epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@epic.org
https://epic.org

April 3, 2026

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:

Thank you for the opportunity to submit testimony in support B26-0525, the Personal Health Data Security Amendment Act of 2025. Sara Geoghegan, Senior Counsel at the Electronic Privacy Information Center, or EPIC, spoke at the Committee's hearing on this bill on March 23. EPIC is an independent nonprofit research organization here in Washington, D.C., established in 1994 to protect privacy, freedom of expression, and democratic values in the information age.[1] EPIC has long advocated for comprehensive privacy laws at both the state and federal level.[2]

EPIC commends the D.C. Council's attention and effort to protecting health data, which is some of the most sensitive consumer data. For more than two decades, powerful tech companies have been allowed to set the terms of our online interactions. Without any meaningful restrictions on their business practices, they have built systems that invade our private lives, surveil our families, and gather the most intimate details about us for profit. But it does not have to be this way, and enacting this bill would be a significant step toward securing privacy for health data. The strongest way for the Council to protect health data is to implement meaningful data minimization standards that tie a business's obligations to the purpose for which data is collected, rather than for whatever purposes a company allows in its privacy policy—as is in the current bill text. EPIC strongly encourages an amendment to the bill to add robust data minimization and move away from the notice and choice regime that has failed consumers for decades.

I. The D.C. Council should act now to protect health data.

It is urgent that D.C. Council enact a health data privacy law. Congress has failed to pass a comprehensive privacy law or a law specifically protecting consumer health data. Because of this gap, states are stepping in and passing their own privacy laws, including laws like Washington State's My Health My Data, which provides similar safeguards for consumer health data as this bill.

[1] EPIC, *About EPIC*, https://epic.org/about/.
[2] *See e.g.*, Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security: Hearing before the Subcomm. on Consumer Protection & Comm. of the H. Comm. on Energy & Comm., 117th Cong. (2022) (testimony of Caitriona Fitzgerald, Deputy Director, EPIC), https://epic.org/wp-content/uploads/2022/06/Testimony_Fitzgerald_CPC_2022.06.14.pdf.

D.C. has the opportunity remain a leader in consumer protection and set the bar high for Congress down the street.

Consumer health data collection has skyrocketed in recent years.[3] 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[.]"[4] The sheer volume of health data has also grown because of companies' ability to infer health-related insights from a widening range of data sources. For example, location data can easily become sensitive health data, such as GPS data indicating that someone has visited a methadone or abortion clinic.[5]

Most people assume that this data is covered by the Health Information Portability and Accountability Act, or HIPAA, because it is health information.[6] Unfortunately, most of this health data collection is not regulated by HIPAA or any other law. Most of the apps, platforms, and companies that collect our most sensitive data, like direct-to-consumer genetic testing companies, fall outside of HIPAA's narrow scope.[7] As a result, there is a tremendous amount of health data in the hands of commercial entities that is largely unregulated.

The current gap in the regulation of commercial health data practices 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. The largely unregulated data brokerage ecosystem that constantly collects, analyzes, and sells health data without consumer knowledge or consent poses stark privacy and security risks to consumers. Data brokers sell health data, including mental health information,[8] to willing buyers, including commercial entities, health insurance companies, law enforcement, and nearly any interested individual. This commercialization of health information poses unique risks to consumers. For example, health insurance companies can purchase and use information collected by data brokers to

[3] Sara Geoghegan, et al., *Beyond HIPAA: Reimagining How Privacy Laws Apply to Health Data to Maximize Equity in the Digital Age*, EPIC at 9–18 (Jan. 2026), https://epic.org/wp-content/uploads/2026/01/EPIC-Beyond-HIPAA-Jan2026.pdf.
[4] *Statement of the Commission on Breaches by Health Apps and Other Connected Devices*, FTC (Sept. 15, 2021), https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf.
[5] Leah R. Fowler, *8th Annual Symposium: Redefining & Regulating Health Data*, 21 Hous. J. Health L. & Pol'y (Nov. 2021), https://houstonhealthlaw.scholasticahq.com/article/31471-8th-annual-symposium-redefining-regulating-health-data.
[6] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, (1996).
[7] *Covered Entities and Business* Associates, HHS (Aug. 21, 2024), https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.
[8] Joanne Kim, *Data Brokers and the Sale of Americans' Mental Health* Data, Duke Sanford Cyber Policy Program (Feb. 2023), https://techpolicy.sanford.duke.edu/wp-content/uploads/2023/02/Kim-2023-Data-Brokers-and-the-Sale-of-Americans-Mental-Health-Data.pdf.

