Institute for Youth in Policy

Policy Media Department | Brief

5214F Diamond Heights Blvd #3055
San Francisco, CA 94109
+1 (509) 565-0545
eic@yipinstitute.org
www.yipinstitute.org

From Tracking to Selling: Protecting Privacy in Consumer Health Apps

Policy Lead: Ava Szajnuk

Policy Editors: Rishya Vemireddy, Irene Kang

Policy Analysts: Gautham Parvathaneni, Jaya Vashisth

Technology Team, Institute for Youth in Policy

[1]avaszajnuk@yipinstitute.org

Abstract: **The general population may assume that health information entered into an app has the same protections as information shared with a doctor. This brief investigates which apps and data are covered by existing laws, where gaps remain, and whether policymakers should establish federal protections specifically for health information collected by consumer apps.**

Keywords **— Consumer health technology & privacy, health data, health apps**

I. Executive Summary

Privacy regulations in the healthcare industry have been outpaced by the growing use of technology in medicine, leaving consumers subject to a variety of potentially harmful privacy breaches. Historically, the first data protections came with the Privacy Act of 1974, expanding to the creation of the HIPAA Privacy, Security, and Breach Notification Rules and the Federal Trade Commission Act. However, these laws often fall short, as most consumer health apps are not classified as "covered entities," which include healthcare providers and their business associates, under the HIPAA rules, and thus, are not subject to the rules and regulations that protect sensitive information. The Federal Trade Commission Act attempted to cover these gaps by regulating any deceptive practices in commerce, including privacy concerns and how they apply to developers of healthcare apps. Despite these efforts, the FTC ultimately rescinded its 2021 policy statement which extended the Health Breach Notification Rule to health apps, leaving this data ultimately unprotected. However, Brookings finds that many companies are not considered "covered entities" because they contract to users and not insurers, making way for the sales of sensitive data like telehealth firm Cerebral's sale to advertisement companies. In today's age of expanding technology within healthcare systems, privacy regulations have become even more sparse. With events such as the overturn of Roe v. Wade and subsequent loss of privacy protections on data, ACLU writer Shreya Tewari confirms that consumers are left drastically underprotected and confused as to how these companies are using their data. This was especially highlighted during the growing use of telemedicine during the COVID-19 pandemic, during which new forms of medicine such as telehealth calls didn't require traditional HIPAA agreements, which brought about the question of how HIPAA rules can expand to safeguard consumers and their information. This brief aims to explore potential policy avenues for closing existing gaps in the current healthcare data landscape by navigating the history and problems

© 2026 Institute for Youth in Policy

surrounding present-day regulations and where they lack.

II. Overview

Consumer health applications have expanded the collection of personal health information beyond traditional healthcare settings. Past attempts at federal regulation of health information was primarily focused on information maintained by traditional healthcare providers and institutions, rather than being built to foresee potential vendors of health information, leading to a conflict in the rise of health applications.

In 1996, the Health Insurance Portability and Accountability Act, also known as HIPAA, was enacted to establish federal privacy and security protections for individually identifiable health information. This act was designed with traditional mechanisms of covered healthcare providers, health plans, and healthcare clearinghouses in mind, meaning that future mobile application usage was not factored into its information coverage restrictions. In modern day, this leaves information collected through fitness trackers, period trackers, and other health platforms outside of the scope and protections of HIPPA. In 2009, Congress passed the Health Information Technology for Economic and Clinical Health (HITECH) Act as part of the American Recovery and Reinvestment Act. The HITECH Act strengthened HIPAA's privacy protections and directed the Federal Trade Commission (FTC) to establish breach notification requirements for vendors of personal health records and other entities outside the scope of HIPAA. Shortly after, the FTC was able to introduce the Health Breach Notification Rule to carry out this instruction.

Federal oversight of consumer health applications has subsequently expanded, however. In September 2021, the FTC issued its *Statement of Commission on Breaches by Health Apps and Other Connected Devices*, clarifying the pre-existing Health Breach Notification Rule could apply to consumer apps and connected devices previously outside of HIPAA. This statement emphasized that apps capable of collecting health information from multiple sources, such as users or wearable devices, could qualify as vendors of personal health records. It additionally clarified that unauthorized sharing of identifiable health information with third parties could constitute a reportable breach, even in the absence of a cybersecurity attack.

