Chairman Phil Mendelson
at the request of the Attorney General

A BILL

IN THE COUNCIL OF THE DISTRICT OF COLUMBIA

To require regulated entities that collect consumer health data to have a consumer health data privacy policy containing specific information about its collection, use and sharing of consumer health data and post it on the home page of their website, to prohibit regulated entities from contracting with processors, affiliates, or third parties to process consumer health data in a manner inconsistent with the policy, to require regulated entities to obtain consumer consent before collecting consumer health data after providing the consumer with requests for consent containing specified information, to limit a regulated entity's collection and sharing of consumer health data to the purposes contained in the consumer's consent, to establish a consumer's right to obtain information about consumer health information collected and shared, to withdraw consent for collection and sharing, and to obtain deletion of information collected and shared, to require a valid consumer authorization before consumer health data may be sold, to prohibit the establishment of geofences around places where health services are delivered under specified circumstances, to make violations of this act unfair and deceptive trade practices, and to exclude certain types of data collection and data sharing from the operation of the act.

BE IT ENACTED BY THE COUNCIL OF THE DISTRICT OF COLUMBIA, That this act may be cited as the "Consumer Health Information Privacy Protection Act of 2024".

Sec. 2. Definitions

For the purposes of this act, the term:

(1) "Abortion" means the termination of a pregnancy for purposes other than producing a live birth.

(2) “Affiliate” means a legal entity that shares common branding with another legal entity and controls, is controlled by, or is under common control with another legal entity. For purposes of this definition, “control” or “controlled” means:

(A) Ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a company;

(B) Control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or

(C) The power to exercise controlling influence over the management of a company.

(3) “Authenticate” means to use reasonable means to determine that a request to exercise any of the rights afforded in this act is being made by, or on behalf of, the consumer who is entitled to exercise such consumer rights with respect to the consumer health data at issue.

(4) “Biometric data” means data that is generated from the measurement or technological processing of an individual’s physiological, biological, or behavioral characteristics and that identifies a consumer, whether individually or in combination with other data. Biometric data includes:

(A) Imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template can be extracted; and

(B) Keystroke patterns or rhythms and gait patterns or rhythms that contain identifying information.

(5) “Clear and conspicuous” means a disclosure that is easily noticeable and easily understandable by the consumer and does not contain any statements that are inconsistent with, or in mitigation of any other statements or disclosures provided by the regulated entity.

"Clear and conspicuous" requires the information to be reasonably accessible to consumers with disabilities, taking into account industry standards for online disclosures.

(6) "Collect" means to buy, rent, access, retain, receive, acquire, infer, derive, or otherwise process consumer health data in any manner.

(7) "Consent" means a clear affirmative act that signifies a consumer's freely given, specific, informed, opt-in, voluntary, and unambiguous agreement, following a clear and conspicuous disclosure to the individual, which shall consist of written consent or consent provided by electronic means. For the purposes of this act "consent" shall not include:

(A) A consumer's acceptance of a general or broad terms-of-use agreement or a similar document that contains descriptions of personal data processing along with other unrelated information;

(B) A consumer's hovering over, muting, pausing, or closing a given piece of electronic content; or

(C) A consumer's agreement obtained through the use of deceptive designs.

(8) "Consumer" means a natural person acting in an individual or household capacity, however identified, including by any unique identifier, who is a District of Columbia ("District") resident or whose consumer health data is collected in the District. "Consumer" does not include an individual acting in the course of their employment.

(9) "Consumer health data" means 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. "Consumer health data" does not include personal information that is used to engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored,

and governed by an institutional review board, human subjects research ethics review board, or a similar independent oversight entity that determines that the regulated entity or the small business has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification.

(10) "Deceptive design" means a user interface designed or manipulated with the effect of subverting or impairing user autonomy, decision making, or choice. "Any practice that the Federal Trade Commission refers to as a "dark pattern" is presumed a deceptive design.

(11) "Deidentified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable consumer, or a device linked to such a consumer. "Deidentified data" includes consumer health data in the possession of a regulated entity where the regulated entity:

(A) Takes reasonable measures to ensure that such data cannot be associated with a consumer;

(B) Publicly commits to maintain and process the data in a deidentified fashion and to not attempt to reidentify the data, except that the regulated entity may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this paragraph; and

(C) Contractually obligates any recipients of such data to maintain the data in a deidentified fashion.

