NELSON HARDIMAN
HEALTHCARE LAWYERS

The “P” is not for Privacy: Unpacking Common Misconceptions about HIPAA

The “P” is not for Privacy:

Unpacking Common Misconceptions about HIPAA

Public perception often associates the Health Insurance Portability and Accountability Act of 1996 (HIPAA) with protecting health privacy. This perception is so pervasive that many people assume the “P” in HIPAA stands for Privacy. This widespread misconception glosses over the fact that HIPAA’s original intent was far more complex and was motived by very different concerns. While HIPAA aimed to regulate the use and disclosure of sensitive patient health information, its primary goal was to enhance the portability of this information to modernize healthcare delivery and reduce costs. This critical detail is often overlooked in public discourse surrounding HIPAA, where privacy tends to take center stage.

In recent years, however, increasing awareness of the vulnerability of health data has shined a light on HIPAA’s limitations. Interestingly, the significant threats to privacy frequently originate not from healthcare providers’ lax adherence to compliance but from external hackers, often from overseas. A case in point occurred in 2015 when the health insurance giant, Anthem, was victim to a data breach conducted by Chinese hackers. This intrusion laid bare the personal information of approximately 78.8 million individuals. Despite the presence of safeguards within HIPAA, such occurrences have regrettably become commonplace, prompting serious doubts about the efficacy of current protective measures. According to one estimate, approximately 52 million people had their private healthcare information exposed in 2022 alone.

Moreover, HIPAA has also had to grapple with the increasingly complex landscape of health information technology. A notable illustration of this complexity is Google’s Project Nightingale, a controversial data-sharing project between Google and Ascension, the second-largest health system in the U.S. The 2019 project, although technically compliant with HIPAA, drew criticism for sharing personal health information of millions of Ascension patients without their explicit knowledge or consent. This scenario demonstrates that even when large organizations are compliant with HIPAA, they may still gain access to data through means that, while lawful, can provoke serious privacy concerns.

As the cyber-landscape of healthcare continues to grow, the digital exchange of electronic health records, involving myriad stakeholders and parties, presents a constellation of vulnerabilities unseen in previous years. Reflecting on this dynamic, it’s compelling to suggest that HIPAA, nearly three decades after its implementation, has inadvertently become a relic within the healthcare ecosystem, viewed by many as overly porous and permeable. But how did we arrive at this junction?

The inception of HIPAA took place during the Clinton administration, a period when improving the “portability” of Protected Health Information (PHI) was seen primarily as an *economic* goal, and only secondarily did it relate to healthcare quality. The Act was designed to tackle issues related to job mobility and the continuity of health insurance coverage – with the goal of bolstering market efficiencies. The establishment of a framework for health data privacy and security formed just a minor piece of this complex legislative puzzle. In the dial-up Internet, pre-smartphone era of 1996, concerns about health privacy and data security were less pronounced compared to the heightened sensitivity surrounding these issues in the digitally interconnected landscape of the 2020s.

Under Title I of HIPAA, the issue of ‘job lock’ – a situation where individuals felt compelled to retain secure jobs with

reliable medical benefits rather than venturing into potentially more rewarding opportunities – was addressed. This scenario was rooted in a very real and reasonable fear of losing healthcare coverage in the stressful intermediate period of leaving one job and finding another with similar benefits. To mitigate such fears, HIPAA's Title I included provisions ensuring that individuals could retain their health insurance coverage even if they changed or lost their jobs for a substantial length of time. Furthermore, it restricted the ability of new health plans to deny coverage due to pre-existing conditions. For the drafters of Title I of HIPAA, health insurance portability was seen as the necessary grease for the wheels of the job market, designed to foster and stimulate job mobility. These concerns were also addressed independently in protections enshrined in the 2009 Affordable Care Act, which specifically dealt with preexisting conditions.

Meanwhile, Title II of HIPAA connected the concept of portability to the enhancement of governmental oversight and data accessibility. In the absence of digitization, auditing paper medical records is a laborious process demanding that investigators manually examine medical files and correlate them with billing data. The advent of digital health records streamlined the auditing process, allowing regulators and insurers to monitor transactions and detect fraudulent activities more efficiently. Title II of HIPAA also strove to standardize the electronic exchange of health information by instituting national identifiers for providers, employers, and health insurance plans. However, instead of facilitating the seamless transfer of health records across healthcare providers, this decision gave rise to various proprietary electronic information management systems such as Cerner, Epic, and Meditech. One immediate and persistent criticism of these systems is their lack of interoperability, a shortfall that contradicts the principle of "portability" and impedes effective medical communication. The organizations that pioneered the electronic health record landscape were primarily focused on safeguarding their digital fiefdoms, often extracting hefty fees for installing and managing their systems across the healthcare industry.

When the healthcare operating systems coalesce, or when Health Maintenance Organizations (HMOs), such as Kaiser Permanente, use a unified electronic system, patient care often improves. Clinicians can quickly review comprehensive patient histories, reducing the need for extended consultations and redundant information-sharing requests among specialists and primary care providers treating a common patient. Furthermore, one of the less direct yet significant benefits of digitizing health records is the enhancement of data recovery. This was starkly illustrated a decade later, when Hurricane Katrina in 2005 resulted in the devastating loss of about 400,000 medical records, highlighting the inherent vulnerabilities of paper-based health data. In a striking contrast, financial firms affected by the September 11, 2001 attacks were largely successful recovering their data from offsite backups, underscoring the resilience of digital data storage.

These concerns emphasized the urgent need for a robust electronic health information system, and led to the passage of the Health Information Technology for Economic and Clinical Health Act (HITECH) in 2009. HITECH aimed to boost the adoption and meaningful use of Electronic Health Records (EHR) by allocating considerable funding towards promoting EHR implementation. But in many ways, HITECH exacerbated the privacy concerns engendered by HIPAA. The Act aligned with the push from both private and public insurers for physicians to store an increasing amount of patient information digitally. Federal funding and private investment accelerated the growth of electronic information management systems without solving interoperability concerns or reducing labor-intensive and time-consuming data entry requirements.

A disconcerting result of this digital shift is the dramatic expansion in the number of stakeholders who have access to personal health information. The interplay between HIPAA and HITECH creates a data-driven healthcare system that potentially grants millions of healthcare professionals, insurers, IT staff, and third-party service providers the right to access PHI as part of their professional duties. Despite the stringent regulations and penalties enforced by both acts for unauthorized access or disclosure of PHI, their efficacy is diminished in our contemporary digital environment. The marked increase in data accessibility and the resulting diminution of patient privacy cannot be fully offset by existing regulations. Paradoxically, the constraints formed within the framework established by HIPAA have ignited the powder keg of today's privacy concerns.

Authors:

Harry Nelson, Managing Partner, Nelson Hardiman

Yehuda Hausman, Law Clerk, Nelson Hardiman

Nelson Hardiman LLP

NELSON HARDIMAN
HEALTHCARE LAWYERS

Healthcare Law for Tomorrow

Nelson Hardiman regularly advises clients on new healthcare law and compliance. We offer legal services to businesses at every point in the commercial stream of medicine, healthcare, and the life sciences. For more information, please contact 877.246.6423.

Please join Nelson Hardiman LLP for “California Calling: How States are Closing the Federal Gap in Consumer Healthcare Privacy,” https://us02web.zoom.us/webinar/register/WN_1cqA0lVbSX-1Gr45TNb1SA, the fourth in its five-part webinar series analyzing the history, progression, and future of healthcare privacy, on Tuesday, July 18, beginning at 12 noon PDT.

NELSON HARDIMAN
HEALTHCARE LAWYERS