Though this expanded the FTC's interpretation of the scope of which companies and disclosures fell under existing requirements, it did not create a new law or act as a formal amendment. This changed, however, in April 2024, when the FTC finalized amendments to the Health Breach Notification Rule, clarifying its application to health applications and digital devices, including fitness trackers. The amendments addressed much-needed changes to the rule's definition of personal health records and unauthorized disclosures, shedding light to modern data-sharing practices and increased risk for cybersecurity breaches. The updated requirements went into effect in July 2024. Eventually, in September 2026, the FTC rescinded the 2021 policy statement, after determining that the guidance recommended within the statement had been appropriately addressed by the 2024 amendments to the Health Breach Notification Rule. While the amendments address the role of companies and their obligations after qualifying breaches or unauthorized disclosures, it does not establish comprehensive federal privacy protections of consumer health information preceding these incidents.

III. History

Over the past few decades, the relationship between healthcare and personal privacy has

undergone a significant transformation. Historically, sensitive health information was primarily collected and maintained by healthcare providers, insurance companies, and medical institutions. In fact, before 1996, there were no comprehensive federal health safety laws. Instead, patient protection relied on state statutes and medical review boards which could revoke a physician's license.

However, that all changed in 1996, when President Bill Clinton signed the Health Insurance Portability and Accountability Act (HIPAA) into law. Originally, HIPAA was primarily designed to improve public administration. Later, the HIPAA privacy rule established national standards to protect individual's health records and health information, and applied to health plans and healthcare providers who conducted transactions electronically. It also included a mandate for federal privacy standards governing health data.

The regulatory framework was quickly challenged during the expansion of technology in the late 2000s and early 2010s, as cell phones became increasingly commonplace. The introduction of this technology into the pockets of millions of Americans meant a multitude of options to track health, through features which documented things like physical activity, sleep patterns, reproductive health, and dietary habits. While they offered potential benefits for consumers, they also introduced new questions regarding data protection, consent, and consumer privacy, as they fell outside of HIPAA guidelines.

Recognizing this gap, Congress passed the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. The HITECH Act required health entities and business associates to notify affected individuals of data breaches, expanded HIPAA compliance and accountability to third-party vendors, and placed tighter restrictions on the sale of protected health information (PHI). Throughout the 2010s, the rapid development and commercialization of healthcare services made it abundantly clear how necessary these regulations were to protect the best interests of consumers.

In April 2023, Washington became the first state to address consumer health data privacy outside of HIPAA, through the My Health My Data Act (HB 1155). The legislation required that consumers acquire consent from users before sharing information with third party services. Further, it also mandated the option to deny consent or withdraw data at any time. This passage reflected a growing recognition that existing federal protections were insufficient to address rapidly shifting health technology, particularly in consumer health apps.

Most recently, at the federal level, the Federal Trade Commission (FTC) finalized changes to the Health Breach Notification Rule from 2009, clarifying that the updated rule would now apply to health applications and connected technology, expanding the definition to include unauthorized disclosures of information, modernizing existing protections to adapt to the continuously evolving digital environment.

Through these developments, one thing is clear: the privacy of consumer health information is a continuously evolving challenge, one which has historically been addressed behind new technological innovations, rather than in anticipation of them.

IV. Policy Problem

A. Stakeholders

Consumers of digital health platforms and apps are the primary stakeholders, often facing direct risk of private, identifiable health information being shared or leaked without prior consent. Patients are frequent users of health apps as a digital tool to track various aspects of health data, including: diets, lifestyle habits, sleep, mental health, menstrual health and cycles, and vital signs. The lack of regulatory guardrails

puts consumers in largely unprotected positions, with a looming risk of data being sent to third parties. Misutilization of such information may cause significant emotional distress for users and a permanent loss of trust in previously helpful apps. As the sole owners and contributors of health data information, consumers remain at the heart of data privacy threats.

The FTC plays a critical role in the enforcement of privacy laws to non-HIPAA entities, which involves third-party digital health apps. As consumer privacy protection gains increasing traction and concern, the scope of regulation falls under the FTC, shaping their role as an essential stakeholder.