(12) "Gender-affirming care information" means personal information relating to seeking or obtaining past, present, or future gender-affirming care services. "Gender-affirming care information" includes:

(A) Precise location information that could reasonably indicate a consumer's attempt to acquire or receive gender-affirming care services;

(B) Efforts to research or obtain gender-affirming care services; or

(C) Any information related to seeking or obtaining past, present, or future gender-affirming care services that is derived, extrapolated, or inferred, including from non-health information, such as proxy, derivative, inferred, emergent, or algorithmic data.

(13) "Gender-affirming care services" means health services or products that support and affirm an individual's gender identity, including social, psychological, behavioral, cosmetic, medical, or surgical interventions. "Gender-affirming care services" includes treatments for gender dysphoria, gender-affirming hormone therapy, and gender-affirming surgical procedures.

(14) "Genetic data" or "genetic information" means any data, regardless of its format, that concerns a consumer's genetic characteristics. "Genetic data" or "genetic information" includes:

(A) Raw sequence data that result from the sequencing of a consumer's complete extracted deoxyribonucleic acid ("DNA") or a portion of the extracted DNA;

(B) Genotypic and phenotypic information that results from analyzing the raw sequence data; and

(C) Self-reported health data that a consumer submits to a regulated entity and that is analyzed in connection with consumer's raw sequence data.

(15) "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 around a specific physical location, or to

locate a consumer within a virtual boundary. For purposes of this definition, “geofence” means a virtual boundary that is 2,000 feet or less from the perimeter of the physical location.

(16) “Health care services” means any service provided to a person to assess, measure, improve, or learn about a person's mental or physical health, including:

(A) Individual health conditions, status, diseases, or diagnoses;

(B) Social, psychological, behavioral, and medical interventions;

(C) Health-related surgeries or procedures;

(D) Use or purchase of medication;

(E) Bodily functions, vital signs, symptoms, or measurements of the information described in this paragraph;

(F) Diagnoses or diagnostic testing, treatment, or medication;

(G) Reproductive health care services; or

(H) Gender-affirming care services.

(17) “Homepage” means the introductory page of an internet website and any internet webpage where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, and a link within the application, such as from the application configuration, “about,” “information,” or settings page.

(18) “Person” means an individual, firm, corporation, partnership, cooperative, association, or any other organization, legal entity, or group of individuals however organized, including agents thereof. The term “person” includes a regulated entity, third party, affiliate, or processor. The term “person or entity” shall not include the government of the United States, the

District of Columbia government, or any of the agencies or instrumentalities of either government.

(19) "Personal information" means information that identifies or is reasonably capable of being associated or linked, directly or indirectly, to a particular consumer. "Personal information" includes data associated with a persistent unique identifier, such as a cookie ID, an IP address, a device identifier, an advertising ID, or any other form of persistent unique identifier. "Personal information" does not include publicly available information or deidentified data.

(20) "Physical or mental health status" includes:

(A) Individual health conditions, treatment, diseases, or diagnoses;

(B) Social, psychological, behavioral, and medical interventions;

(C) Health-related surgeries or procedures;

(D) Use or purchase of prescribed medications;

(E) Bodily functions, vital signs, symptoms, or measurements of the information described in this paragraph;

(F) Diagnoses or diagnostic testing, treatment, or medication;

(G) Gender-affirming care information;

(H) Reproductive or sexual health information;

(I) Biometric data;

(J) Genetic data;

(K) Precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies;

(L) Data that identifies a consumer seeking health care services; or

(M) Any information that a regulated entity, or their processor, processes to associate or identify a consumer with the data described in this paragraph that is derived or extrapolated from non-health information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning).

(21) "Precise location information" means information derived from technology and that is used or intended to be used to locate a consumer within a radius of 1,750 feet.

(22) "Process" or "processing" means any operation or set of operations performed on consumer health data.

(23) "Processor" means a person that processes consumer health data on behalf of a regulated entity.

(24) "Publicly available information" means information about a consumer that a regulated entity has reasonable cause to believe the consumer has lawfully made available to the general public through federal, state, or municipal government records or widely distributed media. "Publicly available information" does not include any biometric data collected about a consumer by a business without the consumer's consent.

(25) "Regulated entity" means any legal entity, including its agents, that conducts business in the District or produces or provides products or services that are targeted to consumers in the District and that alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling consumer health data. "Regulated entity" does not include government agencies, tribal nations, or contracted service providers when processing consumer health data on behalf of a government agency.

