Westlaw Today
powered by Reuters

Recent policy changes in health data privacy: Federal and state policymakers scrutinize non-HIPAA health data use

By Jodi G. Daniel, Esq., Crowell & Moring, and Allison Kwon, Crowell Health Solutions

JANUARY 29, 2024

Recent policy developments indicate that federal and state policymakers are increasingly concerned about organizations' use of individuals' health data. Specifically, policymakers are looking to further protect individuals' health data that is not currently covered under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

HIPAA serves to safeguard protected health information (PHI) by regulating the use and disclosure of such PHI maintained by covered entities, including hospitals, clinics, health care providers, pharmacies, health plans, and their business associates. Entities subject to HIPAA are held to privacy and security standards that generally are more stringent than requirements for entities outside of the health care sector.

As of October 2023, OCR settled or imposed civil money penalties in 138 cases, totaling over $137 million in addition to corrective action plans requiring various compliance actions.

Consumer use of mobile health apps, fitness trackers, wearables, and other digital health technologies (DHTs) has increased significantly in recent years, creating swaths of health information that largely remain unregulated. While direct-to-consumer mobile health apps and other DHTs may collect similar data (and in some cases, the same data) that is maintained by or on behalf of HIPAA-covered entities, data collected by many direct-to-consumer technologies are not subject to the same nationwide privacy and security standards.

Thus, health data and information collected by DHTs may be shared with third parties and used for purposes that are not permitted under HIPAA. In addition, as mentioned in the Executive Order[1] to advance "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," continued developments in health care systems and tools that use artificial intelligence (AI) raise additional questions about protecting consumer and patient privacy when deploying these technologies.

For these reasons, regulators and legislators have made it a priority to protect individuals' data as use of these technologies becomes increasingly widespread. They continue to have discussions and issue proposals to protect consumer data that is not covered by HIPAA. In this article, we summarize recent federal and state policy developments and offer recommendations to support organizations' compliance efforts.

Recent agency action

The Department of Health and Human Services' Office for Civil Rights (OCR) is responsible for developing and enforcing HIPAA privacy and security regulations. OCR investigates complaints to ensure HIPAA compliance. OCR will resolve cases via voluntary compliance, corrective action, a resolution agreement, and/or the imposition of civil money penalties (CMPs). As of October 2023, OCR settled or imposed[2] CMPs in 138 cases, totaling over $137 million in addition to corrective action plans requiring various compliance actions.

OCR recently issued guidance for covered entities and business associates, including recent guidance on the use of online tracking technologies[3] and on the HIPAA Privacy Rule and disclosures of information related to reproductive health care.[4] In 2023, OCR also issued a notice of proposed rulemaking[5] (NPRM) to modify HIPAA by prohibiting the use or disclosure of PHI to identify and take action against patients, providers and others involved in the provision of legal reproductive health care, including abortion.

In addition to OCR, the Federal Trade Commission (FTC) has begun to take a leading role in health privacy enforcement by taking actions against companies that used consumer health data not covered under HIPAA without individuals' authorization. Specifically, beginning in 2023, the FTC has taken enforcement action under section 5 of the FTC Act and the Health Breach Notification Rule (HBNR) against GoodRx, BetterHelp, and the Easy Healthcare Corporation.

The FTC identified several themes from the agency's recent enforcement actions related to health data privacy, including

clarifying its definition of health information as anything that conveys information about a consumer's health; warning companies about the use of third-party tracking technologies; and encouraging them to implement data privacy and security programs to protect health information.

The FTC has also issued a NPRM to amend the HBNR to expand its authority regarding privacy of health data not regulated by HIPAA. The NPRM proposed clarifying that the HBNR applies to health apps and other similar technologies. It also proposed that a "breach of security" encompasses unauthorized acquisitions that occur as a result of a data breach *or* an unauthorized disclosure. This includes voluntary disclosures by Personal Health Record (PHR) vendors or PHR-related entities where such disclosure was not authorized by the consumer. The FTC NPRM signals the agency's increased focus to strengthen the HBNR's applicability to non-HIPAA health information generated by apps and other direct-to-consumer technologies.

During the 2022-23 legislative cycle, at least 16 states have introduced privacy bills that address a range of issues, including protecting biometric identifiers and health data.

The FTC and OCR continue to collaborate on health data privacy enforcement and wrote a July 2023 letter[6] to approximately 130 hospitals, telehealth providers, health app developers, and other health care companies warning of the serious privacy and security risks related to the use of online tracking technologies integrated into their websites and mobile apps. The letter reminds covered entities of their responsibilities under HIPAA in addition to the FTC Act and the FTC HBNR to protect against impermissible disclosures of personal health information and states that FTC and OCR are closely watching developments in health data privacy.

Collectively, recent FTC and OCR actions demonstrate that organizations should expect agencies to remain an active regulator in the health data privacy space.

The ADPPA and congressional activity to pass a national privacy standard

In Congress, there have been ongoing discussions to enact legislation to increase oversight of sharing consumer data, including health care data. In 2022, members introduced the American Data Privacy and Protection Act (ADPPA), which would create a nationwide framework for how companies use personal data. As drafted, the ADPPA would not apply to health data already covered by the HIPAA Privacy Rule or the Health Information Technology for Economic and Clinical Health Act.

The ADPPA proposes to cover a variety of sensitive data types, including geolocation data, log-in credentials, and private communications. For the purposes of health data, the ADPPA proposes to cover "any information that describes or reveals the past, present, or future physical health, mental health, disability, diagnosis, or healthcare treatment of an individual." While the House Energy and Commerce Committee passed[7] the bill at the committee level, the ADPPA has not yet received approval for enactment.