Mobile health app developers and platforms hold great stake in ensuring privacy and vital data protection for users of their creations. Through app development, they are responsible for implementing security measures within apps for data privacy. With a prominent source of privacy risks and invasion stemming from unauthorized health data sharing, it becomes imperative to hold companies and platforms accountable.

B. Risks of Indifference

The risk of indifference involves the continued breach of privacy without consumer knowledge or consent, misuse of sensitive health data by third parties, and exploitation of users through targeted marketing. Around 81% of Americans report they believe their personal health data is protected under HIPAA Privacy and Security Rules, suggesting that the lack of proper consent poses a grave concern. Millions of adults across the nation utilize such apps unaware of the potential risks unregulated health data appliances present. If unauthorized and harmful access to private consumer health data is to persist, it will shape the future of health app usage, erode consumer trust, and leave millions with sensitive health data vulnerable.

C. Nonpartisan Reasoning

With nearly 313 million health app users nationwide, it is imperative to address the health data vulnerabilities associated with such apps. The benefits of eliminating health app privacy risks include but are not limited to:

1) **Protecting consumer privacy:** Most health apps are not covered under HIPAA law and jurisdiction, resulting in sensitive health data having minimal protections. Consumer privacy remains at the forefront of health app privacy prioritizations, and it remains imperative that they have the ability to opt in and out of data sharing without losing access to essential health tracking service.
2) **Preventing exploitative health data usage:** The increase in the commercialization of health data, often without the knowledge of health app users, has put consumers in a harmful position. Such exploitative uses, especially through targeted marketing based on sensitive data, can emotionally and financially harm users. Moreover, limited regulatory safeguards have resulted in health data potentially being sold or shared with third-party entities.
3) **Maintaining public trust in health data tools:** It is worth noting that many physicians and healthcare providers hesitate to recommend health app usage for patients, a primary consumer population of such technologies. While nearly 68% of physicians suggest that

health apps tracking biometrics can be extremely useful for patients aiming to implement a healthy lifestyle, many opt out of providing app recommendations. Data privacy risk has resulted in a deep-rooted mistrust in apps that may have impacts on consumers seeking a method to maintain a healthy life. Furthermore, the continued lack of accountability oversight from the FTC has exacerbated privacy issues, resulting in the erosion of public consumer trust in health apps.

V. Policy Options

Congress faces several distinct policy options when evaluating whether and how to establish federal privacy protections for health information collected by consumer-facing apps, wearables, and trackers.

The first necessitates broadening or adapting the HIPAA framework. By expanding HIPAA or creating a parallel statutory mechanism to treat consumer health data, fiduciary and privacy standards can be established that remain similar to traditional healthcare providers and insurers. According to Health Affairs Policy Research, "As in other squares of America's privacy "patchwork," HIPAA specifies a group of industry actors (health plans, provider organizations, and clearinghouses), designates them as "covered entities," and then regulates how these entities and their subcontractors (business associates) use a certain class of information (individually identifiable health information)." This essentially means that a patient's health information is only "protected" when it is recorded by one of these covered entities. A focus on a limited set of entities however, links privacy protections to a "snapshot" of the industry at one specific point in time, and that entity-based system thereby exempts an extremely fast-growing environment of health management tools. The policy recommendations that Health Affairs and their institute's research provide reiterate that defining "individually identifiable health information as an inherently protected class of data, rather than a class that is protected only when created or held by certain entities" is necessary in order to ensure that legal protections extend over and fill the gaps currently existing in the context of consumer health data. Other recommendations include creating new definitions of individually identifiable health information "custodians" and "processors," whose requirements and liability are like those of "covered entities" and associates of those entities under existing laws. In regards to consumer-led privacy protections, mandating standardized and plain-language privacy notices, and explicit informed consent requirements before health data can be collected, used, or shared adds another layer of necessitated reform.

Building upon existing FTC authority, such as enforcement under their act for unfair or deceptive practices and the FTC's Health Breach Notification Rule, would properly strengthen consumer protections using infrastructure we already have. Legislators can do this by passing legislation that explicitly bans unauthorized sales of sensitive health data. In addition to this, according to an Annals of Internal Medicine report in 2021, "Active oversight and enforcement by an unbiased party is necessary to enforce privacy protections and deter harmful uses of personal health information, including discrimination, exploitation, and stigmatization"; this perspective is a necessary professional lens into what lawmakers should do to retain consumers' right to privacy.

