HIPAA Turns 10: Analyzing the Past, Present and Future Impact

Save to myBoK

By Daniel J. Solove
Photography [in print version] by Tyllie Barbosa

Ten years ago after countless years of germination and many twists and turns, the HIPAA Privacy Rule finally became effective. It would soon be followed by the HIPAA Security Rule-which was published in 2003 and became effective in 2005-and eventually by the HIPAA Enforcement Rule and the Breach Notification Rule as well.

HIPAA's length compares to that of a Tolstoy novel-since it contains some of the most detailed and comprehensive requirements of any privacy and data security law. When the HIPAA regulation initially went into effect, it generated significant skepticism, confusion, and even angst. Many in the healthcare industry asked: Would it be possible to provide efficient healthcare and comply with all of HIPAA's requirements? What did protecting the confidentiality of protected health information mean? How would HIPAA be enforced? Would HIPAA interfere with the relationships between patients and healthcare providers?

Skeptics wondered whether HIPAA might prove to be too cumbersome and expensive to comply with. Some were concerned that HIPAA wouldn't provide meaningful privacy protection. Others worried that HIPAA would be redundant with state health privacy laws and would not add much value. People questioned whether HIPAA would really make an impact, and if any impact would be for the better or the worse.

Ten years later these questions have largely been answered. HIPAA has evolved during the past decade and was greatly fortified by the 2009 HITECH Act and its HIPAA modification regulations released in January 2013. Whatever one might think about HIPAA, it is hard to dispute that it has had a vast impact on patients, the healthcare industry, and many others over the last 10 years-and will continue to shape healthcare and HIM professionals for many more years to come.

HIPAA's Difficult Genesis

The Health Insurance Portability and Accountability Act (HIPAA) is a law that was passed in 1996, designed primarily to modernize the flow of health information. At the time, most medical records were in paper form, but it was becoming clear that health data would become digital in the future.

The challenge of protecting privacy and security of health information was staggering in 1996, as it can be today. Countless people must have access to a person's health data: doctors, nurses, technicians, clerical workers, and administrative staff, as well as the third party personnel in entities involved in healthcare such as health plans, medical supply companies, billing and coding companies, pharmacies, and researchers.

Prior to 1996, there was no federal law regulating the privacy of health information. Even though many other countries at the time regulated personal privacy broadly and uniformly, the United States' privacy regulation consisted of a series of differing, industry-specific laws. Since the 1970s, Congress had been passing a number of privacy statutes that protected driver license records, cable TV records, school records, and phone records. There was even a federal law regulating the privacy of video rental records-but not one regulating the privacy of health records. Congress eventually decided something needed to be done to better protect people's most sensitive information-their health records. But because the individuals and entities that collect, use, and disclose health data are staggering in number and variety, having one regulation to rule them all would be no easy feat.

HIPAA's goal was to create a set of uniform electronic healthcare transaction codes. Privacy was naturally a major concern with the changes contemplated in HIPAA, and it was a challenging issue, so Congress punted to the Department of Health

and Human Services (HHS) to propose regulations to protect the privacy of health. HHS answered by proposing a privacy regulation that was finalized in 2000.

Prominent Healthcare Officials Comment on HIPAA's Past, Present, and Future

Looking back, the past 10 years have demonstrated, much to the surprise of many, the enduring nature of the basic cornerstones of HIPAA. These common sense standards were intended to provide a scalable, flexible framework so that all organizations across the industry-large and small, provider and health plan-could find their way toward compliance.

Whereas many thought HIPAA would "bankrupt" healthcare, shut down research, and otherwise paralyze the industry, instead the industry has learned the benefits of the transaction and code set standards through the ease of electronic transactions. And the balance of the [HIPAA] Privacy and Security protections have paved the way to real benefits for consumers through greater access to quality care.

Enforcement has matured along with industry knowledge and capacity to meet the standards. Early on, we placed an emphasis on learning and helping covered entities weave compliance into the fabric of treatment, payment, and healthcare operations. The HITECH Act brought a stronger enforcement arm to the HIPAA Privacy and Security Rules, resulting in $14,883,345 in resolution amounts and monetary penalties to date. Tools such as breach notification and audit are achieving our twin objectives of increasing public transparency and accountability of covered entities and their business associates.

