Office of Commissioner
Alvaro M. Bedoya

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Statement of Commissioner Alvaro M. Bedoya
Joined by Commissioner Rebecca Kelly Slaughter
Regarding Amazon.com, Inc.'s Acquisition of 1Life Healthcare, Inc.

February 27, 2023

Amazon recently acquired One Medical[1]—along with hundreds of thousands of people's health data.[2] For me, this moment serves as a reminder that U.S. privacy law is both aging and incomplete. I want to highlight some of these shortcomings, encourage Congress and other regulators to act, and remind industry that the Commission stands ready to vigorously enforce existing law.

When people cite "HIPAA," they often believe they are referring to the "Health Information Privacy Act." But that's not the name of our nation's health privacy law, nor is that law primarily elaborated in an "act," that is, a congressionally enacted statute.

In reality, "HIPAA" stands for the Health Insurance Portability and Accountability Act (HIPAA).[3] When it passed HIPAA in 1996, Congress laid the groundwork for health privacy laws through a curious gambit: Instead of spelling out all of the substantive protections that would apply in statute, Congress set a deadline for itself to pass a health privacy law and specified that if it did not meet that deadline, the Department of Health and Human Services (HHS) could proceed with rulemaking.[4] Sure enough, the deadline passed, and in 1999, HHS went ahead and proposed what is now known as the HIPAA Privacy Rule, finalizing it in 2000.[5]

---

[1] Press Release, *One Medical Joins Amazon to Make It Easier for People to Get and Stay Healthier*, AMAZON (Feb. 22, 2023), https://www.aboutamazon.com/news/company-news/one-medical-joins-amazon-to-make-it-easier-for-people-to-get-and-stay-healthier.

[2] Press Release, *One Medical Announces Results for Third Quarter 2022*, ONE MEDICAL (Nov. 2, 2022), https://investor.onemedical.com/news-releases/news-release-details/one-medical-announces-results-third-quarter-2022.

[3] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936. According to the preamble to the Act, the purpose of HIPAA is:

> [T]o amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

Id.

[4] *Id.* § 264 (codified at 42 U.S.C. § 1320d–2 note) (directing the secretary of Health and Human Services to submit standards for protecting privacy); HIPAA Privacy Rule, 45 C.F.R. §§ 164.102–.106, 164.500–.534, 160 (2023).

[5] HIPAA Privacy Rule, 45 C.F.R. §§ 164.102–.106, 164.500–.534, 160 (proposed 1999) (codified 2000) (modified 2013, 2014, 2016); *see also* Office of Civil Rights, *The HIPAA Privacy Rule*, HHS (Mar. 31, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

This is more than trivia. It means that the substance of our health privacy law was not enacted through what can be a chaotic legislative process. Instead, it was crafted pursuant to the Administrative Procedure Act, which requires federal agencies to carefully explain the reasons behind proposed regulations[6]—and gives modern audiences particularly clear insight into *why* the rules exist.

In promulgating the Privacy Rule, HHS tried to balance the need to protect privacy with beneficial *health-related* uses of data, such as medical research and the promotion of public health.[7] So, it exempted from regulation health data that has been "de-identified"—stripped of some information that could be used to link that data back to a specific person.[8]

Notably, HHS repeatedly insisted that the de-identification provision was intended to promote health. In 1999, for example, the agency wrote:

> Large data sets of de-identified information can be used for innumerable purposes that are vital to improving the efficiency and effectiveness of health care delivery, such as epidemiological studies, comparisons of cost, quality or specific outcomes across providers or payers, studies of incidence or prevalence of disease across populations, areas or time, and studies of access to care or differing use patterns across populations, areas or time. Researchers and others often obtain large data sets with de-identified information from providers and payers (including from public payers) to engage in these types of studies. This information is valuable for public health activities (e.g., to identify cost-effective interventions for a particular disease) as well as for commercial purposes (e.g., to identify areas for marketing new health care services).[9]

In formal guidance issued in 2012, it reiterated: "The process of de-identification, by which identifiers are removed from the health information, mitigates privacy risks to individuals and thereby supports the secondary use of data for comparative effectiveness studies, policy assessment, life sciences research, and other endeavors."[10] Tellingly, the agency focused on provision of health care services.

Unfortunately, when it drafted the Privacy Rule, HHS did not limit use of this de-identified data to "improving the efficiency and effectiveness of health care delivery." Rather,

---

[6] 5 U.S.C. § 553.
[7] Other Requirements Relating to Uses and Disclosures of Protected Health Information, 65 Fed. Reg. 82,461, 82,818–820 (Dec. 28, 2000) (codified at 45 C.F.R. § 164.514).
[8] 45 C.F.R. § 164.514.
[9] 64 Fed. Reg. 59,918, 59,946 (proposed Nov. 3, 1999) (codified at 45 C.F.R. § 164).
[10] *See also* HHS OFFICE OF CIVIL RIGHTS, GUIDANCE REGARDING METHODS FOR DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION IN ACCORDANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE (Nov. 26, 2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

HHS has clarified that once data is de-identified, it is *no longer covered by the Privacy Rule*.[11] Those entrusted with the data can do with it as they please, as long as they don't "re-identify" it.[12] The lack of a purpose limitation cuts against longstanding American information policy.[13] More worryingly, one of the methods the Rule sets out to de-identify data has been criticized by technology experts, because it is based on a fixed list of identifiers that will not keep pace with advances in technology.[14]

To boil down this jargon: When you hear a company tell you that they will abide by HIPAA, it does not mean that they cannot use your data for other purposes. Rather, it means they must simply remove from that data certain markers that would tie that data back to you. I think that most people would be surprised to hear that.

When HHS proposed the Privacy Rule in 1999, I doubt that it had reason to anticipate that one day the world's largest retailer—a company of profound technological sophistication—would amass people's health information on this scale. I encourage Congress to continue working toward new privacy laws and HHS to consider updating its Privacy Rule to better reflect the reality of how firms can use health data. In the meantime, the Commission has made clear through its enforcement actions that "health information" is a broader category than what is currently protected under the Privacy Rule,[15] and it will continue to closely monitor this space.

---

[11] Office of Civil Rights, *Summary of the HIPAA Privacy Rule*, HHS (Oct. 19, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/index.html ("There are no restrictions on the use or disclosure of de-identified health information.").

[12] OFFICE OF CIVIL RIGHTS, GUIDANCE REGARDING METHODS FOR DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION IN ACCORDANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE 8–9 (2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf ("If a covered entity or business associate successfully undertook an effort to identify the subject of de-identified information it maintained, the health information now related to a specific individual would again be protected by the [HIPAA] Privacy Rule, as it would meet the definition of PHI.").

[13] In 1980, the U.S. signed the OECD Privacy Guidelines, which adopted a Purpose Specification Principle for both government and commercial data. That Principle says that institutions should be up front about the purposes for which they collect personal data and not use that data in other ways. OECD, RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (Sept. 22, 1980), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.

[14] *See, e.g.*, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1702, 1738 (2010), https://www.uclalawreview.org/pdf/57-6-3.pdf.

[15] *Compare* 45 C.F.R. § 160.103, *with* Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief at 5, United States v. GoodRx Holdings, Inc., No. 23-cv-460 (N.D. Cal. Feb. 1, 2023).