determine healthcare rates, including eligibility and price.[9] Health, demographic, and "lifestyle" information collected from any online activity—like purchasing plus-sized clothing or posting about feeling anxious or depressed from a recent divorce—can yield inferences for predicting health costs. All of this, from the surveillance and data collection to the sale and use of health data, is largely beyond the knowledge or control of consumers.

The Federal Trade Commission has addressed health data privacy through enforcement actions,[10] but these apply only *after* a privacy or data security violation. D.C. has the opportunity to provide consumers with prophylactic safeguards for their consumer health data, preventing harms and mitigating potential risks *before* they materialize.

II. The Personal Health Data Security Amendment Act is a significant step toward protecting consumers' health data.

The Personal Health Data Security Amendment Act would be a positive step toward protecting the health data of people in the District. Three of the most important provisions from the bill are: 1) the data use limitations and transparency provisions, 2) the definition of "personal health data," and 3) the geofence prohibition.

First, the data use limitation and transparency requirements will provide consumers with more control over their health data privacy. Most of the data collection, disclosure, and processing that reveal our health conditions happen without individuals' knowledge. Transparency requirements can provide consumers with information about how their data is collected and how it may be used.

Second, the definition of personal health data is properly scoped to cover the wide range of data that can be used to make inferences about people's health. The bill defines personal health data as "any information that is reasonably linkable to an individual in connection with the physical and mental health of that individual" and includes a non-exhaustive list of examples. The expansive scope of health data and health-related inferences that can be drawn from data collection requires an appropriately broad definition for this bill's protections to be effective. This definition accurately captures health data across the online ecosystem and should not be narrowed.

Finally, EPIC commends the bill sponsor for including a geofencing provision. This geofence provision would make it unlawful to establish geofences to collect consumer health data around places where healthcare services are delivered. This is an important provision because our phones, wearable technologies, or other devices often collect and retain location information without consumer knowledge. If a person is at a hospital, or a health clinic specializing in treatments like

[9] Marshall Allen, *Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates* ProPublica (July 17, 2018), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates.
[10] 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/.

dialysis, methadone, or reproductive care, that location information can immediately become health information. D.C. consumers—and people traveling to D.C. to obtain health care—should feel safe seeking such care without the commercial surveillance apparatus tracking their every move.

III. The Personal Health Data Security Amendment Act should include data minimization principles rather than relying on an ineffective notice-and-choice framework.

EPIC strongly urges the Council to remove the notice and choice provisions in the bill that tie limitations on data collection and use to language contained in privacy policies. The notice-and-choice approach to privacy regulation simply does not work.[11] The focus on notice has led to longer and more complicated privacy policies that users do not read and could not change even if they did. Instead, businesses' obligations should be tied to the purpose for which data is collected rather than whatever companies allow in their own privacy policies. Transitioning away from the failed notice-and-choice framework and toward data minimization also takes the burden off individual people to protect their personal data and instead requires companies to be responsible handlers of the data they collect.

* * *

Privacy is a fundamental right, and it is time for business practices to reflect that reality. Self-regulation is clearly not working, and since Congress has been unable to enact comprehensive privacy protections despite years of discussion on the topic, local jurisdictions must act to protect their residents. D.C. has an opportunity this session to provide real privacy protections with the Personal Health Data Security Amendment Act.

Thank you for the opportunity to testify on this important legislation. EPIC is happy to be a resource to the Committee on these issues.

Sincerely,

/s/ *Suzanne Bernstein*
Suzanne Bernstein
EPIC Counsel

/s/ *Sara Geoghegan*
Sara Geoghegan
Director, Consumer Privacy Program & Senior Counsel

[11] Geoghegan, et al., *Beyond HIPAA*, *supra* note 3 at 13.