On the patient side, who would have thought that giving people the right of access to their health information would prove so powerful? Today, that right has become a critical component to reinventing healthcare delivery: involving patients directly in the management of their treatment in an ever-expanding digital age.

HIPAA has improved patient access to care by delivering on a promise of privacy and security for consumers. It is my hope that the industry will continue to heed our call and adopt a culture of compliance that is essential to maintaining patient trust and public confidence.

-Leon Rodriguez, director of the US Department of Health and Human Services' Office for Civil Rights

---

If asked to name the most important healthcare changes over the past couple of decades, "growing interest in health information privacy and security" would make the list for most health information professionals. Nothing demonstrates that change more clearly than the issuance of HIPAA's Privacy Rule and security regulations.

For many of us working in covered entities, shepherding our organizations toward compliance with the regulations was a major responsibility. We analyzed the regulations, forecasted likely challenges, taught the rules and their nuances to others, and strengthened our privacy and security practices. In doing so we demonstrated, once again, the value of the HIM profession.

We discovered early on in our compliance efforts that change is a tall order, and that privacy and security compliance are a journey without end. But day by day, organization by organization, staff member by staff member, and process by process, we met tough challenges and improved our ability to safeguard protected health information.

When we started this journey, the scope of our task seemed overwhelming. Years later, we've earned the right to celebrate our progress. Yet we're mindful of problems that remain. Published statistics on privacy breaches and enforcement actions are sobering. Bad habits tend to reappear when we don't keep pushing ourselves and our colleagues to recognize that caring well for the patient requires caring well for their information.

As we enter a new HIPAA decade and review the HITECH Act's major revision of the privacy rules, let's take a look back, learn from our successes, and rededicate ourselves to taking the next big step forward in this important journey.

-Jill Callahan Dennis, JD, RHIA, principal at Crittenton Hospital Medical Center and AHIMA past president

---

Audio Extra: HIPAA Before and After journal.ahima.org

AHIMA's President reflects on the development of HIPAA's privacy regulations and the possible effects of the HITECH amendments.

The preamble to the HIPAA Privacy Rule states:

> According to the American Health Information Management Association (AHIMA), an average of 150 people "from nursing staff to X-ray technicians, to billing clerks" have access to a patient's medical records during the course of a typical hospitalization. While many of these individuals have a legitimate need to see all or part of a patient's records, no laws govern who those people are, what information they are able to see, and what they are and are not allowed to do with that information once they have access to it.

Progress was being made, but in 2001, with the change from the Clinton administration to the Bush administration, the future of the HIPAA regulation was thrown into turmoil. The Bush administration criticized the regulations and reopened the period for comments. There were rumors that the regulation might be entirely rolled back and restarted. In 2002, however, the Bush administration announced that the HIPAA Privacy Rule would go into effect, but with some significant changes. The compliance deadline was set for April 14, 2003, except for smaller health plans whose compliance date was set for a year later. In 2003 the HIPAA Security Rule was finalized and scheduled to go into effect in 2005.

Jodi Daniel, JD, MPH, director of policy and planning at HHS' Office of the National Coordinator for Health Information Technology (ONC), was a senior member of the team at the Civil Rights Division of HHS' Office of General Counsel that drafted the final HIPAA Privacy Rule, the Privacy Rule modifications, and the HIPAA Enforcement Rule. "The biggest issue was whether patient consent should be required for using PHI [personal health information] for purposes of treatment, payment, or healthcare operations," Daniel says. "When HHS asked for comments after the change in presidential administration, most of them expressed concern that the initial rule requiring patient consent for treatment, payment, and healthcare operations would be unworkable or difficult to implement. HHS listened and changed it."

Critics Cried Out Against HIPAA

Critics assailed HIPAA from all sides. Privacy advocates were disappointed that HIPAA allowed many uses and disclosures of information without patient consent. Dr. Deborah Peel, a psychiatrist and founder of the Patient Privacy Rights Foundation, was one of the most vocal critics of HIPAA. "Our existing federal privacy law is toothless," she wrote after the rule was released, allowing "more than 600,000 types of businesses and millions of their business associates to access medical records without patient consent for the 'treatment, payment and operations of health-care related activities'… How can anything possibly be private with this type of loophole?"[1] Many of HIPAA's requirements were already required by state law, some of which were even stricter than HIPAA.

