GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE ATTORNEY GENERAL

ATTORNEY GENERAL
BRIAN L. SCHWALB

July 12, 2024

The Honorable Phil Mendelson
Chairman, Council of the District of Columbia
John A. Wilson Building
1350 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

Dear Chairman Mendelson:

I write to transmit the "Consumer Health Information Privacy Protection (CHIPPA) Act of 2024," for consideration and enactment by the Council of the District of Columbia.

Personal health data that is uploaded to online platforms like company websites, search engines, apps, and even social media is being collected, shared, and sold to third parties without the consumer's consent or knowledge. While most people believe that the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA") protects all personal health data from being shared without consent or knowledge, it only applies to data collected by a "covered entity," such as health insurers, hospitals, and healthcare providers. It does not extend to personal health information shared by non-covered entities. For example, health devices, apps, Apple Watch, and patient support groups fall outside of HIPAA regulation.

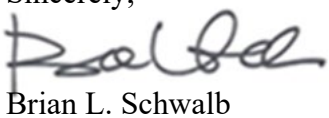
This legislation will ensure regulated entities that obtain, collect, share, and sell consumer personal health data are responsible, transparent, and held accountable to the consumer. CHIPPA will do the following:

1. Require regulated entities to establish and make publicly available a consumer health data privacy policy governing the collection, use, sharing, and sale of consumer health data.
2. Require that regulated entities obtain the consumer's informed consent before collecting and sharing their personal health data.
3. Establish a consumer's right to access and choose whether and how their personal health data is used by a regulated entity.
4. Establish additional protections and consumer authorizations for the sale of personal health data.
5. Require regulated entities to only collect health data that is necessary for the purposes disclosed to the consumers and to only use, share, and retain the consumer health data for that purpose.
6. Prohibit the establishment of geofences around places where health services are delivered under specified circumstances.
7. Make violations unfair and deceptive trade practices.

I ask that the Council enact this legislation to ensure that everyone, regardless of whether they are a patient seeking health care services, a consumer signing-up for a fitness app, or purchasing an item online, knows why, how, and to whom their personal health data is being used, shared, and sold. If you have any

questions, please contact me or Deputy Attorney General for Policy and Legislative Affairs Candyce Phoenix at (202) 788-2066 or Candyce.Phoenix@dc.gov.

Sincerely,



Brian L. Schwalb
Attorney General for the District of Columbia

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 (CHIPPA) 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.

42 (2) “Affiliate” means a legal entity that shares common branding with another legal entity
43 and controls, is controlled by, or is under common control with another legal entity. For purposes
44 of this definition, “control” or “controlled” means:
45 (A) Ownership of, or the power to vote, more than 50 percent of the outstanding
46 shares of any class of voting security of a company;
47 (B) Control in any manner over the election of a majority of the directors or of
48 individuals exercising similar functions; or
49 (C) The power to exercise controlling influence over the management of a
50 company.
51 (3) “Authenticate” means to use reasonable means to determine that a request to exercise
52 any of the rights afforded in this act is being made by, or on behalf of, the consumer who is
53 entitled to exercise such consumer rights with respect to the consumer health data at issue.
54 (4) “Biometric data” means data that is generated from the measurement or technological
55 processing of an individual’s physiological, biological, or behavioral characteristics and that
56 identifies a consumer, whether individually or in combination with other data. Biometric data
57 includes:
58 (A) Imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and
59 voice recordings, from which an identifier template can be extracted; and
60 (B) Keystroke patterns or rhythms and gait patterns or rhythms that contain
61 identifying information.
62 (5) “Clear and conspicuous” means a disclosure that is easily noticeable and easily
63 understandable by the consumer and does not contain any statements that are inconsistent with,
64 or in mitigation of any other statements or disclosures provided by the regulated entity.

