Wake-up Call on the Security Rule

By Chris Dimick

Recent changes to the enforcement of the HIPAA security rule have left many and HIM professionals wondering what, if anything, they need to change in order to stay compliant.

Federal regulation last year introduced the potential for additional random audits, increased fines, and established a requirement that covered entities notify patients of privacy and security breaches. These changes, however, have left the security rule itself mostly intact, says William Miaoulis, CISA, CISM. What they have changed is the impact of noncompliance.

"[The security rule changes] didn't change the standards, really," Miaoulis says. "What it did was tell people that they really need to refocus their efforts on the standards. 'Yes, you did HIPAA three, four, five, maybe six years ago. Okay. But what have you done lately?'"

The best way for organizations to avoid a security rule disaster is to dust off their policies and reevaluate their compliance initiatives, says Miaoulis, a HIPAA security and privacy consultant for Phoenix Health Systems and author of the new book *Preparing for a HIPAA Security Compliance Assessment* (AHIMA Press, 2010). They should heed the fed's wake-up call.

Quiet So Far, OCR Is Gearing Up

Many in the industry expected that the 2009 transfer of HIPAA security rule enforcement powers from the Centers for Medicare and Medicaid Services (CMS) to the Office for Civil Rights (OCR) would lead to dramatically increased compliance reviews and HIPAA violation investigations. While that has yet to be seen, it is clear that OCR is preparing to step up both security violation investigations and random compliance reviews.

Speaking at the Safeguarding Health Information conference last May, Susan McAndrew, OCR deputy director for privacy, said that OCR spent its first year mainly getting acquainted with security enforcement. This year, she said, would be the year OCR moves security enforcement to the forefront of its efforts.

OCR has added investigators in 10 regional OCR offices with the expectation to conduct more HIPAA security compliant investigations and compliance reviews.

Since OCR began reporting its security rule enforcement results in October 2009, the organization has received 166 complaints alleging a violation of the rule through August 2010. During that period, OCR investigated, applied appropriate corrective action, and closed 59 of the cases, according to numbers posted on its Web site.

Not all of these cases likely involved a detailed investigation of the facility's HIPAA security rule compliance, Miaoulis said. Some cases are handled and resolved with the exchange of a few letters. Full compliance evaluations are possible in response to a compliant, however.

OCR also has the ability to also conduct random security rule compliance audits at covered entities. While random audits have not begun, OCR representatives said they do intend to begin them in the future. The office has hired a contractor to recommend strategies for implementing random audits. However, the OCR has not announced when the audits will begin.

OCR, which also enforces the HIPAA privacy rule, was given authority over security rule enforcement through the HITECH Act, a section within the American Recovery and Reinvestment Act of 2009. The HITECH Act also increased monetary fines for HIPAA privacy and security violations, gave state attorneys general authority to prosecute HIPAA violations, and required that business associates of HIPAA covered entities also comply with HIPAA privacy and security regulations.

The HITECH Act also added a requirement that covered entities notify patients of breaches to the privacy and security of their protected health information and submit information on all such incidents to the Department of Health and Human Services. OCR could use these notifications to target healthcare organizations for audits, Miaoulis notes.

Risk Analyses Essential

Being prepared for a HIPAA security rule compliance audit—either conducted at random by OCR or triggered by a security breach incident—has never been more important. The enforcement and policy changes make it vital that healthcare organizations ensure their medical record systems are secure and all policies and operations comply with HIPAA security rules.

"When the impact [of security violations] went up, our risks went up, and our need to have better security went up," Miaoulis says.

The best way to ensure compliance is by conducting an organization-wide security risk analysis.

"Risk analysis and risk management are really the key … to prepare for an OCR security audit," Miaoulis says. Documented risk analyses are required of HIPAA covered entities, and they must be conducted to evaluate and mitigate privacy and security vulnerabilities surrounding personal health information. This has been the case since HIPAA first took effect in 2003.

Risk analysis is a process to identify threats, vulnerabilities, and risks to the organization's protection of health information. These risks are evaluated based on their probability and impact on the organization and then determined to be low, medium, or high. Organizations then use the results to create a plan to minimize the risks and reduce the impact to both the organization and its patients.

If a risk is found, organizations can chose to respond with one of four options, Miaoulis says:
• Accept the risk, which could be done if its probability is low or the harm minimal
• Mitigate the risk by implementing risk controls
• Transfer the risk, typically by purchasing insurance
• Research the risk, a temporary solution that allows further study of the risk and its impact

Selecting the appropriate option for risk mitigation depends on the severity of the risk and the consequences if it occurred. The security rule gives flexibility that allows organizations to enact security controls based on their risk analyses.

"A risk analysis describes what you think your risk threshold is and what additional controls, if any, you want to implement," Miaoulis says.

For example, an organization's physicians store protected health information on laptops. A risk analysis shows this information could be susceptible to breach through theft or other means. The HITECH Act states that if breached PHI is encrypted, the organization does not have to report the incident. The organization categorizes laptop theft as a high-risk scenario, reviews its options for mitigation, and decides to encrypt all laptops. It renders the PHI inaccessible and prevents the need for sending notifications should a breach occur.

Miaoulis offers another example: an EHR system's ability to capture staff access to patient records to monitor unauthorized access. The risk analysis would evaluate the organization's security processes for managing unauthorized accesses, such as audit trials and password protections, and determine any remaining risks to the information.

If ONC conducted a HIPAA security audit, it would look at an organization's analyses and determine if it adequately provides compliance with the HIPAA security rules.

When CMS enforced the security rule, it did conduct some random compliance audits. One of the first things investigators asked for was the organization's risk analysis, Miaoulis says.
The investigations typically found them deficient.

Investigators also found deficiencies in privacy and security training, workforce clearance procedures, workforce security policies, encryption levels of unsecured information, and business associate agreements. These are all areas healthcare

facilities should evaluate in their analyses.

A Carrot, Too—Meaningful Use

The threat of increased fines and enforcement is not the only reasons healthcare organizations should reevaluate their HIPAA security risk analyses. The HITECH "meaningful use" incentive program, which provides Medicare and Medicaid bonuses for meeting specified EHR use, explicitly calls for organizations to conduct and document a risk analysis and implemented security controls, Miaoulis notes.

Avoid the Audit Poster

While ONC has not yet begun its random audits or significantly increased its violation investigations, organizations should not get comfortable. They should use this time to prepare.

"You don't want to be the poster child…," Miaoulis says. Audits "are going to happen, and you want to be prepared now."

Original source:
Dimick, Chris. "Wake-up Call on the Security Rule" (Journal of AHIMA), October 2010.