Rather than creating a siloed health-only rule, Congress can pass a broader baseline federal privacy law that addresses several structural questions identified by the Congressional Research Service. These include the following:

1) Whether to regulate broadly or target specific sensitive categories like health.
2) Whether to establish operator requirements or give consumers active data-portability and control mechanisms.
3) Whether federal law should preempt stricter state-level privacy laws, such as those in Washington, Nevada, or New York's Health Information Privacy Act; or, establish a federal floor.
4) Whether to include a private right of action allowing individuals to sue over violations.

Ultimately, the debate over regulating consumer health apps centers on balancing consumer autonomy with digital innovation. While maintaining the status quo leaves vast amounts of intimate user data exposed to commercial exploitation, implementing overly rigid restrictions could stifle the growth of life-saving digital health tools. Moving forward, Congress must decide whether to expand existing frameworks like HIPAA, empower the FTC with stricter enforcement tools, or pass a comprehensive federal privacy law that establishes a unified standard for sensitive data. The choice Congress makes will fundamentally redefine the boundaries of personal privacy in the digital age.

VI. Impact on Young People

Young people are the most digitally connected demographic, yet they face severe privacy vulnerabilities when using consumer health tools because mobile apps largely fall outside traditional healthcare regulations. While mobile health technologies offer critical support for youth managing chronic or sensitive health conditions, systemic data security failures, third-party data sharing, and low trust in emerging AI tools threaten their long-term privacy and engagement with the healthcare system.

To start off, high digital adoption meets a need for confidentiality. According to a Pew Research Center study in 2018, roughly 95% of U.S. teens have access to a smartphone, and 89% are online "almost constantly" or several times a day. Among young people aged 14-22, 90% go online for health information and 38% actively use health-related mobile apps. Similarly, 70% of young adults (ages 18-29) have used a health care app or website to manage their care. Furthermore, according to a National Library of Medicine mixed-methods study, "Overall, the adolescents expressed positive attitudes toward mental health apps, even though few had experience with using them. A large proportion perceived such apps as useful tools that can help them cope with normal stresses of life, which is important in order to promote well-being and prevent mental health problems." Adolescents frequently use digital health tools because they desire confidentiality, discretion and anonymity, allowing them to seek help or learn about sensitive conditions without fear of judgment from peers or parents.

As we have explored earlier in this brief, there are numerous regulatory gaps and third-party data exposures that pose risks to consumers utilizing health apps, but these areas especially impact our youth population through predatory third-party data sharing and social media integration risks. Scoping reviews, including more from the National Library of Medicine, examining health data failures show that commercial "mHealth" apps routinely lack "data protection by design." Studies of mental health and medication apps reveal that many request unnecessary device permissions. This allows developers to read, modify, or delete data as well as transmit sensitive user info (such as blood pressure, symptoms, and emotional states like anxiety) directly to third-party marketers and parent companies. As for social media integration risks, youth-oriented health interventions

increasingly blend mHealth with social media platforms (such as Instagram, Snapchat, and TikTok) to drive peer connectivity and engagement. However, routing health behaviors through commercial social networks exposes minors' sensitive health interests to behavioral tracking and algorithmic profiling. This is supported by a Journal of Pediatric Nursing review on adolescent mHealth apps, documenting this trend: "A slightly more interactive but useful blend of regularly used technology and health interventions are those incorporating teens' personal social media with newly developed mHealth apps." The authors also note that "mHealth apps use two-way feed technology and/or social media to connect users to support groups, friends, family members, and healthcare providers."

There is also a profound clinical disconnect and low trust in AI coming from providers regarding consumer health apps. While 51% of surveyed physicians are open to discussing health apps with patients, only 18% actively recommend them. Doctors cite a lack of proof regarding app accuracy, poor integration with Electronic Medical Records (EMRs) and major data security concerns, noting that the vast majority of iOS and Android health apps pose risks of data leaks to third parties. Because clinicians rarely prescribe vetted tools, young people are left to navigate an unregulated commercial app marketplace on their own.

