/2013pres/01/20130117b.html. Assessed 5/3/2013.
2. HIPAA Final Rule: Bottom-Line Summary. ecfirst.
3. Summary of the HIPAA privacy rule. OCR Privacy Brief. United States Department of Health & Human Services. http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/. Assessed 5/3/2013.
4. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules. Office for Civil Rights, Department of Health and Human Services. Published 1/25/2013. Pages 41-42.