Doctors complained that they wouldn't be able to have office sign-in sheets or speak to family members about each other's health. There was fear and confusion. When Daniel spoke about patient rights to access health data under HIPAA at a physician conference, the audience did more than "boo."

"Some physicians actually started yelling at me 'But these are *my* notes!'" Daniel says. "I realized that we were making some very big changes. We were changing the expectations of both patients and healthcare providers."

Penalties Light in HIPAA's Early Years

In the early years of HIPAA, organizations scrambled to comply and there was significant confusion. A lengthy article in the October 16, 2003, *USA Today* noted that thousands of providers were taking extreme measures in reaction to HIPAA-no

longer leaving voicemail messages, banning office sign-in sheets, and prohibiting the sending of appointment postcards.[2] This confusion gradually waned as the HIPAA regulations became more familiar.

In the first two years of the regulation, despite more than 13,000 privacy complaints, no civil enforcement actions were brought by the HHS' Office for Civil Rights (OCR), the entity responsible for civil enforcement of HIPAA. In that same period between 2003 and 2005 there was only one HIPAA criminal action-against a lab assistant who used the personal data of a terminal cancer patient for identity theft. By 2008, more than 33,000 complaints had been filed with OCR, of which about 8,000 were investigated. Despite the fact that about 5,600 investigations led to entities taking corrective action, no fines had yet been issued. Critics assailed OCR for not adequately enforcing HIPAA.

"Early on, the philosophy toward enforcement was that HHS wanted to protect privacy without interfering with appropriate information flow or treatment of patients," Daniel says. "The goal was to help covered entities understand it and get it right. HHS didn't want to play gotcha."

What Does HIPAA Require?

HIPAA regulates "covered entities" that consist of healthcare providers, plans, and clearinghouses that process health data in the electronic format specified in the HIPAA statute. With the release of the HITECH-HIPAA modifications, HIPAA also now covers "business associates" or entities that contract with covered entities and that receive, use, and process protected health information (PHI).

The HIPAA Privacy Rule governs PHI, which is any "individually identifiable health information"-a broad definition including paper records. The HIPAA Security Rule is narrower, applying only to "electronic" PHI, or e-PHI.

From a bird's eye view, the key aspects of HIPAA include:

- **Privacy Program.** HIPAA mandates that covered entities designate a privacy official to develop and implement policies for protecting privacy and handle questions and complaints. HIPAA also requires training of personnel.
- **Limitations on Disclosure and Use.** HIPAA requires that people authorize disclosure of their PHI unless an exception applies, such as a legal requirement or to report abuse, or for treatment, payment, or healthcare operations. The "minimum necessary rule" requires that only the minimum necessary PHI be accessed and used.
- **Patient Rights.** HIPAA provides a set of rights to patients, including a right to be given a notice about the privacy practices of a covered entity, a right to access PHI, and a right to file a complaint alleging a HIPAA violation without retaliation.
- **Security Safeguards.** For e-PHI, the HIPAA Security Rule provides a detailed series of administrative, physical, and technical requirements.
- **State Law.** HIPAA did not preempt stronger state law protections, so any more protective state law remains in effect.

The HHS' Office for Civil Rights (OCR) is responsible for the civil enforcement of HIPAA. There are also criminal penalties for certain wrongful disclosures of PHI. However, HIPAA does not have a private right-of-action, meaning that people whose HIPAA rights are violated cannot sue for damages-though they can still sue if state law is violated.