Public polling from KFF health policy research indicates that widespread privacy anxiety is running rampant, with 75% of adults expressing concern over health apps run by private tech companies. Young adults (ages 18-29) are particularly skeptical of artificial intelligence in healthcare; only 28% trust an AI-enabled health tool to access their medical records and provide personalized health advice, and only 37% trust AI chatbots to help manage their care. Unlike stolen credit card numbers, compromised health records, which can sell for up to $100 to $1,000 on the darknet compared to $1 for credit cards, cannot be canceled or reset. For young people, a breach of mental health, reproductive, or chronic illness data creates a permanent digital footprint that can lead to lifelong identity theft, insurance fraud or social stigma.

Evidence shows that when health data breaches or privacy invasions occur, patients lose trust, withhold sensitive medical information from providers, and abandon digital health portals. For adolescents already hesitant to discuss sensitive health issues in-person, eroding trust in digital confidentiality risks deterring them from seeking necessary medical care altogether.

The key policy takeaways from a youth-oriented perspective on consumer health app privacy are numerous. Consumer health data collected by commercial apps, wearables and social-connected wellness platforms used by youth require statutory privacy protections equivalent to clinical records. Policymakers must also restrict third-party data sharing, ban unnecessary app permissions, and prohibit the monetization of youth health and wellness metrics. Given young adults' low trust in AI-driven medical advice (28%), policies should require explicit consent and strict algorithmic accountability before AI tools can ingest youth health data.

VII. Conclusions

While federal privacy frameworks, from HIPAA and the HITECH Act to the FTC's updated Health Breach Notification Rule, have evolved to address digital medicine, they remain primarily reactive and largely fragmented. By restricting strict federal protections to traditional "covered entities," current law leaves vast amounts of sensitive data generated through telehealth, fitness wearables, and reproductive or mental health apps vulnerable to third-party

monetization and breaches. Although recent FTC enforcement and pioneering state-level laws like Washington's "My Health My Data Act" signal growing momentum to hold app developers accountable, reactive breach notifications and patchwork state rules cannot replace proactive, nationwide safeguards. To truly protect consumers in an increasingly digitized healthcare landscape, lawmakers must enact comprehensive federal privacy standards that close the non-HIPAA gap, require explicit user consent before data is shared or sold, and ensure that personal health information receives consistent protection regardless of the platform used to collect it.

VIII. References

[1] Alder, Steve. 2023. "Majority of Americans Mistakenly Believe Health App Data Is Covered by HIPAA." The HIPAA Journal, July 26. https://www.hipaajournal.com/americans-mistakenly-believe-health-app-hipaa/.

[2] Alfawzan, Najd, Markus Christen, Giovanni Spitale, and Nikola Biller-Andorno. 2021. "Privacy, Data Sharing, and Data Security Policies of Women's mHealth Apps: A Scoping Review and Content Analysis." *JMIR mHealth and uHealth* 10 (5). https://doi.org/10.2196/33735.

[3] Alhammad, Nasser, Mohannad Alajlani, Alaa Abd-alrazaq, Gregory Epiphaniou, and Theodoros Arvanitis. 2023. "A Systematic Review of Patients' Perspectives on Data Confidentiality, Privacy, and Security of Mobile Health Applications (Preprint)." *Journal of Medical Internet Research* 26 (26). https://doi.org/10.2196/50715.

[4] Anderson, Monica, and Jingjing Jiang. 2018. "Teens, Social Media & Technology." Pew Research Center, May 31. https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/.

[5] Bari, Lisa, and Daniel O'Neill. 2024. "Rethinking Patient Data Privacy in the Era of Digital Health | Health Affairs Forefront." Health Affairs Forefront. https://www.healthaffairs.org/content/forefront/rethinking-patient-data-privacy-era-digital-health.

[6] Bughdaryan, Sasun. "A Computer Keyboard with a Padlock on Top of It." *Unsplash*, June 7, 2022. https://unsplash.com/photos/a-computer-keyboard-with-a-padlock-on-top-of-it-2T4l02ZYj-k.

[7] Burggraf, Paul. 2018. "Healthcare Evolution Over the Last 25 Years: Key Changes, Lessons, and Future Trends." Thryve.Health. https://www.thryve.health/blog/healthcare-evolution-prevention.