65 "Clear and conspicuous" requires the information to be reasonably accessible to
66 consumers with disabilities, taking into account industry standards for online disclosures.
67 (6) "Collect" means to buy, rent, access, retain, receive, acquire, infer, derive, or
68 otherwise process consumer health data in any manner.
69 (7) "Consent" means a clear affirmative act that signifies a consumer's freely given,
70 specific, informed, opt-in, voluntary, and unambiguous agreement, following a clear and
71 conspicuous disclosure to the individual, which shall consist of written consent or consent
72 provided by electronic means. For the purposes of this act "consent" shall not include:
73 (A) A consumer's acceptance of a general or broad terms-of-use agreement or a
74 similar document that contains descriptions of personal data processing along with other
75 unrelated information;
76 (B) A consumer's hovering over, muting, pausing, or closing a given piece of
77 electronic content; or
78 (C) A consumer's agreement obtained through the use of deceptive designs.
79 (8) "Consumer" means a natural person acting in an individual or household capacity,
80 however identified, including by any unique identifier, who is a District of Columbia ("District")
81 resident or whose consumer health data is collected in the District. "Consumer" does not include
82 an individual acting in the course of their employment.
83 (9) "Consumer health data" means personal information that is linked or can reasonably
84 be linked to a consumer and that identifies the consumer's past, present, or future physical or
85 mental health status. "Consumer health data" does not include personal information that is used
86 to engage in public or peer-reviewed scientific, historical, or statistical research in the public
87 interest that adheres to all other applicable ethics and privacy laws and is approved, monitored,

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

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

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

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

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

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

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

110 (A) Precise location information that could reasonably indicate a consumer's
111 attempt to acquire or receive gender-affirming care services;
112 (B) Efforts to research or obtain gender-affirming care services; or
113 (C) Any information related to seeking or obtaining past, present, or future
114 gender-affirming care services that is derived, extrapolated, or inferred, including from non-
115 health information, such as proxy, derivative, inferred, emergent, or algorithmic data.
116 (13) "Gender-affirming care services" means health services or products that support and
117 affirm an individual's gender identity, including social, psychological, behavioral, cosmetic,
118 medical, or surgical interventions. "Gender-affirming care services" includes treatments for
119 gender dysphoria, gender-affirming hormone therapy, and gender-affirming surgical procedures.
120 (14) "Genetic data" or "genetic information" means any data, regardless of its format,
121 that concerns a consumer's genetic characteristics. "Genetic data" or "genetic information"
122 includes:
123 (A) Raw sequence data that result from the sequencing of a consumer's complete
124 extracted deoxyribonucleic acid ("DNA") or a portion of the extracted DNA;
125 (B) Genotypic and phenotypic information that results from analyzing the raw
126 sequence data; and
127 (C) Self-reported health data that a consumer submits to a regulated entity and
128 that is analyzed in connection with consumer's raw sequence data.
129 (15) "Geofence" means technology that uses global positioning coordinates, cell tower
130 connectivity, cellular data, radio frequency identification, Wi-fi data, or any other form of spatial
131 or location detection to establish a virtual boundary around a specific physical location, or to

132 locate a consumer within a virtual boundary. For purposes of this definition, “geofence” means a
133 virtual boundary that is 2,000 feet or less from the perimeter of the physical location.
134 (16) “Health care services” means any service provided to a person to assess, measure,
135 improve, or learn about a person's mental or physical health, including:
136 (A) Individual health conditions, status, diseases, or diagnoses;
137 (B) Social, psychological, behavioral, and medical interventions;
138 (C) Health-related surgeries or procedures;
139 (D) Use or purchase of medication;
140 (E) Bodily functions, vital signs, symptoms, or measurements of the information
141 described in this paragraph;
142 (F) Diagnoses or diagnostic testing, treatment, or medication;
143 (G) Reproductive health care services; or
144 (H) Gender-affirming care services.
145 (17) “Homepage” means the introductory page of an internet website and any internet
146 webpage where personal information is collected. In the case of an online service, such as a
147 mobile application, homepage means the application's platform page or download page, and a
148 link within the application, such as from the application configuration, “about,” “information,” or
149 settings page.
150 (18) “Person” means an individual, firm, corporation, partnership, cooperative,
151 association, or any other organization, legal entity, or group of individuals however organized,
152 including agents thereof. The term “person” includes a regulated entity, third party, affiliate, or
153 processor. The term “person or entity” shall not include the government of the United States, the