(26) “Reproductive or sexual health information” means personal information relating to seeking or obtaining past, present, or future reproductive or sexual health services. “Reproductive or sexual health information” includes:

(A) Precise location information that could reasonably indicate a consumer's attempt to acquire or receive reproductive or sexual health services;

(B) Efforts to research or obtain reproductive or sexual health services; or

(C) Any reproductive or sexual health information that is derived, extrapolated, or inferred, including from non-health information (such as proxy, derivative, inferred, emergent, or algorithmic data).

(27) “Reproductive or sexual health services” means health services or products that support or relate to a consumer's reproductive system or sexual well-being including:

(A) Individual health conditions, status, diseases, or diagnoses;

(B) Social, psychological, behavioral, and medical interventions;

(C) Health-related surgeries or procedures including abortions;

(D) Use or purchase of medication including medications for the purposes of abortion;

(E) Bodily functions, vital signs, symptoms, or measurements of the information described in this paragraph;

(F) Diagnoses or diagnostic testing, treatment, or medication; and

(G) Medical or nonmedical services related to and provided in conjunction with an abortion, including associated diagnostics, counseling, supplies, and follow-up services.

(28) “Sell” or “sale” means the exchange of consumer health data for monetary or other valuable consideration. “Sell” or “sale” does not include the exchange of consumer health data

for monetary or other valuable consideration to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the regulated entity's assets and that complies with the requirements and obligations of a regulated entity in this act.

(29) "Share" or "sharing" means to release, disclose, disseminate, divulge, make available, provide access to, license, or otherwise communicate orally, in writing, or by electronic or other means, consumer health data to a third party or affiliate. The term "share" or "sharing" does not include:

(A) The disclosure of consumer health data by a regulated entity to a processor when such sharing is to provide goods or services in a manner consistent with the purpose for which the consumer health data was collected and is disclosed pursuant to a binding contract between the regulated entity and the processor;

(B) The disclosure of consumer health data to a third party with whom the consumer has a direct relationship when:

(i) The consumer has requested the disclosure for purpose of obtaining a product or service from the third party;

(ii) The regulated entity maintains control and ownership of the data; and

(iii) The third party uses the consumer health data only at the direction of the regulated entity and in a manner consistent with the purpose for which the consumer provided the data and consented to its release; or

(C) The disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes

control of all or part of the regulated entity's assets and complies with the requirements and obligations of a regulated entity in this act.

(30) “Third party” means an entity other than a consumer, regulated entity, processor, or affiliate of the regulated entity. “Third party” includes a person who purchases consumer health data.

Sec. 3. (a) A regulated entity shall maintain a consumer health data privacy policy that clearly and conspicuously discloses:

(1) The categories of consumer health data collected;

(2) The purposes for which the consumer health data is collected, including how the data will be used;

(3) The categories of sources from which the consumer health data is collected;

(4) The categories of consumer health data that are shared;

(5) A list of the categories of third parties and the specific affiliates with whom the regulated entity shares the consumer health data, whether actively or passively, and the purposes for such sharing;

(6) The length of time the regulated entity intends to retain each category of consumer health data, or if that is not possible, the criteria used to determine that period; provided that a regulated entity shall not retain a consumer’s consumer health data for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose; and

(7) How a consumer can exercise the rights provided in section 5 of this act.

(b) A regulated entity shall prominently publish a link to its consumer health data privacy policy on its homepage.

(c) It is a violation of this act for a regulated entity to contract with a processor, affiliate, or third party to process consumer health data in a manner or for a purpose that is inconsistent with the regulated entity's consumer health data privacy policy.

Sec. 4. (a) A regulated entity shall not collect any consumer health data unless it first obtains consent from the consumer for such collection for a specified purpose. The request for consent shall clearly and conspicuously disclose:

(1) The categories of consumer health data collected;

(2) The purpose of the collection of the consumer health data, including the specific ways in which it will be used;

(3) The length of time the regulated entity intends to retain each category of consumer health data, or if that is not possible, the criteria used to determine that period provided that a regulated entity shall not retain a consumer’s consumer health data for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose; and

(4) How the consumer can withdraw consent from future collection of the consumer's health data.

