THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp
Editor, Kirk J. Nahra, CIPP
September 2011 • Volume 11 • Number 7

Anniversary of a bill

The Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996. On the occasion of its fifteenth anniversary, The Privacy Advisor *takes a closer look.*

By Kirk J. Nahra, CIPP

The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996. As the name indicates, the law was focused on "accountability" and "portability" in the healthcare system, issues that had little or nothing to do directly with privacy or information security. These focuses—designed to "solve" various problems in the healthcare industry—drove the legislation and were passed with very broad support. Beyond these topics, Congress chose to build on this consensus by addressing other, largely unrelated topics in this legislation, affecting portions of the healthcare industry. For example, much of the healthcare fraud enforcement of the past 10 years was driven by various HIPAA proposals.

One of these "add-ons" was the idea (or oxymoron, depending on your perspective) of "Administrative Simplification"—the concept that standardizing certain critical healthcare transactions would improve efficiency and decrease costs. So, Congress mandated a process to develop the technology for these transactions, designed to push the healthcare industry towards a more electronic healthcare

HIPAA then and now

Marcy Wilder

The Privacy Advisor asked Marcy Wilder, Hogan Lovells partner and former deputy general counsel at the Department of Health and Human Services, to look back on HIPAA's beginnings. Wilder was the lead lawyer on the HIPAA Privacy Rule back in 1999. She said, "I can say with certainty we've come a long way. The HIPAA Privacy and Security Rules have been enormously successful in raising awareness about the importance of health privacy; improving the privacy and security of health data and health information systems; limiting the use of medical information for marketing, and ensuring patients have access to and some control over their health information."

Nonetheless, Wilder points out some significant shortcomings, including "requiring privacy notices that read too much like mortgage documents; a failure to strike the right balance on the use of health data for research, and an overly burdensome accounting for disclosure requirement that was only made worse by HITECH."

Looking forward, she says HIPAA will "play a critical role in protecting privacy as we continue our evolution in the U.S. from a paper-based to an electronic healthcare system."

In terms of recent developments related to HIPAA, Wilder says the most dramatic has been the increased enforcement activity on the part of HHS.

"After years of voluntary compliance and corrective action plans, [the Office for Civil Rights] is imposing significant monetary penalties running millions of dollars, planning to conduct 150 HIPAA audits by the end of 2012 and training state AGs in HIPAA enforcement," says Wilder. "As a result, we are seeing increasingly serious HIPAA compliance efforts by covered entities and business associates, including risk assessments, updates to privacy policies and procedures, security incident planning and workforce training."

system. While there was widespread agreement on the desirability of these transactions, there was a general nervousness (remember, this is the beginning of the Internet era) about moving healthcare to an electronic environment. Accordingly, Congress also desired to encourage or require specific privacy and security concerns, but really didn't know what to do on these points. So, the HIPAA law itself says very little about privacy and security other than that there should be rules developed on privacy and security. Congress gave itself three years to pass new privacy and security laws (which it then failed to do) and created a fail-safe vehicle dictating that the Department of Health and Human Services (HHS) issue regulations on these points if Congress was unable to pass a privacy or security law.

That's how we ended up with the HIPAA Privacy and Security Rules, creating privacy and security standards for the healthcare industry. HHS was stuck with many of the jurisdictional components of the HIPAA law (for example, Congress decided who would be "covered entities" under any regulations, driven in part, for example, by entities that would be transmitting standard transactions (providers and health plans) and insurers who were connected to "portable" health coverage (health insurers rather than all insurers that have healthcare information).

So, the HIPAA statute itself did little specifically on privacy and security other than define the overall landscape of who would be covered. HHS did the rest, creating the broad regulatory structure for both privacy and security and (creatively) expanding the scope where it could apply these principles, primarily through the contractual obligations imposed on business associates.

Three key points to remember from this history: First, if someone says that the HIPAA law said something specific about privacy and security, they're probably wrong. Second, because of this history, the HIPAA statutory restrictions hindered the privacy rules somewhat by ensuring that the privacy rule would not be an overall medical privacy rule. Instead, the rule focuses on certain kinds of information when held by certain entities for certain purposes. Third—and for some, most important— despite more than a decade of constant errors, HIPAA is spelled with only one "p," standing for "portability."

***Kirk Nahra**, CIPP, is a partner with Wiley Rein LLP in Washington, DC, where he specializes in healthcare, privacy and information security litigation and counseling. He serves on the Board of Directors of the IAPP and is the editor of The Privacy Advisor. He can be reached at 202.719.7335 or knahra@wileyrein.com.*