COUNCIL OF THE DISTRICT OF COLUMBIA
The John A. Wilson Building
1350 Pennsylvania Avenue, NW
Washington, D.C. 20004

Christina Henderson
Councilmember, At-Large
Chairperson, Committee on Health

Committee Member
Human Services
Facilities
Transportation and the Environment

Statement of Introduction
Personal Health Data Security Amendment Act of 2025
December 1, 2025

Today, I am proud to introduce the Personal Health Data Security Amendment Act of 2025, alongside Councilmembers Brianne K. Nadeau, Matthew Frumin, Anita Bonds, Janeese Lewis George, Charles Allen, and Robert White. This legislation would establish privacy protections for the personal health data of District residents. Every day, thousands of DC residents use apps, search engines, and devices to track their health, schedule medical appointments, and access critical care. At the same time, private companies can collect and share that same data with hundreds of third parties for purposes beyond the app's core functionality or disclosed third-party sharing, often without an individual's consent or

Even when health-related apps have privacy policies, they often do not fully disclose how personal health data is shared. In a study of 36 popular smartphone apps for depression and smoking cessation, only 43% of apps that sent data to Google and 50% of apps that sent data to Facebook fully disclosed these practices.[1]

As more companies continue to collect personal health data for corporate purposes, states are seeking to regulate the collection and use of personal health information by private entities. Currently, 20 states have enacted comprehensive legislation strengthening protections for personal data, and twenty additional state legislatures have introduced data privacy bills.[2]

The Personal Health Data Security Amendment Act establishes clear rules for transparency, consent, and accountability. This bill would:

- Prohibit geofencing around facilities that provide health services, preventing the tracking or targeting of individuals based on their location.
- Require controllers (the entities that determine how and why personal health data is used) to publish clear, accessible privacy policies describing what data is collected, how it is used, and with whom it is shared.
- Mandate consent before any collection, processing, or disclosure of personal health data, and allows individuals to withdraw consent at any time.
- Create a right to deletion, requiring entities to establish a deletion process, honor verified deletion requests within 183 days, and ensure that their partners do the same.

I look forward to working with my colleagues to advance this bill and provide residents with the ability to control their personal health data and privacy.



Councilmember Janeese Lewis George



Councilmember Christina Henderson



Councilmember Brianne K. Nadeau



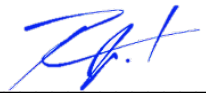
Councilmember Anita Bonds



Councilmember Matthew Frumin



Councilmember Charles Allen



Councilmember Robert White

A BILL

IN THE COUNCIL OF THE DISTRICT OF COLUMBIA

To amend Chapter 38 of Title 28 of the District of Columbia Official Code to prohibit the use of geofencing technology around entities providing in-person health care services, to prohibit the processing of personal health data by controllers without first gaining consent from a data subject, to require controllers to maintain a publicly available personal health data privacy policy, to ban the processing of personal health data in a manner inconsistent with a controller's published personal health data privacy policy, to require controllers to establish and maintain a process for the deletion of personal health data, to require controllers to delete personal health data upon request from a data subject and to notify and direct processors, affiliates, and third parties to delete such data, to require processors to notify sub-processors of a deletion request and confirm deletion in writing, and to grant data subjects the right to confirm whether a controller is processing their personal health data, to request deletion of their personal health data, and to withdraw consent from a controller.

BE IT ENACTED BY THE COUNCIL OF THE DISTRICT OF COLUMBIA, That this act may be cited as the "Personal Health Data Security Amendment Act of 2025".

Sec. 2. Chapter 39 of Title 28 of the District of Columbia Official Code is amended as follows:

(a) The table of contents is amended by adding a new subchapter designation to read as follows:

"Subchapter V. Personal Health Data Security.

"28-3881. Definitions.

"28-3882. Personal health data security protections.".

(b) A new subchapter V is added to read as follows:

"Subchapter V. Personal Health Data Security.

"§ 28-3881. Definitions.

"For purposes of this subchapter, the term:

"(1) "Affiliate" means an entity that controls, is controlled by, or is under common control with another entity.

"(2) "Control" means ownership or the power to exercise a controlling influence over the management or policies of an entity.