(b) A regulated entity shall not share any consumer health data unless it first obtains consent from the consumer for such sharing for a specified purpose. This consent for sharing shall be separate and distinct from the consent obtained to collect consumer health data. The request for consent shall clearly and conspicuously disclose:

(1) The categories of consumer health data shared;

(2) The purpose of the sharing of the consumer health data, including the specific ways in which it will be used;

(3) The categories of entities with whom the consumer health data is shared; and

(4) How the consumer can withdraw consent from future sharing of the consumer's health data.

(d) A regulated entity shall not collect, use, or share additional categories of consumer health data not disclosed in the consumer health data privacy policy without first disclosing the additional categories and obtaining the consumer's consent prior to the collection, use, or sharing of such consumer health data.

(e) A regulated entity shall not collect, use, or share consumer health data for additional purposes not disclosed in the consumer health data privacy policy without first disclosing the additional purposes and obtaining the consumer's consent prior to the collection, use, or sharing of such consumer health data.

(f) A regulated entity’s collection, use, retention, disclosure, and sharing of a consumer’s consumer health data shall be reasonably necessary and proportionate to achieve the purposes for which the consumer health data was collected or processed, or for another disclosed purpose that is compatible with the context in which the consumer health data was collected, and not further processed in a manner that is incompatible with those purposes.

(g) A regulated entity that shares or otherwise discloses consumer health data with an affiliate, processor, or third party shall enter into a binding contract with the affiliate, processor, or third party that specifies how the processor, affiliate, or third party may receive, use, manage, and store the consumer health data it receives from regulated entity and contractually obligates the affiliate, processor, or third party to comply with the requirements and obligations in this act.

(h) It is a violation of this act for a regulated entity to contract with a processor to process consumer health data in a manner or for a purpose that is inconsistent with the consent a consumer has given for the collection, use, or sharing of data.

(i) A regulated entity shall not unlawfully discriminate against a consumer for exercising any rights included in this act.

Sec. 5. (a) A consumer has the right to confirm whether a regulated entity is collecting, sharing, or selling consumer health data concerning the consumer. The regulated entity shall provide the consumer with access to such data as expeditiously as possible and without unreasonable delay. This information shall include a list of all third parties and affiliates with whom the regulated entity has shared or sold the consumer health data, and an active email address or other online mechanism that the consumer may use to contact these third parties.

(b) A consumer has the right to withdraw consent from the regulated entity's collection and sharing of consumer health data related to the consumer.

(c) A consumer has the right to have consumer health data related to the consumer deleted from the database of the regulated entity and any other entity to which the regulated entity has shared or sold the consumer health data. The consumer may exercise this right by requesting the deletion pursuant to subsection (g) of this section.

(d) A regulated entity that receives a consumer's request to delete any consumer health data concerning the consumer shall:

(1) Delete the consumer health data from its records, including all parts of the regulated entity's network, including archived or backup systems; and

(2) Notify all affiliates, processors, and third parties with whom the regulated entity has shared or sold consumer health data of the deletion request.

(e) Each affiliate, processor, and third party that receives notice of a consumer's deletion request shall honor the consumer's deletion request and delete the consumer health data from its records according to the same requirements applicable to a regulated entity.

(f) If consumer health data that a consumer requests to be deleted is stored on archived or backup systems, the request for deletion may be delayed for up to 6 months from the authentication of the deletion request to enable restoration of the archived or backup systems.

(g) A consumer may exercise the rights set forth in this section by submitting a request, at any time, to a regulated entity. Such a request may be made by a secure and reliable means established by the regulated entity and clearly and conspicuously described in its consumer health data privacy policy. The method shall take into account the ways in which consumers normally interact with the regulated entity, the need for secure and reliable communication of such requests, and the ability of the regulated entity to authenticate the identity of the consumer making the request. A regulated entity shall not require a consumer to create a new account to exercise consumer rights under this section but may require a consumer to use an existing account.

(h) If a regulated entity is unable to authenticate the request using commercially reasonable efforts, the regulated entity is not required to comply with a deletion request under this section and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.

(i) The regulated entity shall provide information in response to a consumer request at least twice during any 12-month period upon request of the consumer and without charge to the consumer. If requests from a consumer are manifestly unfounded, excessive, or repetitive, the regulated entity may charge the consumer a reasonable fee to cover the administrative costs of

complying with the request or decline to act on the request. The regulated entity shall bear the burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of the request.