[8] Chesnes DAD, Matthew, BE Antitrust I, and Ted Rosenbaum Acting BE Director. 2014. "Health Breach Notification Rule." Federal Trade Commission, September 19. https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule.

[9] Chesnes DAD, Matthew, BE Antitrust I, and Ted Rosenbaum Acting BE Director. 2024. "FTC Finalizes Changes to the Health Breach Notification Rule." Federal Trade Commission, April 25. https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-finalizes-changes-health-breach-notification-rule.

[10] Chesnes DAD, Matthew, BE Antitrust I, and Ted Rosenbaum Acting BE Director. 2026. "FTC Withdraws Obsolete Policy Statement." Federal Trade Commission, September 9. https://www.ftc.gov/news-events/news/press-releases/2026/09/ftc-withdraws-obsolete-policy-statement.

[11] Essén, Anna, Ariel D. Stern, Christoffer Bjerre Haase, et al. 2022. "Health App Policy: International Comparison of Nine Countries' Approaches." *Npj Digital Medicine* 5 (1). https://doi.org/10.1038/s41746-022-00573-1.

[12] Federal Trade Commission. 2021. "Statement of the Commission on Breaches by Health Apps and Other Connected Devices." September 15. https://www.ftc.gov/legal-library/browse/statement-commission-breaches-health-apps-other-connected-devices.

[13] Grundy, Quinn, Lindsay Jibb, Elsie Amoako, and Geoffrey Fang. 2021. "Health Apps Are Designed to Track and Share." *BMJ* 373 (8296): n1429. https://doi.org/10.1136/bmj.n1429.

[14] Hunter, Tatum, and Jeremy Merrill. 2022. "Health Apps Share Your Concerns With Advertisers. HIPAA Can't Stop It.." *The Washington Post*, September 22. https://www.washingtonpost.com/technology/2022/09/22/health-apps-privacy/.

[15] Høgsdal, Helene, Henriette Kyrrestad, Marte Rye, and Sabine Kaiser. 2024. "Exploring Adolescents' Attitudes Toward Mental Health Apps: Concurrent Mixed Methods Study." *JMIR Formative Research* 8 (January): e50222. https://doi.org/10.2196/50222.

[16] Iwaya, Leonardo Horn, M. Ali Babar, Awais Rashid, and Chamila Wijayarathna. 2022. "On the Privacy of Mental Health Apps." *Empirical Software Engineering* 28 (1). https://doi.org/10.1007/s10664-022-10236-0.

[17] Jesus, Douglas De. 2022. "How to Navigate Mental Health Apps That May Share Your Data | News & Commentary." American Civil Liberties Union, September 28. https://www.aclu.org/news/privacy-technology/how-to-navigate-mental-health-apps-that-may-share-your-data.

[18] kffjulianm. 2025. "KFF Health Tracking Poll: Public Use and Trust in Health Care Apps and Websites | KFF." KFF, October 24. https://www.kff.org/public-opinion/kff-health-tracking-poll-public-use-and-trust-in-health-care-apps-and-websites/.

[19] Kong, Tracie, Mary Morgan Scott, Yang Li, and Cynthia Wichelman. 2020. "Physician Attitudes Towards—and Adoption of—Mobile Health." *Digital Health* 6 (February). https://doi.org/10.1177/2055207620907187.

[20] Linebaugh, Chris, and Steve Mulligan. 2019. *Data Protection Law: An Overview*. https://crsreports.congress.gov/product/pdf/R/R45631.

[21] Lopez, Ivan. 2025. "Assessing Privacy Risks in the White House's Private Health Tracking System." Brookings, August 27. https://www.brookings.edu/articles/assessing-privacy-risks-in-the-white-houses-private-health-tracking-system/.

[22] McClain, Colleen, Michelle Faverio, Monica Anderson, and Eugenie Park. 2023. "How Americans View Data Privacy." Pew Research Center, Pew Research Center, October 18. https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.

[23] Nadrag, Paul, and Capsule Technologies. 2021. "Industry Voices—Forget Credit Card Numbers. Medical Records Are the Hottest Items on the Dark Web." Fierce Healthcare, January 26. https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web.

