

# HIPAA Mighty and Flawed: Regulation has Wide-Reaching Impact on the Healthcare Industry

Save to myBoK

By Daniel J. Solove

How HIPAA has performed overall as a privacy law is open to interpretation, but most agree it has had a wide-reaching impact on the healthcare industry. In comparison to the dozens of federal privacy laws for various industries, HIPAA is one of the most comprehensive and detailed.

It mandates the components of a facility's privacy program. It requires training. It specifies measures that must be taken to protect data security. It addresses de-identification of data. It has the only data breach notification requirement in federal law. It has potent fines for violations. Most other laws fail to do all these things. For example, the law regulating financial institutions-the Gramm Leach-Bliley Act-is rather vague about what must be done to protect security, and its privacy protections are minimal. The Family Educational Rights and Privacy Act (FERPA), which regulates privacy in schools, lacks specifics about creating a privacy program. FERPA also doesn't call for periodic assessment or training, nor does it say much about data security. Its enforcement is through an implausible sanction (denial of all federal funds) that has never been imposed.

"We often hear about how much stronger privacy law is in the EU [European Union] than in the US," says Joy Pritts, chief privacy officer at the Office of the National Coordinator for Health IT (ONC). "But HIPAA is more detailed, more specific, and in some ways stronger than EU privacy law. HIPAA provides a clearer sense of what is expected than many other privacy laws."

In short, when comparing HIPAA with other federal laws, hardly any is as comprehensive and specific as HIPAA. Of course, there are elements of other laws that HIPAA lacks, such as a provision that allows people to sue for violations. HIPAA contains many provisions allowing for disclosure with consent that have generated controversy. But these issues notwithstanding, it is hard to find a federal or state law or regulation that provides such a thorough blueprint for protecting privacy and data security.

"As much as HIPAA has been criticized and kicked around, I am seeing other sectors looking to HIPAA as a model for privacy regulation," says Deven McGraw, director of the Health Privacy Project at the Center for Democracy & Technology, "because it does a reasonably good job at balancing the needs of the healthcare industry with the rights and concerns of patients."

As far as impact, HIPAA really has made a difference. Even where it didn't change the law dramatically, the amount of awareness to health privacy and security it has brought-and the amount of compliance it has engendered-has been substantial.

"HIPAA Privacy and Security Rules have been extremely 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 that patients have access to and some control over their health information," says Marcy Wilder, co-director of Hogan Lovells' Global Privacy and Information Management practice.

HIPAA introduced privacy and security rights and regulation to the mass populous, Pritts says. Likewise, "[HIPAA] placed privacy and security of health data on the radar screen in a way that had not been done before," she says.

One of those rights widely introduced to patients by HIPAA was the ability to amend medical records, McGraw says. "The right to request an amendment is critical to achieving high quality care, because it is well known that data in clinical records is often of poor quality and wrong," she says. "Patients can play an important role in making sure data is correct."

Rebecca Herold, information security and privacy expert and CEO of The Privacy Professor, points out that HIPAA has resulted in a dramatic increase in funding for protecting health data. “I was responsible for information security and privacy at a large healthcare and financial organization throughout the 1990s, before there were any privacy or data protection regulations that had to be followed,” Herold says. “I can tell you that it was very hard convincing upper management of the need to invest in information security and privacy resources, technologies, and activities.”

For Chrisann Lemery, HIPAA security officer and assistant privacy officer at WEA Trust Insurance, HIPAA brought industry recognition to HIM professionals’ knowledge and expertise. “HIM professionals had been balancing an individual’s right to privacy against requests for release of healthcare information for decades unnoticed,” she says.

The biggest impact HIPAA had is that it shifted the way people think about health data, says Jodi Daniel, JD, MPH, director of office policy and planning at ONC. “Health data is collected and maintained not just for the purposes of the provider, but for both the provider and the patient.”

But HIPAA is far from perfect. Wilder observes the primary weaknesses of HIPAA as “requiring a privacy notice that reads like a mortgage document, an imbalance in permitting the use of health data for research, and the accounting for disclosure requirements, which are too burdensome to operationalize.”

One of the biggest areas of confusion under HIPAA involves appropriate access to health data, Daniel says. “There are still quite a number of instances when patients, caregivers, and others who should have access are denied access in the name of ‘privacy,’” she says. And despite the recent expansion in HIPAA’s scope to cover business associates, its coverage remains limited, McGraw says. “The public generally thinks that HIPAA applies to all health data, so many are unaware that the protections they enjoy in their doctors’ offices do not extend to their health apps or their personal health record,” McGraw says. “Today, we have as much of a problem with over-interpretation of HIPAA-[or] ‘HIPAA won’t let me share your data with you or with your other physicians’-as we do with under-interpretation. Yet we are only addressing the latter. The former creates unnecessary obstacles to data sharing, even in circumstances where there is enormous individual and public benefit from sharing.”

The key for the healthcare industry and its patients to best utilize HIPAA lies in education and guidance-and not as one-time exercises, McGraw says. “We have done a terrible job of assuring compliance and understanding,” she says.

Daniel J. Solove ([dsolove@law.gwu.edu](mailto:dsolove@law.gwu.edu)) is the John Marshall Harlan Research Professor of Law at George Washington University Law School, the founder of [TeachPrivacy](#), a privacy/data security training company, and a senior policy advisor at Hogan Lovells. The opinions expressed in this article are solely the author’s and not of any affiliated organization.

---

**Article citation:**

Solove, Daniel J. "HIPAA Mighty and Flawed: Regulation has Wide-Reaching Impact on the Healthcare Industry" *Journal of AHIMA* 84, no.4 (April 2013): 30-31.

---

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.