HIPAA Gets Teeth with HITECH Act Regulations

Over the next several years HIPAA began to embed in the everyday practices of providers and healthcare staff. HIM professionals found a new career avenue as healthcare facilities developed new roles like privacy and security officers, who were hired to ensure HIPAA compliance. But just as the industry got used to the regulations, HIPAA enforcement and compliance changed in a dramatic way after 2009. As part of the American Recovery and Reinvestment Act (ARRA), Congress passed in 2009 the Health Information Technology for Economic and Clinical Health Act (HITECH). The HITECH

Act greatly strengthened HIPAA by dramatically increasing the penalties for HIPAA violations-up to $1.5 million for a violation in certain circumstances. The HITECH Act included the first federal data security breach notification requirement, and also required HHS to conduct HIPAA privacy and security audits. The act also authorized HIPAA enforcement by states' attorneys general.

With newfound leverage, OCR began to ratchet up HIPAA enforcement in dramatic fashion. For example, in 2009 OCR settled with CVS Caremark for $2.25 million for failure to properly dispose of PHI. In 2011, OCR fined Cignet Health Center $4.35 million for a HIPAA violation and its corresponding failure to cooperate with OCR's investigation. In 2012, HHS settled with the Alaska Department of Health and Social Services, which agreed to pay a $1.7 million fine for an incident involving the theft of a USB drive. This was the first settlement with a state agency, and it turned heads since many didn't expect HHS to focus on state agencies. Additionally, in 2012, OCR settled with Phoenix Cardiac Surgery for $100,000. This small physician group had posted appointments on a publicly available online calendar and failed to have adequate privacy and security policies and procedures, document training, or conduct a risk analysis. The high fine for a small practice group sent a powerful message that anyone could be subject to OCR enforcement. HHS also settled with Blue Cross Blue Shield of Tennessee for $1.5 million for HIPAA violations involving 57 unencrypted hard drives that were stolen from a call center.

Experts have noted the significance of the shift in OCR's enforcement strategy, including Marcy Wilder, co-director of Hogan Lovells' Global Privacy and Information Management practice. "After years of voluntary compliance and corrective action plans, OCR is imposing significant monetary penalties for HIPAA violations," Wilder says. Susan Lucci, president of Privacy Officer Services, LLC and the 2013 AHIMA co-chair of the Privacy and Security Practice Council, also observes that "one of the most notable changes in HIPAA over the last decade has been in enforcement." Non-compliance can result in a "serious financial impact and reputational loss," Lucci says.

HITECH-HIPAA Final Rule Released

In January 2013, after years of industry anticipation, HHS issued the final regulation implementing the HITECH Act's HIPAA modifications. According to OCR Director Leon Rodriguez, the rule "marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented."

One of the most notable changes was expanding HIPAA to be directly applicable to business associates. Subcontractors of business associates receiving or processing PHI were also deemed to be "business associates." Previously, business associates were governed by their contract with a covered entity, but after HITECH's HIPAA modification, they are now subject to HIPAA sanctions and enforcement. "Moving to hold business associates to the same high standard as covered entities is a huge step in the direction to protect patient privacy," Lucci says. This is because more than 20 percent of all the breaches reported on the HHS website "known as the 'wall of shame'" are caused by business associates, she says. "This equates to over 12 million patients who have had their information at risk due to an organization outside of the healthcare organization itself," Lucci says.

The changes made by the HITECH Act to HIPAA will usher in a new level of compliance, according to Rebecca Herold, a longtime information security and privacy expert and CEO of The Privacy Professor. Herold notes that when many covered entities saw no sanctions were being applied for non-compliance by OCR, many "became much less concerned with implementing the Security Rule requirements" and "have not updated any of their privacy polices since they were first established back in 2002 or 2003." Business associates were generally not concerned with HIPAA beyond simply having the business associate agreement in place, she says. However, today many in the healthcare industry are beginning to realize the importance and seriousness of HIPAA compliance.

