HIPAA AT TWENTY-FIVE

The Evolution of Privacy Law and Its Expanding Reach

Sydney Stuart MehaffyWeber

Twenty-five years ago, privacy law was a relatively modest corner of American regulatory practice. It largely consisted of discrete, sector-specific statutes, rarely discussed outside compliance departments and seldom treated as a board-level risk. Today, privacy law is one of the most consequential and fast moving areas of regulation, touching nearly every aspect of modern business operations and legal practice. As technology has reshaped how information is created, stored, shared, and monetized, privacy law has evolved in lockstep—often reactively, and sometimes imperfectly, but consistently expanding in reach and importance. Today, privacy regulation sits squarely at the intersection of business operations, cybersecurity, litigation risk, and professional responsibility.

Few statutes illustrate this transformation more clearly than the Health Insurance Portability and Accountability Act of 1996 (HIPAA). What began as an effort to promote insurance portability and administrative efficiency has become one of the most influential privacy regimes in American law. HIPAA's reach now extends well beyond hospitals and physicians to insurers, vendors, litigation support teams, and law firms—often in ways that would have seemed implausible when the statute was first passed.

This article looks back at how privacy law has evolved over the past quarter century and examines how HIPAA, in particular, has come to shape the daily realities of clients, insurers, and practicing attorneys.

THE PRIVACY LANDSCAPE

At the turn of the millennium, U.S. privacy law was defined more by fragmentation than by coherence. Rather than a unified body of principles, practitioners navigated a collection of targeted statutes, each addressing a narrow slice of personal information:

- The Privacy Act of 1974, governing federal agencies
- The Fair Credit Reporting Act (FCRA), focuses on consumer credit data
- The Family Educational Rights and Privacy Act (FERPA), protecting educational records
- The Video Privacy Protection Act (VPPA), famously aimed at video rental histories
- HIPAA, enacted in 1996 but not fully operational until the early 2000s

What was largely absent from this landscape was a shared understanding of data as both a core business asset and a significant legal liability. A broad, unified concept of "data privacy" as we understand it today had not yet firmly taken hold. Cybersecurity rarely features in boardrooms. Compliance programs were lean. And few organizations appreciated that a single privacy failure could simultaneously trigger regulatory scrutiny, civil litigation, contractual exposure and reputational harm.

That world would not last long.

THE FORCES THAT CHANGED EVERYTHING

Several converging developments fundamentally altered the privacy landscape over the ensuing decades.

Digitization Became the Default. Paper records gave way to electronic systems, and electronically stored information became the norm across industries. Efficiency increased, but so did vulnerability. Regulatory attention followed closely behind.

Personal Data Became a Commodity. The rise of e-commerce, social media, mobile platforms, and cloud computing transformed personal information into both currency and risk. Data could be leveraged, monetized, shared—and breached.

Cyber Incidents Went Mainstream. Highly publicized breaches made clear that data security failures carried staggering financial, legal, and reputational consequences. Health care systems and insurers, in particular, became frequent targets.

Data Crossed Borders. Global data flows forced policymakers to confront inconsistencies among national privacy regimes. European developments – most notably the General Data Protection Regulation (GDPR) – began influencing U.S. expectations even without their outright adoption.

Public Expectations Shifted. Consumers increasingly demanded transparency, accountability, and meaningful control over their personal information. Privacy concerns moved from the abstract to the personal.

Together, these forces transformed privacy law from a background compliance issue into a central operational concern. In the business and insurance context, they vaulted HIPAA from a sector-specific statute to a de facto privacy and security benchmark for privacy and security practices

.

EXPANDING PRIVACY EXPECTATIONS IN THE UNITED STATES

Despite the absence of a single comprehensive federal privacy statute, the United States has seen significant expansion of privacy regulations through overlapping mechanisms.

State Privacy Laws. An increasing number of states have enacted consumer privacy statutes modeled loosely on GDPR style principles. Although many of these laws carve out HIPAA covered data, they still intersect with health care and insurance operations through breach notification requirements, vendor oversight, and data governance obligations.