154 District of Columbia government, or any of the agencies or instrumentalities of either
155 government.
156 (19) "Personal information" means information that identifies or is reasonably capable of
157 being associated or linked, directly or indirectly, to a particular consumer. "Personal
158 information" includes data associated with a persistent unique identifier, such as a cookie ID, an
159 IP address, a device identifier, an advertising ID, or any other form of persistent unique
160 identifier. "Personal information" does not include publicly available information or deidentified
161 data.
162 (20) "Physical or mental health status" includes:
163 (A) Individual health conditions, treatment, diseases, or diagnoses;
164 (B) Social, psychological, behavioral, and medical interventions;
165 (C) Health-related surgeries or procedures;
166 (D) Use or purchase of prescribed medications;
167 (E) Bodily functions, vital signs, symptoms, or measurements of the information
168 described in this paragraph;
169 (F) Diagnoses or diagnostic testing, treatment, or medication;
170 (G) Gender-affirming care information;
171 (H) Reproductive or sexual health information;
172 (I) Biometric data;
173 (J) Genetic data;
174 (K) Precise location information that could reasonably indicate a consumer's
175 attempt to acquire or receive health services or supplies;
176 (L) Data that identifies a consumer seeking health care services; or

177 (M) Any information that a regulated entity, or their processor, processes to
178 associate or identify a consumer with the data described in this paragraph that is derived or
179 extrapolated from non-health information (such as proxy, derivative, inferred, or emergent data
180 by any means, including algorithms or machine learning).
181 (21) "Precise location information" means information derived from technology and that
182 is used or intended to be used to locate a consumer within a radius of 1,750 feet.
183 (22) "Process" or "processing" means any operation or set of operations performed on
184 consumer health data.
185 (23) "Processor" means a person that processes consumer health data on behalf of a
186 regulated entity.
187 (24) "Publicly available information" means information about a consumer that a
188 regulated entity has reasonable cause to believe the consumer has lawfully made available to the
189 general public through federal, state, or municipal government records or widely distributed
190 media. "Publicly available information" does not include any biometric data collected about a
191 consumer by a business without the consumer's consent.
192 (25) "Regulated entity" means any legal entity, including its agents, that conducts
193 business in the District or produces or provides products or services that are targeted to
194 consumers in the District and that alone or jointly with others, determines the purpose and means
195 of collecting, processing, sharing, or selling consumer health data. "Regulated entity" does not
196 include government agencies, tribal nations, or contracted service providers when processing
197 consumer health data on behalf of a government agency.

198 (26) “Reproductive or sexual health information” means personal information relating to
199 seeking or obtaining past, present, or future reproductive or sexual health services.
200 “Reproductive or sexual health information” includes:
201 (A) Precise location information that could reasonably indicate a consumer's
202 attempt to acquire or receive reproductive or sexual health services;
203 (B) Efforts to research or obtain reproductive or sexual health services; or
204 (C) Any reproductive or sexual health information that is derived, extrapolated, or
205 inferred, including from non-health information (such as proxy, derivative, inferred, emergent, or
206 algorithmic data).
207 (27) “Reproductive or sexual health services” means health services or products that
208 support or relate to a consumer's reproductive system or sexual well-being including:
209 (A) Individual health conditions, status, diseases, or diagnoses;
210 (B) Social, psychological, behavioral, and medical interventions;
211 (C) Health-related surgeries or procedures including abortions;
212 (D) Use or purchase of medication including medications for the purposes of
213 abortion;
214 (E) Bodily functions, vital signs, symptoms, or measurements of the information
215 described in this paragraph;
216 (F) Diagnoses or diagnostic testing, treatment, or medication; and
217 (G) Medical or nonmedical services related to and provided in conjunction with
218 an abortion, including associated diagnostics, counseling, supplies, and follow-up services.
219 (28) “Sell” or “sale” means the exchange of consumer health data for monetary or other
220 valuable consideration. “Sell” or “sale” does not include the exchange of consumer health data

