wiley

NEWSLETTER

Federal Efforts Introduced to Protect Non-HIPAA Health Data

April 2022

Privacy In Focus®

Under federal law, much of the health data recorded from wearable devices, health care applications, and health IoT devices is beyond the reach of the Health Insurance Portability and Accountability Act (HIPAA), which protects only interactions between a "covered entity" in connection with the provision of medical services. On February 9, 2022, Sens. Tammy Baldwin (D-WI) and Bill Cassidy, M.D. (R-LA) introduced bipartisan legislation, S.3620, the *Health Data Use and Privacy Commission Act*, to establish a Commission to analyze potential threats to health care privacy.

State Attorneys General (AG) and the Federal Trade Commission (FTC or Commission) have historically used their respective authorities – under unfair, deceptive, or abusive acts and practices (UDAAP/UDAP) statutes – to ensure that health data that isn't covered by HIPAA is nonetheless protected. For example, in early 2017, the New York Attorney General investigated the privacy practices of three mobile health app developers, requiring in settlement agreements that, among other things, the developers make changes to protect consumers' privacy. And in California, the state AG reached a settlement in September 2020 with Glow, requiring the ovulation and period-tracking app to bolster its security practices. On the federal level, the FTC signaled increased scrutiny on the protection of health data with the release of its Policy Statement affirming that connected device and health app companies that collect user health data must comply with the Health Breach Notification Rule.

Authors

Antonio J. Reynolds
Partner
202.719.4603
areynolds@wiley.law

Tawanna D. Lee
Consulting Counsel
202.719.4574
tdlee@wiley.law

Practice Areas

Digital Health
FTC Regulation
Health Care
Privacy, Cyber & Data Governance
State Attorneys General

Health Data Use and Privacy Commission Act

While introducing the Health Data Use and Privacy Commission Act, the bill sponsors noted that "[d]ue to a lack of Federal guidelines and a range of different State and local rules regarding privacy protection for individually identifiable health information, there is a growing concern about the confidentiality of personal health information collected outside the context of health care delivery, payment, and the practice of medicine generally." According to the sponsors, privacy regulations promulgated under HIPAA have provided a clear baseline for covered entities and business associates covered with respect to responsibilities and enforcement; however, HIPAA "should be assessed to account for the evolution of emerging technologies, data and data management tools, and the modernization of health care delivery."

Specifically, the Commission would be charged with drafting recommendations and conclusions on "issues relating to protection of individual privacy and the appropriate balance to be achieved between protecting individual privacy and allowing and advancing appropriate uses of personal health information," including:

- The potential threats posed to individual health privacy and legitimate business and policy interests;
- The purposes for which sharing health information is appropriate and beneficial to consumers and the threat to health outcomes and costs if privacy rules are too stringent;
- The effectiveness of existing statutes, regulations, private sector self-regulatory efforts, technology advances, and market forces in protecting individual health privacy;
- Recommendations on whether federal legislation is necessary, and if so, specific suggestions on proposals to reform, streamline, harmonize, unify, or augment current laws and regulations relating to individual health privacy, including reforms or additions to existing law related to enforcement, preemption, consent, penalties for misuse, transparency, and notice of privacy practices;
- Analysis of whether additional regulations may impose costs or burdens, or cause unintended consequences in other policy areas, such as security, law enforcement, medical research, health care cost containment, improved patient outcomes, public health or critical infrastructure protection, and whether such costs or burdens are justified by the additional regulations or benefits to privacy, including whether such benefits may be achieved through less onerous means;
- The cost analysis of legislative or regulatory changes proposed in the report;
- Recommendations on non-legislative solutions to individual health privacy concerns, including education, market-based measures, industry best practices, and new technologies; and
- Review of the effectiveness and utility of third-party statements of privacy principles and private sector self-regulatory efforts, as well as third-party certification or accreditation programs meant to ensure compliance with privacy requirements.

Recommendations

Legislators are looking to encourage quick action on issues around health privacy. The bill provides that "no later than six months after the appointment of all of the Commission members, the Commission must report on its findings from the study to the Committee on Health, Education, Labor, and Pensions of the Senate, the Committee on Energy and Commerce of the House of Representatives, the Secretary of Health and Human Services, and the President." As policymakers weigh important privacy and security issues affecting the health data of Americans, they should consider:

1. Maintaining a technology "agnostic" approach that encourages innovation in consumer-facing health care technology. It is important that any future regulation not impede the beneficial uses of technologies in the health IoT ecosystem.
2. Adopting a framework that affords uniform protection for protected health information (PHI) and other non-clinical health data.