HIPAA Timeline-Tracking Important Dates

- **August 21, 1996**
  HIPAA Passed by Congress Designed primarily to modernize health information exchange
- **2000-HIPAA Privacy Rule Finalized by HHs**
  Becomes the first federal healthcare information privacy law
- **2001-HIPAA Stalls**
  New Bush administration reopens HIPAA Privacy Rule comment period

- **2002-Bush Administration Announces Support of Modified HIPAA**
  Exceptions for "treatment, payment, and healthcare operations" added
- **2003**
  HIPAA Security Rule Finalized
- **April 14, 2003**
  HIPAA Privacy Rule Compliance Deadline
- **April 21, 2005**
  HIPAA Security Rule Compliance Deadline
- **2008-Lack of HIPAA Enforcement**
  More than 33,000 HIPAA complaints filed with OCR to date, only 8,000 investigated with no fines issued
- **February 17, 2009**
  ARRA's HITECH Act Signed into Law
  HIPAA revised to strengthen enforcement penalties, require breach notifications, and expand patient rights
- **2009-OCR Ratchets up HIPAA Enforcement**
  Some entities fined millions of dollars for privacy breaches
- **January 25, 2013**
  HITECH's HIPAA Modification Final Rule Released

HIPAA's New Era Just Beginning

With HITECH dawning a new era for HIPAA, the future of the privacy rule is wide open. Many industry experts expect HHS will be increasing its HIPAA audits in the near future, and that business associates will now be audited too. "The best advice is to implement HIPAA compliance efforts that include risk assessments, updating privacy and security policies and procedures, security incident planning, and workforce training," Wilder says.

This is done with due reason, since privacy incidents remain a problem for healthcare providers and their associates, Lucci says. "The growing number of data breaches indicates that we must do a better job of protecting PHI from theft, the leading breach incident." According to HHS' breach reporting website, as of January 2013 there were over 274 reported breach incidents due to theft-the top breach cause, accounting for 52 percent of incidents.

New issues are emerging that might require special consideration. The burgeoning use of social media by healthcare personnel is posing substantial challenges to patient privacy. HIPAA rules clearly forbid disseminating patient information on social media, but they say little about the kinds of measures healthcare providers can take to get a handle on this problem. Mobile devices and unencrypted laptops remain a great challenge to healthcare privacy and security. Lucci notes that laptops remain in the top spot for device types involved in data breaches that have currently impacted more than 2 million patients' privacy. Herold believes that HIPAA is fast becoming the "de-facto information security and privacy standard" beyond healthcare because many business associates provide services to many other industries.

The various new ways that health data can flow, and the new types of entities that may handle that data, will pose challenges in the near future, Daniel says. "It is too early to tell yet, but this shift in how data will be created, will flow, be maintained, and be accessed might require new thinking about how health information could be protected," she says.

Joy Pritts, ONC's chief privacy officer, echoes this sentiment. "People sometimes ask of HHS-'So are you finished changing the rules now?' There is no ending point. Technology is constantly changing, and there are always new challenges," she says. "Protecting the privacy and security of health information is a continuous process. HIPAA must be reassessed all the time to make sure it is working optimally."

In addition to the dynamism of HIPAA, compliance is not something that is ever completely solved. Chrisann Lemery, a HIPAA security officer and assistant privacy officer at WEA Trust Insurance, a Wisconsin-based health plan, points out that in the course of business and the ever-changing environment of healthcare, HIPAA is not a one-time implementation. "Rather it is a challenge daily to administer," she says.

After a long and contentious birth and formative years filled with confusion and growing pains, HIPAA is now entering into its second decade. With the release of the HITECH Act modifications, HIPAA is poised to enter its teens with confident enforcement powers and a renewed mission to protect patient privacy and security. Though it still has its critics, it also still has its supporters. "HIPAA's future is pretty well assured," says Deven McGraw, director of the Health Privacy Project at the Center for Democracy & Technology. "Like it or hate it, I think it's here to stay."

With the increased enforcement and auditing, as well as its increased scope, HIPAA is a force to be reckoned with. It has come out of the last decade stronger and more influential. And its influence will surely grow.

Notes

1. Peel, Deborah. "Privacy and Health Research Can Co-Exist." *Government Health IT*. April 17, 2006. http://www.govhealthit.com/news/peel-privacy-and-health-research-can-co-exist.
2. Parker, Laura. "Medical Privacy Law Creates Wide Confusion." *USA Today*. Oct. 16, 2003.

Daniel J. Solove (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 Turns 10: Analyzing the Past, Present and Future Impact" *Journal of AHIMA* 84, no.4 (April 2013): 22-28.

Driving the Power of Knowledge

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