"(3) "Controller" means a person, organization, entity, or affiliate that determines the purposes and means of processing personal health data, which includes how and why personal health data is collected, shared, disclosed, used, and stored.

"(4) "Data subject" means an individual who is identified or identifiable, directly or indirectly, through their personal health data, including byname, identification number, online identifier, location data, or other factors specific to the individual's physical or mental health, reproductive or gender-affirming care status, or biometric information.

"(5) "Deidentified data" means information that cannot reasonably be used to infer information about, or otherwise be linked to a particular individual, household, or device.

"(6) "Geofence" means technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, Wi-fi data, or any other form of spatial or location detection to establish a virtual boundary or to locate an individual within a virtual boundary 2,000 feet or less from the perimeter of a specific physical location.

"(7) "Personal health data" means any information that is reasonably linkable to an individual in connection with the physical or mental health of that individual, including:

"(A) Medical records, histories, or diagnoses;

"(B) Genetic information, biometric data, or other physiological indicators;

"(C) Prescription and medication information;

"(D) Laboratory test results;

"(E) Health insurance, billing, or payment records related to health care or services; and

"(F) Any information collected by a health care provider, health plan, or legal entity regarding the individual's health status, care, or related payments.

"(8) "Process" means an operation or set of operations performed on personal health data, including the collection, use, access, sharing, sale, monetization, analysis, retention, creation, generation, derivation, recording, organization, structuring, storage, disclosure, transmission, disposal, licensing, destruction, deletion, or modification of personal health data.

"(9) "Processor" means any person, organization, entity, or affiliate that processes personal health data on behalf of a controller but does not independently determine the purposes or means of processing.

"(10) "Sell" means to transfer personal health data to a third party for monetary value or other forms of consideration. The term "sell" does not include the transferring of personal health data to a third party as part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.

"(11) "Sub-processor" means a person or entity engaged by a data processor to process personal data on behalf of a data controller.

"(12) "Third party" means a person or entity, other than the individual who is the subject of the personal health data, a controller, or a processor, that receives, obtains, or otherwise accesses personal health data for the third party's own independent purposes.".

"§ 28-3882. Personal health data protection procedures.

"(a) No person or entity may implement a geofence around a location that provides in-person health care services where the geofence is used to:

"(1) Identify or track individuals seeking health care services;

"(2) Collect personal health data; or

"(3) Send notifications, messages, or advertisements to individuals related to their personal health data or health care services.

"(b) A controller that enters into an agreement with a processor to process personal health data on behalf of the controller shall:

"(1) Maintain a health data privacy policy thar clear and conspicuously discloses:

"(A) The categories of personal health data collected;

"(B) The purposes for which the personal health data is collected, including how the data will be used;

"(C) The categories of sources from which the personal health data is collected;

"(D) The categories of personal health data that are shared;

"(E) A list of the categories of third parties and the specific affiliates with whom the controller shares the personal health data, whether actively or passively, and the purposes for such sharing;

"(F) The length of time the controller intends to retain each category of personal health data, or if that is not possible, the criteria used to determine that period; and

"(G) How an individual can exercise the rights provided in subsection (d) of this section; and

"(2) Limit access to personal health data to individuals or entities who need it to:

"(A) carry out the purposes for which the data subject gave consent; or

"(B) provide a product or service requested by the data subject.

"(c) A controller may not:

"(1) Sell or offer to sell personal health data without the data subject's affirmative consent;

"(2) Collect or disclose personal health data for a purpose not reasonably necessary to provide a product or service requested by the data subject without obtaining consent;

"(3) Retaliate against or deny services to a data subject for exercising rights provided under this section;

"(4) Fail to delete personal health data upon verified request from the data subject;

"(5) Contract with a processor to process personal health data in a manner inconsistent with the controller's privacy policy; or

"(6) Disclose personal health data to a third party unless the disclosure is consistent with the controller's published policy and the data subject's consent.

"(d) Data subjects may exercise the right to:

"(1) Confirm whether a controller is processing personal health data in relation to the data subject;

"(2) Withdraw consent that was once given to a controller to process personal health data at any time for whatever reason; and

"(3) Request to delete personal health data that is associated with the data subject within the database of the controller and any other legal entity whom the controller disclosed the personal health data to, except to the extent necessary to comply with the controller's legal obligations.

