Preparing for the Next Big April

Save to myBoK

by Mary Thomason, RHIA, CHP, CISSP

Yesterday's privacy compliance preparations can contribute to meeting tomorrow's security mandates. One organization is tackling risk analysis with both matrix and memories.

The 2003 HIPAA privacy rule implementation is still fresh in many minds throughout healthcare organizations. And that's good, because some of the work done for the privacy rule can be helpful in preparing for the upcoming security rule. Intermountain Health Care (IHC), a nonprofit integrated delivery system based in Salt Lake City, UT, is approaching the mandated systems risk analysis with an efficient, two-part plan based in part on data compiled for privacy rule compliance.

IHC began its overall planning for the security rule with a review of the processes, policies, and data related to the earlier privacy rule implementation. The healthcare system found it could model its security implementation committees and their roles on the matrix used for the privacy rule. Several privacy policies overlapped—or at least made a good starting point— such as the sanctions policy and the record and data destruction sections in the reasonable safeguards policy. Some data carried over, also. The list of data and record sets, previously compiled to determine the designated record sets required under the privacy rule, helped IHC informationtechnology (IT) staff identify and prioritize technology systems for the risk analysis. Performing that assessment efficiently is important for any organization, but given IHC's size, efficiency is a necessity.

A Studied Approach to the Risk Analysis

IHC is comprised of approximately 24,000 employees, 21 hospitals, 100 associated clinics, a health plan with 480,000 covered lives, and a physician's division with 400 employed physicians. The technology behind this network is considerable. IHC assigns a master number for all persons served as members of the health plan as well as those who have been patients. The system has a clinical data repository, centralized facility billing systems, and enterprise data warehouse, as well as a multitude of databases and systems and a complex web of interfaces. At last count, IHC has close to 100 major databases and systems and thousands of applications.

At first glance, implementing the self-assessment required by the security rule in such a large and complex organization is overwhelming. IHC approached their risk analysis in two key steps: a "best practice/common practice" assessment and a system-criti-cality assessment. These steps make sense for a large and complex organization where implementation of the security rule may be costly and time consuming if not carefully managed. However, the model also provides a useful tool for benchmarking and ranking security systems for organizations of any size.

Identifying "Best" and "Common" Practices

Because implementation of the security rule is intended to be scalable, it makes sense to compare an organization's security practices to similarly sized organizations. IHC choose to classify and compare their practices according to two categories.

Best practices are methods based on generally accepted principles as determined by IT security professionals. They are guidelines for developing and implanting security policies and procedures and deploying technologies in order to comply with regulatory requirements and to protect business interests. Best practices may meet or exceed regulatory standards.

Common practices refer to average practices within which the majority of healthcare organizations fall. Typically, common practices are below the best practice levels for IT security in a given area and may be less than what the security rule requires. However, they help determine a baseline of where the industry may be at a given point in time, and they determine how far an organization needs to go to meet a reasonable standard.

The first step completed by Ryan Smith, director of IHC's enterprise information security and Web operations, was to analyze the security rule and determine the key standards. He then contacted several other healthcare systems to determine what their procedures were in these areas and compared these with current IHC practices. From this comparison, Smith generated a list of areas in which IHC exceeded other organizations and a list of areas in which it was more in line with common practice. The common practice items were then assigned higher priorities for detailed assessment and risk analysis.

Prioritizing Systems

The IT security team then began to assess the different IHC systems. As a matter of policy, IHC decided to apply the same standards of security to any critical business system, not just systems that contained PHI covered by the security rule. However, the team began with the list of systems containing PHI and the list of designated record sets compiled as part of the privacy rule compliance effort. It then deleted the paper-only record systems and added in the business critical electronic record systems.

The data were first classified by content, with systems containing PHI given the highest rating. Systems were then given an operation disruption score based on impact to patient care and safety, as well as overall impact to IHC's business. Finally, the systems were rated as to extent of use within IHC: were they enterprise-wide, division- or department-specific, or for local use only?

Based on these ratings, the most critical systems are being reviewed first for security practices and risk assessment. It's a long and complex analysis, but a head start gained from experience with the privacy rule implementation and a process of benchmarking and prioritizing systems allows IHC to undertake the task efficiently.

Mary Thomason *(mary.thomason@ihc.com) is HIPAA oversight project leader at Intermountain Health Care in Salt Lake City, UT.*

Article citation:
Thomason, Mary. "Preparing for the Next Big April." *Journal of AHIMA* 75, no.4 (April 2004): 24-25.