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

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

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

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

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

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

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

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

243 control of all or part of the regulated entity's assets and complies with the requirements and
244 obligations of a regulated entity in this act.
245 (30) “Third party” means an entity other than a consumer, regulated entity, processor, or
246 affiliate of the regulated entity. “Third party” includes a person who purchases consumer health
247 data.
248 Sec. 3. (a) A regulated entity shall maintain a consumer health data privacy policy that
249 clearly and conspicuously discloses:
250 (1) The categories of consumer health data collected;
251 (2) The purposes for which the consumer health data is collected, including how
252 the data will be used;
253 (3) The categories of sources from which the consumer health data is collected;
254 (4) The categories of consumer health data that are shared;
255 (5) A list of the categories of third parties and the specific affiliates with whom
256 the regulated entity shares the consumer health data, whether actively or passively, and the
257 purposes for such sharing;
258 (6) The length of time the regulated entity intends to retain each category of
259 consumer health data, or if that is not possible, the criteria used to determine that period;
260 provided that a regulated entity shall not retain a consumer’s consumer health data for each
261 disclosed purpose for which the personal information was collected for longer than is reasonably
262 necessary for that disclosed purpose; and
263 (7) How a consumer can exercise the rights provided in section 5 of this act.
264 (b) A regulated entity shall prominently publish a link to its consumer health data
265 privacy policy on its homepage.

266 (c) It is a violation of this act for a regulated entity to contract with a processor, affiliate,
267 or third party to process consumer health data in a manner or for a purpose that is inconsistent
268 with the regulated entity's consumer health data privacy policy.
269 Sec. 4. (a) A regulated entity shall not collect any consumer health data unless it first
270 obtains consent from the consumer for such collection for a specified purpose. The request for
271 consent shall clearly and conspicuously disclose:
272 (1) The categories of consumer health data collected;
273 (2) The purpose of the collection of the consumer health data, including the
274 specific ways in which it will be used;
275 (3) The length of time the regulated entity intends to retain each category of
276 consumer health data, or if that is not possible, the criteria used to determine that period provided
277 that a regulated entity shall not retain a consumer's consumer health data for each disclosed
278 purpose for which the personal information was collected for longer than is reasonably necessary
279 for that disclosed purpose; and
280 (4) How the consumer can withdraw consent from future collection of the
281 consumer's health data.
282 (b) A regulated entity shall not share any consumer health data unless it first obtains
283 consent from the consumer for such sharing for a specified purpose. This consent for sharing
284 shall be separate and distinct from the consent obtained to collect consumer health data. The
285 request for consent shall clearly and conspicuously disclose:
286 (1) The categories of consumer health data shared;
287 (2) The purpose of the sharing of the consumer health data, including the specific
288 ways in which it will be used;

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

290 (4) How the consumer can withdraw consent from future sharing of the

291 consumer's health data.

292 (d) A regulated entity shall not collect, use, or share additional categories of consumer

293 health data not disclosed in the consumer health data privacy policy without first disclosing the

294 additional categories and obtaining the consumer's consent prior to the collection, use, or sharing

295 of such consumer health data.

296 (e) A regulated entity shall not collect, use, or share consumer health data for additional

297 purposes not disclosed in the consumer health data privacy policy without first disclosing the

298 additional purposes and obtaining the consumer's consent prior to the collection, use, or sharing

299 of such consumer health data.

300 (f) A regulated entity's collection, use, retention, disclosure, and sharing of a consumer's

301 consumer health data shall be reasonably necessary and proportionate to achieve the purposes for

302 which the consumer health data was collected or processed, or for another disclosed purpose that

303 is compatible with the context in which the consumer health data was collected, and not further

304 processed in a manner that is incompatible with those purposes.

305 (g) A regulated entity that shares or otherwise discloses consumer health data with an

306 affiliate, processor, or third party shall enter into a binding contract with the affiliate, processor,

307 or third party that specifies how the processor, affiliate, or third party may receive, use, manage,

308 and store the consumer health data it receives from regulated entity and contractually obligates

309 the affiliate, processor, or third party to comply with the requirements and obligations in this act.

