

October 17, 2024

Chair Christina Henderson
D.C. Council Committee on Health
1350 Pennsylvania Avenue NW
Washington, D.C. 20004

Dear Chair Henderson and Members of the Committee:

Good morning, Chair Henderson and members of the Committee. Thank you for the opportunity to testify in support of Bill 25-0930, the Consumer Health Information Privacy Protection Act. My name Suzanne Bernstein, and I am Counsel at the Electronic Privacy Information Center, also known as EPIC. EPIC is an independent nonprofit research organization here in Washington, DC, established in 1994 to protect privacy, freedom of expression, and democratic values in the information age.¹

In my testimony, I will discuss why it is urgent that the Council act to protect health data privacy, provide an overview of the health data privacy risks that this bill will mitigate, and highlight two of the most important aspects of CHIPPA: the enforcement mechanisms and definition of consumer health data.

I. A Critical Moment to Protect Consumer Health Data

It is time for DC Council to act to meaningfully protect consumer health privacy. To set the stage: Congress has failed to pass a comprehensive federal privacy law, or a law specifically aimed at protecting consumer health data. States are stepping in and enacting state-level comprehensive data privacy laws to fill this gap, as well as laws specific to consumer health data like Washington State's My Health My Data Act. By passing CHIPPA, DC has the opportunity remain a leader in consumer protection and set the bar high for Congress to do the same.

Consumer health data collection has skyrocketed in recent years. The broad availability and convenience of smartphones and internet access has enabled "Americans to turn to apps and other technologies to track diseases, diagnoses, treatment, medications, fitness, fertility, sleep, mental health, diet and other vital areas[.]"² Our understanding of what constitutes health data has grown as

¹ EPIC, *About EPIC*, <https://epic.org/about/>.

² *On Breaches by Health Apps and Other Connected Devices*, Statement of the Commission, Federal Trade Commission (Sept. 15, 2021), https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_b_reaches_by_health_apps_and_other_connected_devices.pdf.

data analysts and data brokers have demonstrated their ability to infer health-related insights from a widening range of data sources.

Unbeknownst to many consumers, most of this health data collection is not regulated by HIPAA. Most of the apps, platforms, and companies that collect our most sensitive data, like direct-to-consumer genetic testing companies for instance, fall outside of HIPAA's narrow scope.³

The current gap in the regulation of consumer health data poses significant risks to consumers. The mismanagement or breach of sensitive health data can result in a range of privacy injuries, from stigma and humiliation to financial and reputational injuries. What's more, the largely unregulated data brokerage ecosystem that constantly collects, analyzes, and sells health data without consumer knowledge or consent poses stark privacy and data security risks to consumers. Data brokers sell health data, including mental health information,⁴ to willing buyers including commercial entities, health insurance companies, law enforcement, and nearly any interested individual.

In recent years, the Federal Trade Commission has ramped up its health data privacy enforcement actions,⁵ but these apply only after a privacy or data security violation has already occurred. DC has the opportunity to provide our consumers with preventative safeguards for their consumer health data, mitigating potential risks or harms before they materialize.

II. CHIPPA's Strong Private Right of Action and Consumer Health Data Definition

Turning to CHIPPA, I want to highlight two important provisions that will go a long way to protect consumers. First, CHIPPA's private right of action rightly ties into DC consumer protection law.⁶ As CHIPPA makes clear, a privacy violation should not be treated differently than any other unfair and deceptive trade practices. Individuals and groups of individuals who use these online services are in the best position to identify privacy issues and bring actions to vindicate their interests. Allowing consumers to enforce their own privacy rights preserves DC's resources, and statutory damages ensure that companies will face real consequences if they violate the law. Private rights of action are extremely effective in ensuring that the rights in privacy laws are meaningful for consumers.

³ See *Covered Entities and Business Associates*, Department of Health and Human Services (Aug. 21, 2024), <https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html>.

⁴ Joanne Kim, *Data Brokers and the Sale of Americans' Mental Health Data*, Duke University Cyber Policy Program (Feb. 2023), <https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/02/Kim-2023-Data-Brokers-and-the-Sale-of-Americans-Mental-Health-Data.pdf>.

⁵ Suzanne Bernstein, *Data Minimization: Bolstering The FTC's Health Data Privacy Authority*, EPIC (July 13, 2023), <https://epic.org/data-minimization-bolstering-the-ftcs-health-data-privacy-authority/>.

⁶ Consumer Health Information Privacy Protection Act of 2024, §3(c), as introduced on July 12, 2024 (Bill 25-0930).

Another important aspect of CHIPPA is the definition of consumer health data. The bill defines consumer health data as "personal information that is linked or can reasonably be linked to a consumer and that identifies the consumer's past, present, or future physical or mental health status."⁷ As I referenced earlier, the expansive scope of health data and health-related inferences that can be drawn from data collection require a broad definition like this one for CHIPPA's protections to be effective.

III. Conclusion

Thank you for the opportunity to speak today. EPIC is happy to serve as a resource to the Committee on these issues and plans to submit supplemental testimony before the record closes on October 31st.

Respectfully submitted,

/s/ Suzanne Bernstein
Suzanne Bernstein
EPIC Counsel

⁷ *Id.* at §2(9).