ACLU District of Columbia

529 14th Street NW
Ste 722
Washington, DC 20045
(202) 457-0800
www.acludc.org

Statement on behalf of the
American Civil Liberties Union of the District of Columbia
before the D.C. Council Committee on Health
Hearing on Bill 26-0525, the Personal Health Data Security Amendment Act of 2025
by
Melissa Wasser, Senior Policy Counsel
March 23, 2026

Good morning, Chair Henderson and members of the Committee. My name is Melissa Wasser, and I am a Senior Policy Counsel at the American Civil Liberties Union of the District of Columbia (ACLU-D.C.). I present the following testimony on behalf of our over 14,000 members and supporters in all 8 wards.

ACLU-D.C. supports Bill 26-0525, the Personal Health Data Security Amendment Act of 2025 and would urge the Committee to move the bill forward with some changes to strengthen the legislation. There are wide ranging reasons for valuing the protection of our health information. Beyond basic notions of choice, individual rights, and privacy from intrusion, personal health information is in urgent need of protection because it provides insight into some of the most closely held details about our personhood and lives. These details, unknowingly collected, stored, or ill-used, could result in health discrimination, economic harm, and further stigma. Individuals, therefore, should be able to know about and affirmatively consent to the uses of this especially sensitive type of information.

I. Prohibiting geofencing will prevent further tracking and targeting of individuals based on their location alone, but any exemptions for HIPAA's existing coverage should be tailored to protected health information, not entire entities.

B26-0525 takes important, targeted steps to establish protections for the personal health data of District residents, including limiting one of the greatest threats posed by the sea of data we are swimming in: abuse of our geolocation. The bill would prohibit geofencing around facilities that provide health services. The Federal Trade Commission has brought enforcement actions in the past against data brokers that collected location data through code quietly slipped into other

companies' apps. Those data brokers then marketed that location data as identifying individuals who visited internal medicine facilities, pharmacies, and infusion centers.[1] B26-0525 would prohibit using location data to track or target individuals based on their location alone.

While individuals are generally aware of the fact that federal law protects some health information, many are not aware that this protection only extends to health information shared with entities covered under the federal Health Insurance Portability and Accountability Act (HIPAA) – namely healthcare providers, healthcare plans, and similar entities. While individuals in the past shared health information with a relatively small number of entities, many of which were covered by HIPAA, individuals today often share personal health data with – or have their health data captured by – non-covered entities.

To further accommodate other important uses of health information, the Committee should ensure exemptions to accommodate HIPAA are limited to the protected health information already covered by HIPAA – not entire entities. This is crucial. Many large companies have multiple lines of business, only a small number of which may be covered by HIPAA. Exempting an entire entity based on one line of business would eviscerate protections for data collected by a retailer's *other* lines of business.

II. Consent cannot be buried in broad terms of service, and as such, B26-0525 should be amended to require clear, affirmative, specific, and unambiguous consent before an entity can sell, collect, or disclose personal health data.

B26-0525 would also require consent from a person before an entity could sell, offer to sell, collect, or disclose personal health data to a third party. However, in its current form, that version of consent is super easy to manufacture in a form that buries consent in legalese at the bottom of a nine-page document[2] or has been

---

[1] *FTC Cracks Down on Mass Data Collectors: A Closer Look at Avast, X-Mode, and InMarket*, Federal Trade Commission (Mar. 4, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/03/ftc-cracks-down-mass-data-collectors-closer-look-avast-x-mode-inmarket; *FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data*, Federal Trade Commission (Jan. 9, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.

[2] Alex Rosenblat, "During my kid's surgery, I was denied a copy of my consent form – then sent to a ghost office," The Markup (July 19, 2025, 8:00 AM), https://themarkup.org/hello-world/2025/07/19/patient-data-use.

designed to prevent you from declining.[3] In both healthcare[4] and data[5] contexts, research has consistently shown that people either do not read or do not understand consent forms. To strengthen the legislation, the bill should require clear, affirmative, specific, and unambiguous consent from a person before an entity can sell, collect, or disclose personal health data.

III. A right to deletion period should be shortened to 45 days to be in line with other states' deletion requirements.

B26-0525 would create a right to deletion, requiring entities to establish a deletion process, honor verified deletion requests within 183 days, and ensure that partners do the same. While this is a good start, more can be done to strengthen the legislation. 183 days is an extremely long period of time to honor a deletion request while data is being actively sold, shared, and used to monitor someone. Combined with the required notices and permissible extensions currently outlined in the legislation, it could be well over a year before a consumer's sensitive health data is deleted. During that time, it could be further shared or processed against the consumer's wishes. To prevent this from occurring, we urge the Committee to change this language to reflect a 45-day requirement, bringing D.C. in line with other states.[6]

IV. Conclusion

Health data protection laws serve as vital guardrails of personal information in an increasingly interconnected world. ACLU-D.C. recognizes the paramount importance of health data security and privacy, and as such, we urge the Committee to move Bill 26-0525 forward with the suggested changes included. We will also follow up with the Committee directly to discuss additional necessary changes to

---

[3] Alex R. Rosenblat, "I declined to share my medical data with advertisers at my doctor's office. One company claimed otherwise," Stat News (Apr. 7, 2023), https://www.statnews.com/2023/04/07/medical-data-privacy-phreesia/; *see also* The Indicator from Planet Money, "Ad targeting gets into your medical file," NPR (Jan. 9, 2024, 8:26 PM), https://www.npr.org/transcripts/1197960899.

[4] Parth Shah, Imani Thorton, Nancy Kopitnik, and John E. Hipskind, *Informed Consent* (Nov. 24, 2024), https://www.ncbi.nlm.nih.gov/books/NBK430827/.

[5] Jonathan A. Obar and Anne Oeldorg-Hirsch, "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services," TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465.

[6] Nearly every state comprehensive privacy law requires a response to deletion requests within 45 days. *See Time Limits for Responding to Privacy Requests*, TrueVault, https://knowledge.truevault.com/article/237-time-limits-for-responding-to-privacy-requests.

the legislation. These commonsense changes will help safeguard critical personal health data and significantly reduce the likelihood that the most private parts of our lives will end up in the wrong hands. Thank you for the invitation to testify at today's hearing, and we stand ready to help the Council strengthen these important privacy protections for the personal health data of District residents.