310 (h) It is a violation of this act for a regulated entity to contract with a processor to process
311 consumer health data in a manner or for a purpose that is inconsistent with the consent a
312 consumer has given for the collection, use, or sharing of data.
313 (i) A regulated entity shall not unlawfully discriminate against a consumer for exercising
314 any rights included in this act.
315 Sec. 5. (a) A consumer has the right to confirm whether a regulated entity is collecting,
316 sharing, or selling consumer health data concerning the consumer. The regulated entity shall
317 provide the consumer with access to such data as expeditiously as possible and without
318 unreasonable delay. This information shall include a list of all third parties and affiliates with
319 whom the regulated entity has shared or sold the consumer health data, and an active email
320 address or other online mechanism that the consumer may use to contact these third parties.
321 (b) A consumer has the right to withdraw consent from the regulated entity's collection
322 and sharing of consumer health data related to the consumer.
323 (c) A consumer has the right to have consumer health data related to the consumer
324 deleted from the database of the regulated entity and any other entity to which the regulated
325 entity has shared or sold the consumer health data. The consumer may exercise this right by
326 requesting the deletion pursuant to subsection (g) of this section.
327 (d) A regulated entity that receives a consumer's request to delete any consumer health
328 data concerning the consumer shall:
329 (1) Delete the consumer health data from its records, including all parts of the
330 regulated entity's network, including archived or backup systems; and
331 (2) Notify all affiliates, processors, and third parties with whom the regulated
332 entity has shared or sold consumer health data of the deletion request.

333 (e) Each affiliate, processor, and third party that receives notice of a consumer's deletion
334 request shall honor the consumer's deletion request and delete the consumer health data from its
335 records according to the same requirements applicable to a regulated entity.
336 (f) If consumer health data that a consumer requests to be deleted is stored on archived or
337 backup systems, the request for deletion may be delayed for up to 6 months from the
338 authentication of the deletion request to enable restoration of the archived or backup systems.
339 (g) A consumer may exercise the rights set forth in this section by submitting a request, at
340 any time, to a regulated entity. Such a request may be made by a secure and reliable means
341 established by the regulated entity and clearly and conspicuously described in its consumer
342 health data privacy policy. The method shall take into account the ways in which consumers
343 normally interact with the regulated entity, the need for secure and reliable communication of
344 such requests, and the ability of the regulated entity to authenticate the identity of the consumer
345 making the request. A regulated entity shall not require a consumer to create a new account to
346 exercise consumer rights under this section but may require a consumer to use an existing
347 account.
348 (h) If a regulated entity is unable to authenticate the request using commercially
349 reasonable efforts, the regulated entity is not required to comply with a deletion request under
350 this section and may request that the consumer provide additional information reasonably
351 necessary to authenticate the consumer and the consumer's request.
352 (i) The regulated entity shall provide information in response to a consumer request at
353 least twice during any 12-month period upon request of the consumer and without charge to the
354 consumer. If requests from a consumer are manifestly unfounded, excessive, or repetitive, the
355 regulated entity may charge the consumer a reasonable fee to cover the administrative costs of

356 complying with the request or decline to act on the request. The regulated entity shall bear the
357 burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of the request.
358 (j) A regulated entity shall comply with a deletion request without undue delay, and in all
359 cases within 45 days of receipt of the request. A regulated entity shall promptly take steps to
360 authenticate a consumer request, but these steps shall not extend the regulated entity's duty to
361 comply with the consumer's request within 45 days of receipt. The regulated entity may extend
362 the response period once for 45 additional days when reasonably necessary, taking into account
363 the complexity and number of the consumer's requests, if the regulated entity informs the
364 consumer of any such extension within the initial 45-day response period, together with the
365 reason for the extension.
366 (k) A regulated entity shall establish a process for a consumer to appeal the regulated
367 entity's refusal to take action on a request within a reasonable period of time after the consumer's
368 receipt of the decision. The availability of the appeal process shall be clearly and conspicuously
369 included in the regulated entity’s consumer health data privacy policy. Within 45 days of receipt
370 of an appeal, a regulated entity shall inform the consumer in writing of any action taken or not
371 taken in response to the appeal, including a written explanation of the reasons for the decisions.
372 If the appeal is denied, the regulated entity shall also provide the consumer with an online
373 mechanism, if available, or other method through which the consumer may contact the attorney
374 general to submit a complaint.
375 (l) If a regulated entity dissolves or terminates its operations, the regulated entity shall
376 delete all consumer health data from its records, including any archived or back-up systems and
377 provide each consumer whose data has been shared with or sold to a processor, affiliate, or third

