As the Health Insurance Portability and Accountability Act of 1996 (HIPAA) — which was a step toward greater health information privacy — turns 25, U.S. health disclosure norms are changing, with openness and sharing becoming more commonplace. For many Americans, however, health information remains among the most sensitive of categories of personal information. Although its disclosure can have notable benefits, it can also lead to embarrassment, social censure, and discrimination. Confidentiality in the provider–patient relationship may encourage people to seek medical attention and discuss their symptoms and behaviors frankly.

From the perspective of privacy rights, celebrating a single birth date for HIPAA feels wrong. HIPAA’s personal privacy and security regulations arrived neither all at once nor fully formed. Today, HIPAA is best viewed as a framework of evolving regulation that’s revised periodically in response to demands of biomedical innovation and public health in the digital age. That capacity for adaptive modification is among the greatest strengths of HIPAA and its rules — a strength lost on critics who judge HIPAA in isolation.

Signed into law by President Bill Clinton on August 21, 1996, HIPAA was heralded as the United States’ first, and sorely needed, major national health privacy statute. At a time when federal statutes regulated access to federal government files, telephone records, school transcripts, and even video-rental histories, the health care industry lacked uniform federal privacy and security standards for protecting individual health information. Promoted as a health insurance continuity and portability measure for workers losing or changing jobs, HIPAA also authorized the Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of personal health information (PHI) and the electronic health or medical record (EHR or EMR).

More than 4 years later, on December 28, 2000, HHS delivered Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule), which improved protection of informational privacy in clinical and research settings, mandating measures that are mostly invisible to patients and consumers, who now routinely sign pro forma authorizations. Under the Privacy Rule, covered entities — health plans, health care clearinghouses, and most health care providers — must protect patients’ identifiable health information from misuse and must limit sharing. With exceptions for emergencies and disasters, covered entities must obtain written permission, in plain language, under a valid HIPAA authorization before using or disclosing identifiable health information for treatment, payment, health care operations, or commercial purposes. Business associates — persons or companies that partner with covered entities to perform health care functions — must sign HIPAA contracts that explicitly permit use or disclosure of health information.

The Privacy Rule did not go into full effect for all regulated
parts until 2004. Required compliance with HIPAA’s Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) came even later. HHS delivered the final rule in 2003, but compliance dates were set for 2005 and 2006. These rules are thus not ready to celebrate their 25th birthday. In significantly shorter life spans, however, they have spawned massive changes in health industry practices and, initially, prompted myriad lawsuits — litigating, among other issues, HIPAA’s constitutionality, the extent of preemption of state laws, allowed damages, exceptions to patient-consent rules, malpractice defense attorneys’ permission to speak directly to treating physicians (“ex parte communication”), and patients’ right to personally sue covered entities (“private rights of action”).

HIPAA was not destined to be a “one and done” law. Given innovations in medical informatics, encryption, genomics, medicine, “big data” analytics, wearable health devices, and telemedicine, it’s not surprising that its requirements have been supplemented and amended several times. In 2008, President George W. Bush signed the Genetic Information Nondiscrimination Act (GINA), amending HIPAA to restrict health insurers’ and employers’ use of individuals’ genetic data. In 2009, President Barack Obama signed the Health Information Technology for Economic and Clinical Health (HITECH) Act, promoting the use of EHRs and other information technology while strengthening HIPAA and GINA.

In 2013, a new Omnibus Rule modified HIPAA, GINA, and the HITECH Act to improve their workability, effectiveness, and flexibility. This rule aimed to better balance individual rights with public health and medical research by, for example, continuing to allow access without specific patient authorization to limited data sets and deidentified patient information. The Omnibus Rule created direct liability for business associates under the Privacy and Security Rules, further restricted nonconsensual sale of PHI, allowed patients to withhold information from nonpayer health plans, and expanded patients’ rights to obtain electronic copies of health information. It also changed how covered entities may manage privacy notices, modified authorization requirements for research and disclosure of immunizations to schools, and adopted rules regarding noncompliance with HIPAA regulations due to willful neglect.

In December 2020, HHS proposed amending the Privacy Rule again to, as former HHS Secretary Alex Azar put it, “break down barriers that have stood in the way of commonsense care coordination and value-based arrangements for far too long.” The aims of the proposed new rules are “strengthening individuals’ rights to access their own health information, including electronic information; improving information sharing for care coordination and case management for individuals; facilitating greater family and caregiver involvement in the care of individuals experiencing emergencies or health crises; enhancing flexibilities for disclosures in emergency or threatening circumstances, such as the Opioid and COVID-19 public health emergencies; and reducing administrative burdens on HIPAA-covered health care providers and health plans, while continuing to protect individuals’ health information privacy interests.” The potential for HIPAA rules to be amended in response to Covid-19, contact-tracing technologies, and other emergency data sharing exemplifies the statute’s adaptability.

HIPAA thus gradually ushered in a sweeping new legal landscape for health information privacy. It slowly replaced the genteel approach to patient confidentiality, based largely on custom and trust, with a modern regime of technically regulated individual rights and responsibilities. Because of HIPAA regulations, patients and consumers are more able to understand and control how their health information is used and disclosed. Today, vehement opposition to HIPAA is unusual, and compliance is strong.

Most HIPAA violations involve unauthorized disclosures, inadequate record disposal, poor training, dishonesty, hacking, data breaches, or identity theft. The HHS Office for Civil Rights (OCR) is responsible for enforcing the Privacy Rule and, since 2009, the Security Rule. HHS receives and investigates complaints, dictates remedial measures, and imposes civil penalties on the public’s behalf. As of March 31, 2021, the OCR had received almost 260,000 HIPAA complaints and had settled or imposed civil penalties in 99 cases, resulting in more than $135 million in fines. The OCR has investigated national pharmacy chains, major medical centers, group health plans, hospital chains, and small provider offices.

HHS provides technical assistance to covered entities seeking to comply with HIPAA, and the Food and Drug Administration issues guidance on HIPAA interpretation related to drugs and devices. In addition to penalties imposed by the OCR, the Federal Trade Commission can sanction health care entities that mislead...
HIPAA and the Leak of “Deidentified” EHR Data
Kenneth D. Mandl, M.D., M.P.H., and Eric D. Perakslis, Ph.D.

The permissible sharing of patient data among health care organizations and their business associates for treatment, payment, and operations purposes has led to a torrent of electronic health record (EHR) data flowing out of health care provider silos. The Health Insurance Portability and Accountability Act (HIPAA) also permits business associates to deidentify data on behalf of a health care provider, insurance plan, or clearinghouse (so-called covered entities); once data are deidentified, the business associate may use them freely, unless it is contractually prohibited from doing so. Organizations that don’t qualify as business associates under HIPAA may also gain access to and use deidentified data sets. Such policies have enabled the rise of a multibillion-dollar industry comprising dozens of health-data aggregation companies and hundreds more companies producing tools and technologies that aggregate, link, and monetize EHR data.

This phenomenon has been amplified by the explosion of data production since the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 began promoting widespread adoption of EHRs to en-

HIPAA had not bankrupted health care, shut down research, and paralyzed industry, as critics had feared. Instead, it “paved the way to real benefits for consumers through greater access to quality care.” At 25, HIPAA is further along in paving the same important road.

Disclosure forms provided by the author are available at NEJM.org.

From the University of Pennsylvania School of Law, Philadelphia.

This article was published on June 5, 2021, at NEJM.org.


DOI: 10.1056/NEJMmp2100090
Copyright © 2021 Massachusetts Medical Society.