[24] Nass, Sharyl J., Laura A. Levit, Lawrence O. Gostin, and Institute of Medicine US Committee on Health Research and the Privacy of Health Information The HIPAA Privacy Rule. 2009. *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research.* National Academies Press (US). https://www.ncbi.nlm.nih.gov/books/NBK9576/.

[25] Office for Civil Rights (OCR). 2024. "Covered Entities and Business Associates." HHS.Gov, August 21. https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

[26] Perakslis, Eric, and Geoffrey S. Ginsburg. 2020. "Digital Health—the Need to Assess Benefits, Risks, and Value." *JAMA* 325 (2). https://doi.org/10.1001/jama.2020.22919.

[27] Pool, Javad Khazaei, Saeed Akhlaghpour, Farhad Fatehi, and Andrew Burton Jones. 2024. "A Systematic Analysis of Failures in Protecting Personal Health Data: A Scoping Review." *International Journal of Information Management* 74 (102719). https://www.sciencedirect.com/science/article/pii/S0268401223001007.

[28] Redhead, Stephen. 2025. "The Health Information Technology for Economic and Clinical Health (HITECH) Act." Congress.Gov. https://www.congress.gov/crs-product/R40161.

[29] Rockwern, Brooke, Dejaih Johnson, and Lois Snyder Sulmasy. 2021. "Health Information Privacy, Protection, and Use in the Expanding Digital Health Ecosystem: A Position Paper of the American College of Physicians." *Annals of Internal Medicine* 174 (7): 994–98. https://doi.org/10.7326/m20-7639.

[30] Scott, Karen, Deborah Richards, and Rajindra Adhikari. 2015. "A Review and Comparative Analysis of Security Risks and Safety Measures of Mobile Health Apps." *Australasian Journal of Information Systems* 19 (1). https://doi.org/10.3127/ajis.v19i0.1210.

[31] Shah, Alaap. 2026. "Epstein Becker & Green, P.C.." Ebglaw, September 11. https://www.ebglaw.com/health-law-advisor/ftc-reverses-course-on-health-app-privacy.

[32] SuperUser Account. 2021. "Putting Patients First: How HIPAA Changed the Health Information Landscape." Ahima.Org, Journal of AHIMA, May 27. https://journal.ahima.org/AMP_EDN/383/Putting-Patients-First-How-HIPAA-Changed-the-Health-Information-Landscape-2387.amp.html.

[33] Tangari, Gioacchino, Muhammad Ikram, Kiran Ijaz, Mohamed Ali Kaafar, and Shlomo Berkovsky. 2021. "Mobile Health and Privacy: Cross Sectional Study." *BMJ* 373 (8296): n1248. https://doi.org/10.1136/bmj.n1248.

[34] Theodos, Kim, and Scott Sittig. 2020. "Health Information Privacy Laws in the Digital Age: HIPAA Doesn't Apply." *Perspectives in Health Information Management* 18 (1). https://pmc.ncbi.nlm.nih.gov/articles/PMC7883355/.

[35] Theodos, Kim, and Scott Sittig. 2026. "Ahisp." Kglmeridian.Com. https://ahisp.kglmeridian.com/view/journals/phim/18/1/article-1l.xml.

[36] U.S. Department of Health & Human Services. 2024. "The HIPAA Privacy Rule." HHS.Gov, September 27. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

[37] Washington State Office of the Attorney General. 2023. "Protecting Washingtonians' Personal Health Data and Privacy." Washington State Office of the Attorney General, April 17. https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy.

[38] Wells, Charlotte, and Carolyn Spry. 2022. *An Overview of Smartphone Apps: CADTH Horizon Scan*. Canadian Agency for Drugs and Technologies in Health. https://www.ncbi.nlm.nih.gov/books/NBK595384/.

[39] Wyatt, Tami, Adaya Bayless, Patti Krauskopf, and Nan Gaylord. 2021. "Using mHealth Applications to Promote Self-Managed Health Behaviors Among Teens." *Journal of Pediatric Nursing* 59 (59): 164–72. https://doi.org/10.1016/j.pedn.2021.04.025.

[40] Wylie, Louise. 2024. "Health App Revenue and Usage Statistics (2023)." Business of Apps, September 30. https://www.businessofapps.com/data/health-app-market/.