Federal Health Data Privacy Laws are Outdated

By: Abrahm Hill

Introduction

In 1963, years before the development of the internet, Justice Earl Warren stated, "The fantastic advances in the field of electronic communication constitute a greater danger to the privacy of the individual."[1] His words ring ever louder as the twenty-first-century economy becomes more and more fueled by personal data.[2]

I. Development of U.S. Healthcare Data Privacy Laws

The first data privacy law enacted in the U.S. was the Privacy Act of 1974. In part, the Act protected health records collected and maintained by the federal government.[3] However, only federal agencies were required to comply, leaving the healthcare industry largely unaffected.[4]

Then, in 1996, the federal government passed the Health Insurance Portability and Accountability Act (HIPAA) to regulate health data. HIPAA laid out comprehensive restrictions for health data privacy, giving the right of privacy to all patients.[5] Specifically, HIPAA sets restrictions on "protected health information," which is individually identifiable information about care, health condition, or payment for care. However, HIPAA does not govern "de-identified information."[6] Also, HIPAA only applies to "covered entities" and "covered entities' business associates." "Covered entities" are health plans, healthcare clearinghouses, and most healthcare providers.[7] "Covered entities' business associates" are businesses with access to or using "protected health information" when performing specified functions or services for the covered entity.[8]

Since HIPAA, the federal government has passed three other acts impacting healthcare data privacy. In 2008, Congress passed the Genetic Information Nondiscrimination Act (GINA) to regulate the collection, use, and disclosure of genetic information.[9] GINA generally prohibits health plans from using genetic information to make coverage-related decisions and employers from discriminating against employees or applicants based on genetic information.[10] In 2009, Congress passed the Health Information Technology for Clinical Health Act (HITECH) to strengthen HIPAA.[11] HITECH amended certain privacy provisions in HIPAA by redefining key terms and creating an official structure for governance of policy and standards relating to health

---

[1] Kim Theodos & Scott Sittig, *Health Information Privacy Laws in the Digital Age: HIPAA Doesn't Apply*, 18(Winter) PERSPECT HEALTH INF MANAG. 1, 7 (2021).
[2] *See* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELATIONS (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection
[3] Theodos, supra, at 2.
[4] *See id.*
[5] *See id.* at 3.
[6] Jane Thorpe & Elizabeth Gray, *Big Data and Public Health: Navigating Privacy Laws to Maximize Potential*, 130(2) PUBLIC HEALTH REP. 171 (2015)
[7] *Id.*
[8] *Id.* at 172.
[9] Theodos, *supra* note 1, at 2.
[10] *See* Thorpe, *supra* note 6, at 172.
[11] *See* Theodos, *supra* note 1, at 2.

care privacy and security.[12] Most recently, in 2016, Congress passed the 21st Century Cures Act to modernize drug development in the U.S. pharmaceutical industry.[13] Specifically, the Act addressed interoperability issues associated with data exchange and emphasized the patient's right to access their information.[14]

II. Growth of New Technologies Post-HIPAA

Since the passage of HIPAA in 1996, the world has seen an explosion in digital data. In 2000, the percent of the world's stored information that was in digital format was 25%. In 2013, more than 98% of the world's stored information was in digital format.[15] Moreover, the majority of digital data measures consumers' lives and most consumer data is health data (any data associated with users' health conditions).[16]

In the past two decades, health data has exploded through the development of new technologies. One such technological development is genealogical databases that store genetic data, such as 23andMe and Ancestry.[17] Another sector of the healthcare industry that has exploded is informatics. Informatics include patient portals, online forums, personal health records, wearables, medical Internet of Things, and mobile health applications.[18] Also under informatics are mobile medical apps that measure physiological, physical, and behavioral activities.[19]

III. Current Gaps in U.S. Healthcare Data Privacy Laws

Problematically, the federal government does not regulate these new health data technologies because Congress has not passed any new laws to protect consumer health data since HIPAA enacted. As a result, a multi-billion-dollar industry has sprung up to collect, analyze, and sell consumer data.[20]