(j) A regulated entity shall comply with a deletion request without undue delay, and in all cases within 45 days of receipt of the request. A regulated entity shall promptly take steps to authenticate a consumer request, but these steps shall not extend the regulated entity's duty to comply with the consumer's request within 45 days of receipt. The regulated entity may extend the response period once for 45 additional days when reasonably necessary, taking into account the complexity and number of the consumer's requests, if the regulated entity informs the consumer of any such extension within the initial 45-day response period, together with the reason for the extension.

(k) A regulated entity shall establish a process for a consumer to appeal the regulated entity's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The availability of the appeal process shall be clearly and conspicuously included in the regulated entity’s consumer health data privacy policy. Within 45 days of receipt of an appeal, a regulated entity shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the regulated entity shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general to submit a complaint.

(l) If a regulated entity dissolves or terminates its operations, the regulated entity shall delete all consumer health data from its records, including any archived or back-up systems and provide each consumer whose data has been shared with or sold to a processor, affiliate, or third

party with a notice of how the consumer can contact the processors, affiliates, or third parties to request deletion of their information.

Sec. 6**.** A regulated entity shall:

(a) Restrict access to consumer health data by the employees, affiliates, processors, and third parties of such regulated entity to only those employees, affiliates, processors, and third parties for which access is necessary to further the purposes for which the consumer provided consent or where necessary to provide a product or service that the consumer to whom such consumer health data relates has requested from such regulated entity; and

(b) Establish, implement, and maintain administrative, technical, and physical data security practices that, at a minimum, satisfy reasonable standard of care within the regulated entity's industry to protect the confidentiality, integrity, and accessibility of consumer health data appropriate to the volume and nature of the consumer health data at issue.

Sec. 7. (a) A processor, affiliate, or third party may receive, use, or process consumer health data only pursuant to a binding contract with the regulated entity that specifies how the processor, affiliate, or third party may receive, use, manage, and store the consumer health data it receives from regulated entity.

(b) A processor, affiliate, or third party shall not further share or sell consumer health data it has received from a regulated entity with any other person or entity.

(c) A processor, affiliate, or third party shall assist the regulated entity by appropriate technical and organizational measures, insofar as this is possible, in fulfilling the regulated entity's obligations under this act.

(d) If a processor, affiliate or third party fails to adhere to the regulated entity's contractual requirements or receives, uses, manages, or stores consumer health data in a manner

that is outside the scope of the contract with the regulated entity, the processor, affiliate, or third party shall be considered a regulated entity with regard to such data and shall be subject to all the requirements of this act.

Sec. 8. (a) It is unlawful for any person to sell or offer to sell consumer health data related to a consumer without first obtaining valid authorization from the consumer. This authorization shall be separate and distinct from the consent obtained to collect or share consumer health data required under section 4 of this act.

(b) A valid authorization to sell consumer health data shall be a written or electronic document consistent with this section. It shall be in plain language and contain the following:

(1) The specific consumer health data concerning the consumer that the person intends to sell;

(2) The name and contact information of the person selling the consumer health data;

(3) The name and contact information of the regulated entity that originally collected the consumer health data;

(4) The name and contact information of the person purchasing the consumer health data from the seller identified in paragraph (2) of this subsection;

(5) A description of the purpose for the sale, including how the consumer health data will be gathered and how it will be used by the purchaser identified in paragraph (4) of this subsection when sold;

(6) A statement that the provision of goods or services may not be conditioned on the consumer signing the valid authorization;

(7) A statement that the consumer has a right to revoke the valid authorization at any time and a description of how to submit a revocation;

(8) An expiration date for the valid authorization that is no later than one year after the date the consumer signs the valid authorization; and

(9) The signature or e-signature of the consumer and date.

(c) An authorization shall be invalid if it contains any of the following defects:

(1) The expiration date has passed;

(2) The authorization does not contain all the information required under this section;

(3) The consumer has revoked the authorization;

(4) The authorization has been combined with other documents to create a compound authorization; or

(5) The provision of goods or services is conditioned on the consumer signing the authorization.

(d) The seller shall obtain the valid authorization from the consumer and provide copies to the consumer and the purchaser.

(e) The seller and purchaser of consumer health data shall retain a copy of all valid authorizations for sale of consumer health data for 6 years from the date of the consumer's signature or the date when it was last in effect, whichever is later.

(f) A person may sell consumer health data only pursuant to a binding contract between the person selling the consumer health data and the person purchasing the consumer health data that identifies the purpose and use of the consumer health data and contractually obligates the

person purchasing the consumer health data to comply with the applicable requirements and obligations in this act.

