HIPAA at 20: Looking back at two decades of patient privacy protections

More than two decades ago, on August 21, 1996, then-President Bill Clinton signed the Health Insurance Portability and Accountability Act (HIPAA) into law. Since then, healthcare has changed a lot and HIPAA has helped guide those changes every step of the way.

HIPAA's early years

Although HIPAA was passed in 1996, it would take nearly seven years for the initial HIPAA Privacy Rule to go into effect. As the first federal law to address the privacy and security of health information, the HIPAA Privacy Rule was inherently complex. Privacy provisions in the original legislation signed by President Clinton totaled 337 words. The final rule issued in March 2002 was around 101,000 words long and spanned more than 500 pages, according to an October 2003 USA Today article.

"When the HIPAA regulation initially went into effect, it generated significant skepticism, confusion, and even angst," Jocelyn Samuels, director of the HHS' Office for Civil Rights (OCR), told Healthcare Dive.

Criticism of HIPAA came from all directions, Samuels said. On one side, healthcare providers wondered whether HIPAA might prove to be too cumbersome and expensive to comply with. On the other, patient advocates expressed concern that HIPAA wouldn't provide meaningful protections.

In the early years of HIPAA privacy protections, HHS and OCR, which was responsible for enforcing the Privacy Rule, seemed content to let noncompliant healthcare providers slide with a warning. From April 2003 to 2008, around 35,000 HIPAA privacy violations were reported, but not a single civil fine was levied against a healthcare provider.

HHS said it had worked with around 6,000 providers reported for violations to help them achieve "voluntary compliance," according to an April 2008 article in the Wall Street Journal. Their approach was to encourage "improvements that were constructive and were achieved more quickly than through imposition of monetary penalties." This approach would change with the passage of the HITECH Act in 2009.

HITECH & HIPAA

In many ways, HIPAA was ahead of its time. Although it passed before widespread adoption of EHRs, HIPAA recognized in 1996 that digitization of health data was right around the corner. One of its goals was to standardize the electronic exchange of sensitive health information. HIPAA laid the groundwork for future efforts to advance health IT and those efforts, in turn, strengthened HIPAA's privacy protections.

In many ways, HIPAA was ahead of its time. "HIPAA has transformed healthcare and healthcare delivery over the past two decades, evolving itself alongside of technology," Samuels said. "The HIPAA standards have helped pave the way for the widespread adoption of the electronic health record and the interoperability of health data."

When the HITECH Act passed in 2009, it included provisions to strengthen HIPAA privacy protections and HHS' ability to enforce them. The HITECH Act expanded compliance requirements to business associates of covered entities, required self-reporting of privacy breaches, and increased potential fines for violations to up to $1.5 million. Later that year, OCR would issue the first of many multi-million dollar fines for HIPAA violations.

HITECH changes to HIPAA were finalized in January 2013 with the release of the HIPAA/HITECH Omnibus Final Rule. "The final omnibus rule marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented," then-OCR Director Leon Rodriguez said.

Where has HIPAA fallen short?

While patients are technically afforded the right under HIPAA to access their own personal health information, this is easier said than done. "Far too often individuals face obstacles to accessing their health information, even from entities required to comply with the HIPAA Privacy Rule," Samuels wrote in a January blog post.

By accessing their own personal health information, patients could better manage chronic health conditions and help to coordinate their care. While HIPAA makes this a possibility in theory, it is much more difficult in practice.

Third parties often have more access to personal health information than patients themselves. Even worse, third parties often have more access to personal health information than patients themselves. Anonymized health data may be doled out for research purposes that do indeed help patients, but it can also be used for marketing and other commercial practices. In May 2014, the Federal Trade Commission issued a report showing how much personal health information data brokers are collecting.

Supposedly anonymized health data can also be used to connect medical records to the individuals to which they belong. In 2005, Carnegie Mellon University Professor Latanya Sweeney told the Privacy and Integrity Advisory Committee of the Department of Homeland Security that she was able to compare hospital data to voter registration rolls to identify medical records belonging to former Massachusetts Governor William Weld.

"The public has been misled and most still have no knowledge of their lack of control over their sensitive health data," Dr. Deborah Peel, founder and president of Patient Privacy Rights, told Healthcare Dive. "Today, no nation has a comprehensive map of all flows of personal health data. How can personal data possibly be secured, much less private, if we have no idea where it is or how it's used?"

HIPAA is an imperfect law, but, at 20 years old, it could mature and grow stronger. As OCR Director Samuels said, HIPAA has been a blue print for healthcare reform. At this point, it will likely be a mainstay in blue prints for healthcare reforms of the future.