First, third-party data brokers and Internet companies collect health data outside of HIPAA.[21] Then, they combine the health data with a wide range of personal information about consumers' daily activities, transactions, movements, and demographics.[22] This combined data is then used for predictive profiling of individual health status and sold for advertising.[23] For example, Target predicted that a customer was pregnant due to her purchasing patterns.[24]

IV. Fragmentation of Data Privacy Laws across Federal and State Levels

---

[12] *Id.*
[13] *See* Theodos *supra* note 1, at 4.
[14] *Id.*
[15] Tasha Glenn & Scott Scott Monteith, *Privacy in the digital world: medical and health data outside of HIPAA protections*, 494 CURR PSYCHIATRY REP. 1, 2 (2014).
[16] Dingyi Xiang & Wei Cai, *Privacy Protection and Secondary Use of Health Data: Strategies and Methods*, BIOMED RES INT. 1, 2 (2021).
[17] *See* Theodos, *supra* note 1, at 5.
[18] *Id.*
[19] See Glenn, *supra* note 15, at 3.
[20] *See id.* at 2
[21] *Id.*
[22] *Id.*
[23] *See id.*
[24] *See id.*

Currently, the U.S. lacks a single, comprehensive federal law to regulate the collection and use of personal data.[25] As a result, individual states have had to enact their own privacy framework to establish stricter privacy laws. For example, California passed the California Consumer Privacy Act (CCPA) to the increase privacy and security of consumer data.[26] Concerning health data, the CCPA provided opt-out options for consumers who do not want their information to be sold to third parties.[27] Furthermore, the CCPA requires third-party data brokers and Internet companies to provide detailed disclosures of how consumer data is stored.[28] In the wake of the CCPA, Colorado passed the Colorado Consumer Privacy Act[29] and nine other states have followed suit. However, U.S. privacy laws are a patchwork of often overlapping federal and state laws without a comprehensive federal data protection law.[30]

V. International Healthcare Data Privacy Laws

Countries – like Canada, China, and the European Union (EU) – have enacted comprehensive data privacy laws.[31] Canada and China both passed laws that regulate consumer health data.[32] The EU passed the General Data Protection Regulation (GDPR), essentially an upgraded version of HIPAA.[33] The GDPR requires organizations to gain explicit consent from data subjects.[34] Additionally, individuals have the right to restrict data processing and a right to data breach notifications.[35] Overall, the GDPR protects all personal data, regardless of who collects it or how it is processed.[36]

VI. Conclusion

The U.S. needs a new federal baseline data protection law. The Federal Trade Commission has continually called on Congress to enact new privacy and security laws.[37] In 2012, the Obama administration put forward a blueprint for its Consumer Privacy Bill of Rights, recognizing Americans have a right to know how information about them is collected, used, and shared by companies and government entities.[38] However, Congress never passed the Consumer Privacy Bill of Rights into law.

Ultimately, the federal government must pass a new comprehensive data privacy law with four underlying qualities: (1) cover all institutions (not just tech companies and credit-rating agencies), (2) fill the data privacy gaps within HIPAA, (3) incentivize companies to skew toward data prevention, and (4) provide ways to address the harms that result from

---

[25] *See* O'Connor, *supra* note 2, at 2.
[26] *See* Theodus, *supra* note 1, at 4.
[27] *Id.*
[28] *Id.*
[29] *See id*.
[30] *See* Thorpe, *supra* note 6, at 171.
[31] *See* Xiang, *supra* note 16, at 4.
[32] *Id.*
[33] *See* Theodus, *supra* note 1, at 5.
[34] *See* Xiang, *supra* note 16, at 4.
[35] *Id.*
[36] *See* O'Connor, *supra* note 2, at 2.
[37] *Id.*
[38] *Id.*

privacy violations.[39] Without a new federal baseline data-protection law, Americans will see further erosion to their right of privacy.

[39] *Id.*