"(e) Each controller shall establish, maintain, and make publicly available a secure and accessible process by which a data subject may request the deletion of their personal health data. The deletion process shall:

"(1) Allow a data subject to submit a request electronically and, where applicable, through the interface the data subject regularly uses to access the controller's product or service;

"(2) Include commercially reasonable methods for authenticating the identity of the requesting data subject;

"(3) Provide a mechanism for a data subject to track the status of their deletion request; and

"(4) Establish internal procedures for promptly transmitting verified deletion requests to all processors and third parties with whom the controller has shared the data.

"(f) Upon receiving a valid request for data deletion from a data subject, the controller shall:

"(1) Delete the personal health data of the data subject from all systems within its possession or control, including active databases, archived storage, and backup systems within 183 days, unless retention is required by District or federal law; and

"(2) Notify all processors, affiliates, and third parties to whom the controller has disclosed the personal health data of the data subject's deletion request and direct each to delete such data in accordance with this subchapter within the preceding 24 months, unless retention is required by District or federal law; or

"(3) Where deletion within 183 days is not feasible, the controller shall, within that period, submit a written explanation to the Office of the Attorney General identifying the reason for the delay, the data retained, and any other relevant information.

"(g)(1) Each processor who is notified by a controller of a deletion request pursuant to subsection (f) of this section shall, in turn, notify all sub-processors engaged in processing the data of the deletion request and ensure deletion is completed and confirmed in writing to the controller.

"(2) Processors and third parties shall complete deletion within 120 days of receiving the controller's direction and shall confirm deletion in writing to the controller.

"(h)(1) A controller shall respond to a verified deletion request within 183 days of receipt of the request.

"(2) The controller may extend the response period once for an additional 60 days when reasonably necessary, taking into account the complexity and number of requests. Any such extension shall be communicated to the data subject within the initial 183-day period, including the reasons for the delay.

"(3) A controller shall provide information in response to a deletion request at least twice during any 12-month period.

"(h)(1) The controller shall take reasonable steps to authenticate the request for data deletion promptly and shall not use authentication procedures to delay compliance with this section.

"(2) If a controller is unable to authenticate a data subject's request for data deletion using commercially reasonable efforts, the controller shall not required to comply with the request and may request that the data subject provide additional information reasonably necessary to authenticate the individual and the request.

"(3) In the event that a controller determines that a data subject's requests for deletion are excessive or repetitive, the controller may:

"(A) Charge a reasonable fee to cover administrative costs; or

"(B) Decline to act on the request; provided, that the controller bears the burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of the request.

"(4) Controllers shall maintain written documentation of all deletion requests, actions taken, and confirmations received for at least two years for inspection by the Office of the Attorney General.

"(i)(1) The Office of the Attorney General shall have exclusive authority to enforce the provisions of this subchapter.

"(2) The Attorney General may investigate alleged violations of this act, issue subpoenas, compel the production of documents or testimony, and bring a civil action in the Superior Court of the District of Columbia to:

"(A) Enjoin further violations of this subchapter;

"(B) Obtain restitution or other appropriate relief for individuals whose personal health data was processed in violation of this subchapter; and

"(C) Seek civil penalties of not more than $10,000 for each violation, or such other amount as the court deems just and reasonable.

"(m) The Office of the Attorney General, pursuant to § 2-501 *et seq*., shall issue rules to implement the provisions of this subchapter.

Sec. 3. Fiscal impact statement.

The Council adopts the fiscal impact statement in the committee report as the fiscal impact statement required by section 4a of the General Legislative Procedures Act of 1975, approved October 16, 2006 (120 Stat. 2038; D.C. Official Code § 1-301.47a).

Sec. 4. Effective date.

This act shall take effect following approval by the Mayor (or in the event of veto by the Mayor, action by the Council to override the veto) and a 30-day period of congressional review as provided in section 602(c)(1) of the District of Columbia Home Rule Act, approved December 24, 1973 (87 Stat. 813; D.C. Official Code § 1-206.02(c)(1)).