Federal Enforcement Through the FTC. Relying on its authority to police unfair and deceptive practices, the Federal Trade Commission has effectively assumed the role of a national privacy regulator. Its enforcement posture reshaped expectations across industries, including health care and insurance.

HIPAA's Regulatory Maturation. HIPAA itself has evolved through successive layers of regulation, including the Privacy Rule, the Security Rule, the Breach Notification Rule, the HITECH Act, and subsequent omnibus updates. Collectively, these developments produced a robust and continuously evolving framework that reaches far beyond hospitals and physician offices.

HIPAA'S QUIET EXPANSION

HIPAA was never intended to be the backbone of American privacy law. Over time, however, it has effectively assumed that role within the business and insurance ecosystem.

Defining the Rules of Disclosure. The Privacy Rule formalized limits on the use and disclosure of protected health information (PHI) while granting individuals enforceable rights. These requirements reshaped how information flows among providers, insurers, vendors, and counsel.

Requiring Ongoing Security Judgment. The Security Rule established a flexible, risk based obligation to safeguard electronic PHI. For insurers and law firms managing large volumes of sensitive data, this obligation is both demanding and legally consequential.

Making Breaches Public. The Health Information Technology for Economic and Clinical Health Act (HITECH) introduced mandatory breach notification and significantly expanded enforcement authority. Public reporting obligations, regulatory investigations, and reputational fallout became unavoidable features of data incidents.

Bringing Business Associates into the Fold. Perhaps most significantly, HIPAA now directly regulates business associates. Law firms that handle medical records—whether in claims administration, litigation, or employment matters—are no longer peripheral participants. They are regulated entities with independent compliance obligations.

PRACTICAL IMPLICATIONS FOR CLIENTS, INSURERS AND LAW FIRMS

Clients. For client organizations handling PHI, HIPAA compliance has evolved well beyond a static checklist. Meaningful compliance now requires formal policies, workforce training, periodic risk assessments, and tested incident response plans. Technology safeguards—from encryption to access controls—are essential, not optional. Enforcement risk has increased, with investigations often lasting years even when no penalties are ultimately imposed. Reputational stakes are higher than ever.

Insurers. Insurers sit at the crossroads of health care delivery, data, and regulatory oversight. They process enormous volumes of PHI, rely on complex vendor ecosystems, and must underwrite privacy risk amid shifting enforcement standards. HIPAA compliance is now inseparable from insurers' operational and underwriting strategies.

Law firms. Law firms, particularly those in litigation and insurance defense, have experienced HIPAA's expansion acutely. Firms handling PHI are business associates subject to direct regulatory obligations. Clients increasingly demand sophisticated cybersecurity controls and documentation. Discovery involving PHI requires careful management, from protective orders to secure data transfer and storage. Ethical duties of competence and confidentiality now clearly encompass privacy and cybersecurity literacy. In practice, firms are expected to operate with security sophistication approaching that of their clients.

LOOKING AHEAD

Over the past 25 years, HIPAA has evolved from a narrow administrative statute into a defining pillar of American privacy law. In doing so, it has reshaped the obligations of clients, insurers, and legal professionals alike.

For attorneys advising clients in these spaces—or simply handling medical records in the ordinary course of practice—HIPAA compliance is no longer incidental. It is a core professional responsibility and a strategic imperative.

The next phase of privacy law will be shaped by increased use of artificial intelligence, remote care, and connected health technologies, alongside escalating cyber threats and continued pressure for privacy reform. HIPAA will remain foundational—but it will not stand still.

Sydney Stuart has been practicing law for over three decades and is a shareholder with the firm of MehaffyWeber. Sydney has an active insurance defense practice and extensive in-house and general counsel experience in both insurance and health law. She has first-chair litigated over 40 jury trials to verdict and is a credentialed and experienced mediator.

1 U.S. Department of Health & Human Services, Direct Liability of Business Associates, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/

2. U.S. Department of Health & Human Services, HIPAA Security Risk Assessment Tool, https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool.

3. IBM Security, Cost of a Data Breach Report 2024, https://www.ibm.com/reports/data-breach.

4. Marsh McLennan, Cyber Insurance Market Trends, https://www.marsh.com/us/insights/research/cyber-insurance-market-trends.html.