Briefings on HIPAA

Happy Birthday, HIPAA: Reflections on the 28th anniversary of the law

by Dom Nicastro

In August, the Office for Civil Rights (OCR) celebrated the 28th anniversary of the signing of the Health Insurance Portability and Accountability Act of 1996, better known as HIPAA.

HIPAA is best associated with requiring, for the first time, a set of standards for safeguarding the privacy and security of individually identifiable health information.

“HIPAA is the cornerstone law that advances patient privacy, data protection, and health information security in our nation’s healthcare system,” Melanie Fontes Rainer, director of OCR, said in a statement. “Importantly, HIPAA, through the HIPAA Rules, empowers patients and consumers to take their own health data into their own hands and instills trust in the patient-provider relationship to allow for better care and outcomes. With the rise of cyberattacks breaching patient privacy, HIPAA is more relevant than ever. OCR continues to prioritize health information privacy by updating and rigorously enforcing the HIPAA Rules that safeguard our national security in the health care system.”

OCR officials went on to celebrate the birthday milestone of HIPAA with some reminders:

OCR has implemented the requirements of HIPAA and related statutes with the creation and modifications of the HIPAA Privacy, Breach Notification, Security, and Enforcement Rules. These rules set forth the requirements that health plans, health care clearinghouses, and most healthcare providers, and their business associates (e.g., third party administrator that assists a health plan with claims processing, accountant providing services to a healthcare provider, medical transcriptionist services to a physician) must follow relating to the privacy and security of protected health information (e.g., medical records, personally identifiable information).

The HIPAA Rules work together to protect the privacy and security of health information and ensure the continuity of our nation’s healthcare systems, including critical protections against cybersecurity threats, specifically:

- *The HIPAA Privacy Rule establishes national standards to protect individuals’ medical records, sets limits and conditions on the uses and disclosures of protected health information, and gives individuals certain rights, including the right to timely access and to obtain a copy of their health records.*
- *The HIPAA Breach Notification Rule establishes requirements for healthcare providers, health plans and healthcare clearinghouses, and their business associates when a breach occurs to help notify the public, ensure patients understand the implications of the breach to their privacy and ensure continuity of care.*
- *The HIPAA Security Rule establishes national standards to protect individuals’ electronic personal health information (ePHI) and ensure the confidentiality, integrity, and security of electronic protected health information.*
- *The HIPAA Enforcement Rule contains provisions relating to compliance and investigations, the imposition of civil money penalties for violations of the HIPAA Administrative Simplification Rules, and procedures for hearings.*

Reflections: Evolving sanctions and access rights

Rebecca Herold, CDPSE, FIP, CISSP, CIPM, CIPP/US, CIPT, CISM, CISA, FLMI, CEO of Privacy & Security Brainiacs SaaS services, recalls the first monetary penalty for HIPAA and how those sanctions have evolved.

“The first monetary penalty occurred in 2008: a comparatively small slap-on-the-wrist settlement (similar to a penalty) of $100,000, in addition to requiring a corrective action plan (CAP) to be implemented,” Herold says. “Since that time, the monetary penalties/settlements have significantly increased, with the largest to date being given to Anthem, Inc. for $16,000,000 in addition to a detailed CAP and continued ongoing oversight from the HHS for at least a period of two years.”

Ultimately, HIPAA has had a profound impact on healthcare security and privacy, Herold says. In addition, she argues that the benefits of HIPAA include:

- **Increased security of PHI.** This has been accomplished by requiring protections throughout three major domains of the HIPAA Security Rule: administrative, technical, and physical.
- **Increased privacy protections for patients and insureds.** The Privacy Rule requirements established some very important requirements for restricting the use, retention, and sharing of PHI. Prior to HIPAA, many healthcare entities and associated organizations were using PHI with impunity to perform research, to use in marketing, and to impact decisions for a wide range of insurances and loans. Such practices now cannot occur under HIPAA without consent from the associated individuals (patients and insureds).

- **Increased rights and controls of PHI by the associated individuals.** Prior to HIPAA, patients and insureds had no explicitly provided rights to obtain copies of their health records, to limit how their health data could be used, to correct their health records, to request their health records to be sent to other providers, or to limit the use of their health records, among many other rights now provided through the HIPAA Privacy Rule.

But Herold still sees areas for improvements:

- **More covered entities (CE) and business associates (BA) need to take action to be HIPAA compliant.** Many CEs, and the large majority of BAs, are far from being compliant. Concerningly, too many have not even started trying to meet HIPAA compliance after 28 years.
- **More public awareness is needed.** The more patients and insureds take actions to ensure their CEs are following HIPAA, the more CEs will realize that they need to do more to follow HIPAA.
- **Attorney generals need to take more HIPAA compliance actions.** Attorney general offices are slowly beginning to take more action in this area, but these is still plenty of room for the law to do more in enforcing HIPAA compliance.
- **HIPAA rules should keep pace with new tech and healthcare practices.** Everyone receiving healthcare services in the U.S. has benefited from the additional HIPAA rules targeted at specific issues and associated risks in the past few years.

“We look forward to seeing the actions that HHS and the state attorneys general offices take in the coming months for updating HIPAA,” says Herold, who authored an expanded blog post on the topic. “We hope to see the actions listed among them.”

Next wave of HIPAA compliance

Frank Ruelas, MBA, a compliance professional located in Casa Grande, Arizona, says he’s noticing a wave of people who are in what he calls the "new" generation of HIPAA compliance professionals; he calls them Gen2 since other generations are often referred to by letters or words such as Gen Z or millennials.

“These folks are replacing those who are retiring from the profession or venturing into other opportunities,” Ruelas says. “Consequently, I am seeing a resurgence in the number of questions that were commonly asked 10–15 years ago when everyone was still trying to figure out HIPAA.”

The availability of guidance, suggestions, and comments regarding HIPAA is tremendous, according to Ruelas. Using simple online searches can identify useful resources for just about any HIPAA professional, he adds.

“The sky is the limit in terms of how much one can find to help in answering questions for finding possible solutions to current issues or problems,” Ruelas says.

Further, Ruelas says he reads and hears people making statements related to HIPAA that quite simply are wrong.

“For example, on one online event the speaker talked about how breaches were identified if they caused financial or reputational harm to those affected by the breach,” Ruelas says. “We know this changed some years ago. [But] given how some people use these online sessions to educate themselves on HIPAA, it should be no surprise that people continue to get incorrect information.”

In addition, he notes that tried and true methods are still relevant today.

“Though the world is constantly changing and the use of technology continues to expand, sticking to the basics and what has worked in the past can be very beneficial,” Ruelas says. “One example I believe in is that there is no substitute for getting your nose into the HIPAA text and actually reading it. By developing a reasonable familiarity with the HIPAA regulations, one is much better informed, which can translate into better decision-making.”