Additionally, Senator Bill Cassidy (R-LA), Ranking Member of the Senate Committee on Health, Education, Labor and Pensions, issued last year a request for information (RFI) for stakeholder feedback to identify solutions to modernize HIPAA and ensure that health data is properly safeguarded.

The letter[8] expresses concern about the creation and collection of health data that is not covered by HIPAA and poses questions related to Congressional action to update the HIPAA framework and other legislative solutions to improve health data privacy; specific concerns regarding the use of sensitive data (e.g., genetic, biometric, and location data); privacy and security challenges related to AI; and the development of international and state-specific frameworks to regulate health data privacy. Notably, it requests stakeholder feedback on the implementation of state-level health data privacy laws in addition to ongoing federal compliance and enforcement efforts, including those from OCR and the FTC.

Enactment of state data privacy laws

State legislatures are also focused on protecting consumer health data outside the scope of HIPAA. As a result of *Dobbs v. Jackson Women's Health Organization* overturning the constitutional right to abortion, many state legislatures are moving to implement laws and regulations to protect the confidentiality of reproductive and other types of sensitive health data. During the 2022-23 legislative cycle, at least 16 states[9] have introduced privacy bills that address a range of issues, including protecting biometric identifiers and health data. Most recently, Washington, Nevada, and Connecticut have passed consumer health data privacy laws.

While state-level health data privacy laws vary in scope and content depending on the state, they generally apply to for-profit businesses operating in the state's jurisdiction, include an exemption for HIPAA-covered data, and contain specific definitions of sensitive data (e.g., reproductive, genetic, health and sexual orientation data). We expect that other states will continue to pass laws bolstering protections for consumers' health data.

Key takeaways

In the absence of a federal privacy standard, organizations that collect, maintain, and use health data not covered under HIPAA must pay close attention to the nuances of federal and state policies. Recent activity in health data privacy could pose compliance and liability risks for companies that have multistate operations — adding more complexity to an already difficult to navigate legal and regulatory environment. In order to support compliance efforts, organizations should consider the following:

- Align data use practices with current regulations and guidance: In general, organizations should hold themselves

to high privacy and security standards, including complying with HIPAA, the FTC Act, the FTC's HBNR and relevant state laws. As outlined in a recent FTC blog,[10] in order to comply with existing federal regulations, the FTC makes several recommendations to companies, including obtaining an individual's authorization electronically or in non-electronic form before making use or disclosing their data. The FTC also recommends that companies review their entire user interface and avoid making misleading or false claims (e.g., ensuring compliance with HIPAA).

Companies that collect and use health data should review recent FTC activity and guidance and assess how the company's practices fit within these new standards being defined by the FTC. It is critical for any company gathering and using health data to evaluate previous guidance and assess how the organizational practices fit within standards defined by regulators. Organizations should also designate a compliance and privacy officer who will serve as the primary responsible official for ensuring compliance and seek to create a culture of compliance that proactively addresses risks and identifies vulnerabilities.

- Assess data usage and current privacy compliance programs: Organizations should conduct an assessment on how they collect and use health data (especially if data is shared with third parties). Organizations may want to consider how recently enacted state laws would impact privacy compliance programs. Organizations should assess use of individuals' health data to determine if their current operations will need to be adjusted to meet new compliance obligations.
- Develop and maintain robust data privacy and security programs: As recommended by the FTC, organizations should implement formalized data privacy and security programs to protect health information. Organizations' privacy and security programs should include data protection safeguards, risk assessments, and employee training and supervision. These programs should also establish policies related to data retention, purpose, and use limitations. Organizations should have documented policies and procedures on privacy and security policies, including creating mechanisms to report complaints and suspected incidents and outlining procedures if a data breach occurs.

  The Office of the National Coordinator for Health Information Technology (ONC), in collaboration with OCR, developed a Security Risk Assessment Tool[11] to help health care providers and organizations conduct a risk assessment for their organization. This tool may be helpful to small and medium organizations while larger organizations should consider third-party certification or verification.
- Engage with legislators and government agencies: With the release of the Congressional RFIs, organizations have a unique opportunity to provide direct feedback to lawmakers about health care data privacy issues. Organizations may consider submitting comments on proposed changes to HIPAA and other health data privacy improvements, updates to current federal enforcement and compliance mechanisms, and the impact of AI development and use on health data privacy. In addition, organizations may want to consider providing comments as federal agencies continue to issue guidance on health data privacy. Organizations should continue to monitor privacy discussions at the state level and engage in legislative negotiations.

Notes

[1] https://bit.ly/48Wb2NE

[2] https://bit.ly/3HpmxkZ

[3] https://bit.ly/3O3WyDd

[4] https://bit.ly/3O86USB

[5] https://bit.ly/3HqeaFR

[6] https://bit.ly/48VBxmn

[7] https://bit.ly/3S2XmcQ

[8] https://bit.ly/47EQ44P

[9] https://bit.ly/3tQyRYv

[10] https://bit.ly/48BKcul

[11] https://bit.ly/48Gu4YE

About the authors

Jodi G. Daniel (L) is a partner at **Crowell & Moring**, where she leads the firm's digital health practice. She is also a managing director at Crowell Health Solutions, a director at C&M International, an assistant adjunct professor at the Yale University School of Medicine and a former lead policymaker at the U.S. Department of Health and Human Services. She counsels health technology companies, health care providers, health plans, life science companies and others on regulatory issues, including data access and use, privacy and security, interoperability, health information exchange, information blocking, telehealth, FDA oversight, federal reimbursement, and state law issues. She can be reached at jdaniel@crowell.com.

Allison Kwon (R) is a health care policy consultant at **Crowell Health Solutions**. She can be reached at akwon@crowell.com. Both authors are in Washington, D.C.

This article was first published on Westlaw Today on January 29, 2024.