A Decade of HIPAA

By Mac McMillan

The Health Insurance Portability and Accountability Act (HIPAA) has ushered in a new era in healthcare that has transformed the way information is managed and used to deliver care. While we often say we still have a long way to go before achieving compliance with HIPAA, it is clear to anyone who has worked in this industry for the past decade that a tremendous amount of progress has already occurred since the Privacy Rule went into effect in 2003. As more patient information has become digitized and systems and data have become critical components of hospital operations, data security and privacy have become more important and as a result are receiving more attention.

HIPAA's Early Days

Prior to 2003 the average healthcare entity had very little remote access or external connectivity to its clinical data. A considerable amount of patient information was still in paper files. The typical healthcare provider had a security program that was extremely immature with very few policies beyond acceptable use. Security technology was limited to firewalls, antivirus, spam filters, and web content managers. Encryption was nonexistent. Audit and monitoring was exclusively a manual reactive process. Mobile device access was limited to e-mail. And security staff, if it existed, was all too often just one individual with other responsibilities—lacking in formal training and without certifications in information security. Disciplined configuration management practices or hardening of systems was unheard of; adherence to an established security framework was not even possible. An initial security assessment revealed an enterprise and organization widely susceptible to compromise and for the most part unaware of its security risk.

Healthcare providers have seen significant change since those early days. Today the vast majority of patient information is digitized, living in hundreds of applications and millions of files on the network. Virtually every operational process is automated or relies on computer-generated data. The four walls of the earlier entity have been replaced by a new environment that seeks ubiquitous access to data via unlimited connections on a wide array of devices.

As a result of these changes and HIPAA's focus, organizations began to address their security controls. Functional responsibility for security was assigned, security programs established, risk assessments and vulnerability testing began to raise awareness, and expanded compliance programs provided oversight and visibility. Healthcare also added to the inventory of security technologies by introducing privacy monitoring tools capable of processing audit logs from health IT applications to monitor user activity and rules. HITECH enhancements to HIPAA privacy and security rules introduced incentives and public scrutiny, as well as greater consequences. More sophisticated security technologies emerged, such as data loss protection and security incident event managers. Stage 2 of the Centers for Medicare and Medicaid Services' (CMS) "meaningful use" EHR Incentive Program has led organizations to pursue global deployment of encryption solutions to protect PHI wherever it's stored or transmitted.

Health Information Technology Evolution

Health IT has also evolved significantly as a result of HIPAA in the last decade. In 2003 very few health information technologies or medical systems had security functionality. That has changed, and in 2009 the HITECH Act expanded HIPAA and introduced incentives for adoption of electronic health record technologies. This was necessary to achieve the goals of administrative simplification and to support health information exchange, but it also introduced greater risk as more information became data. In recognition of these risks, certification criteria were introduced requiring vendors to incorporate security functionality into their products and for organizations to implement them in a meaningful way. One notable player in this space, the EPIC Corporation, not only created a fully integrated EHR significantly reducing risks, but incorporated a security module in its solution and called for a dedicated security analyst position within the EPIC support team.

In addition to enhancements within electronic health records, the US healthcare industry has also begun work on frameworks and standards for interoperability and information exchange. Most recently, the US Food and Drug Administration (FDA) is looking at standards for mobile applications that may interface with clinical systems.

Evolving Workforce

HIPAA has also raised awareness in healthcare and is supporting the emergence of a new specialization for information security professionals. HIPAA privacy and security, which calls for accountability for both corporate and individual behavior, has increased the level of awareness of workforce members. Training is now mandatory for anyone accessing patient information. As mentioned before, there are also better tools for monitoring, providing better insight into where risks exist, and contributing to knowledge of threats. Well informed users contribute to the success of any information security program.

The role most critical to the success of the program is the individual managing it. HIPAA's impacts are seen here as well. Today, the professional filling the critical role of managing a security program is more likely to have their position dedicated to security, has received security training, carries security-specific certifications, and has had previous security experience. While all these attributes mark a departure from environment in the early days of HIPAA, one of the biggest indicators of change is that professionals in a security management role are also more likely to manage a small staff of direct reports with respective dedicated security duties.

Enforcement and Compliance

In the early years of HIPAA, rule enforcement was focused on encouraging compliance. Prior to 2009 there were very few corrective actions issued and even fewer punitive fines. Congress sought to remedy this in 2009 with two actions:

- Shifting responsibility from CMS to the Office for Civil Rights (OCR) for enforcement oversight
- Developing a combination of public reporting requirements that introduced reputational risk and strengthened penalties —increasing both the risks and costs of noncompliance

Today OCR handles more than 10,000 complaints and over 100 major breach investigations, and also conducts random compliance audits to measure the industry's performance annually. CMS has also added meaningful use attestation audits to the list of accountability tests healthcare must be ready for. On the positive side, greater accountability has also spawned greater investment and additional resources for privacy and security.

HIPAA Today

The average HIPAA-covered healthcare provider has seen significant changes in the last decade. Many are actively preparing for stage 2 of the meaningful use program, pursuing HIE membership, or establishing an accountable care organization. An average covered entity is also likely focusing on physician alignment with patient engagements, and even embracing social media and the ever-expanding mobile environment. Remote users and vendors use two-factor authentication to gain access. Generic logins no longer exist. The network is segmented—both ether and wireless. Systems are hardened before going into production and are scanned afterwards. Vulnerability scans are conducted monthly, as is patching. The network is constantly and consistently monitored by a third party. Encryption is deployed everywhere—even texting—with the exception of a small number of back end databases. Back up tapes have been eliminated with disk-to-disk back up in redundant certified data centers and there are a number of other security technologies deployed.

The program itself has moved beyond HIPAA, now measured against a matrix of requirements that include HIPAA, HITECH, ISO 27002, PCI/DSS, multiple NIST and FIPS guidelines, and state laws.

With one decade under its belt, the changes that have sprung from HIPAA will continue to expand as the US healthcare industry landscape continues to develop and evolve.

Mac McMillan is chief executive officer at CynergisTek.

Original source:
McMillan, Mac. "A Decade of HIPAA" (Journal of AHIMA website), April 12, 2013.