(g) The person who purchases consumer health data shall only use, retain, and share a consumer's health data in a manner compatible with purpose and use identified in a valid authorization from a consumer.

Sec. 9. It is unlawful for any person to implement a geofence around an entity that provides in-person health care services where the geofence is used to:

(a) Identify or track consumers seeking health care services;

(b) Collect consumer health data; or

(c) Send notifications, messages, or advertisements to consumers related to their consumer health data or health care services.

Sec. 10**.** A violation of this act is an unfair and deceptive trade practice pursuant to D.C. Official Code § 28-3904.

Sec. 11. (a) This chapter does not apply to:

(1) Information that meets the definition of:

(A) Health information protected under the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), approved August 21, 1996 (Pub. L. 104-191; 110 Stat. 1936), and related regulations;

(B) Patient identifying information collected, used, or disclosed in accordance with 42 C.F.R. Part 2 and section 131 of the ADAMHA Reorganization Act, approved July 10, 1992 (106 Stat. 368: 42 U.S.C. § 290dd-2);

(C) The following research-related information:

(i) Identifiable private information under the federal policy for the protection of human subjects pursuant to 45 C.F.R. Part 46;

(ii) Identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the international council for harmonization;

(iii) Information made private for the protection of human subjects under 21 C.F.R. Parts 50 and 56; or

(iv) Personal data used or shared in research conducted in accordance with one or more of the requirements in this paragraph;

(D) Information or documents created for purposes of the federal Health Care Quality Improvement Act of 1986, approved November 14, 1986 (100 Stat. 3784; 42 U.S.C. § 11101), and related regulations;

(E) Patient safety work product under 42 C.F.R. Part 3 and section 2 of the Patient Safety and Quality Improvement Act of 2005, approved July 29, 2005 (119 Stat. 424; 42 U.S.C.§§ 299b-21 - 299b-26);

(F) Information that is deidentified in accordance with 45 C.F.R. Part 164, and derived from any of the health care-related information listed in subsection (a)(1) of this section;

(2) Information originating from, and intermingled to be indistinguishable with, information under paragraph (1) of this subsection that is maintained by:

(A) A covered entity or business associate as defined by HIPAA and related regulations;

(B) A program or a qualified service organization under 42 C.F.R. Part 2 and section 131 of the ADAMHA Reorganization Act, approved July 10, 1992 (106 Stat. 368: 42 U.S.C. § 290dd-2); and

(3) Information used only for public health activities and purposes as described in 45 C.F.R. §. 164.512 or that is part of a limited data set that is used, disclosed, and maintained in the manner required by 45 C.F.R. § 164.514;

(b) Personal information that is governed by and collected, used, or disclosed pursuant to the following regulations, parts, titles, or acts, is exempt from this chapter:

(1) The Gramm-Leach-Bliley Act, approved November 12, 1999 (113 Stat. 1338; 15 U.S.C. § 6801 *et seq*..) and implementing regulations;

(2) Part C of Title XI of the Social Security Act, approved August 21, 1996 (110 Stat. 1936; 42 U.S.C. § 1320d *et seq*.);

(3) The Fair Credit Reporting Act, approved May 29, 1968 (82 Stat. 146; 15 U.S.C. § 1681 *et seq*.);

(4) The Family Educational Rights and Privacy Act, approved August 21, 1974 (88 Stat. 57; (20 U.S.C. § 1232g) and 34 C.F.R. Part 99.

(c) The obligations imposed on regulated entities and processors under this act do not restrict a regulated entity's or processor's ability to collect, use, or disclose consumer health data to prevent, detect, protect against, or respond to security incidents, identity, theft, fraud, harassment, malicious or deceptive activities, or any activity that is illegal under District or federal law; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action that is illegal under District or federal law.

(d) If a regulated entity or processor processes consumer health data pursuant to subsection (c) of this section, such entity bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements of this section.

Sec. 12. D.C. Official Code § 28-3904 is amended as follows:

(a) Subsection (kk) is amended by striking the word "or" at the end.

(b) Subsection (ll) is amended by striking the period at the end and inserting the phrase "; or" in its place.

(c) A new subsection (mm) is added to read as follows:

"(mm) violate any provision of the Consumer Health Information Privacy Protection Act of 2024.".

Sec. 13. 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. 14. Effective date.

This act shall take effect following approval by the Mayor (or in the event of a veto by the Mayor, action by the Council to override the veto), 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)), and publication in the District of Columbia Register.