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

380 Sec. 6. A regulated entity shall:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

423 (7) A statement that the consumer has a right to revoke the valid authorization at
424 any time and a description of how to submit a revocation;
425 (8) An expiration date for the valid authorization that is no later than one year
426 after the date the consumer signs the valid authorization; and
427 (9) The signature or e-signature of the consumer and date.
428 (c) An authorization shall be invalid if it contains any of the following defects:
429 (1) The expiration date has passed;
430 (2) The authorization does not contain all the information required under this
431 section;
432 (3) The consumer has revoked the authorization;
433 (4) The authorization has been combined with other documents to create a
434 compound authorization; or
435 (5) The provision of goods or services is conditioned on the consumer signing the
436 authorization.
437 (d) The seller shall obtain the valid authorization from the consumer and provide copies
438 to the consumer and the purchaser.
439 (e) The seller and purchaser of consumer health data shall retain a copy of all valid
440 authorizations for sale of consumer health data for 6 years from the date of the consumer's
441 signature or the date when it was last in effect, whichever is later.
442 (f) A person may sell consumer health data only pursuant to a binding contract between
443 the person selling the consumer health data and the person purchasing the consumer health data
444 that identifies the purpose and use of the consumer health data and contractually obligates the

445 person purchasing the consumer health data to comply with the applicable requirements and
446 obligations in this act.
447 (g) The person who purchases consumer health data shall only use, retain, and share a
448 consumer's health data in a manner compatible with purpose and use identified in a valid
449 authorization from a consumer.
450 Sec. 9. It is unlawful for any person to implement a geofence around an entity that
451 provides in-person health care services where the geofence is used to:
452 (a) Identify or track consumers seeking health care services;
453 (b) Collect consumer health data; or
454 (c) Send notifications, messages, or advertisements to consumers related to their
455 consumer health data or health care services.
456 Sec. 10. A violation of this act is an unfair and deceptive trade practice pursuant to D.C.
457 Official Code § 28-3904.
458 Sec. 11. (a) This chapter does not apply to:
459 (1) Information that meets the definition of:
460 (A) Health information protected under the federal Health Insurance
461 Portability and Accountability Act of 1996 ("HIPAA"), approved August 21, 1996 (Pub. L. 104-
462 191; 110 Stat. 1936), and related regulations;
463 (B) Patient identifying information collected, used, or disclosed in
464 accordance with 42 C.F.R. Part 2 and section 131 of the ADAMHA Reorganization Act,
465 approved July 10, 1992 (106 Stat. 368: 42 U.S.C. § 290dd-2);
466 (C) The following research-related information:

467 (i) Identifiable private information under the federal policy for the
468 protection of human subjects pursuant to 45 C.F.R. Part 46;
469 (ii) Identifiable private information that is otherwise information
470 collected as part of human subjects research pursuant to the good clinical practice guidelines
471 issued by the international council for harmonization;
472 (iii) Information made private for the protection of human subjects
473 under 21 C.F.R. Parts 50 and 56; or
474 (iv) Personal data used or shared in research conducted in
475 accordance with one or more of the requirements in this paragraph;
476 (D) Information or documents created for purposes of the federal Health
477 Care Quality Improvement Act of 1986, approved November 14, 1986 (100 Stat. 3784; 42
478 U.S.C. § 11101), and related regulations;
479 (E) Patient safety work product under 42 C.F.R. Part 3 and section 2 of the
480 Patient Safety and Quality Improvement Act of 2005, approved July 29, 2005 (119 Stat. 424; 42
481 U.S.C.§§ 299b-21 - 299b-26);
482 (F) Information that is deidentified in accordance with 45 C.F.R. Part 164,
483 and derived from any of the health care-related information listed in subsection (a)(1) of this
484 section;
485 (2) Information originating from, and intermingled to be indistinguishable with,
486 information under paragraph (1) of this subsection that is maintained by:
487 (A) A covered entity or business associate as defined by HIPAA and
488 related regulations;

489 (B) A program or a qualified service organization under 42 C.F.R. Part 2
490 and section 131 of the ADAMHA Reorganization Act, approved July 10, 1992 (106 Stat. 368: 42
491 U.S.C. § 290dd-2); and
492 (3) Information used only for public health activities and purposes as described in
493 45 C.F.R. §. 164.512 or that is part of a limited data set that is used, disclosed, and maintained in
494 the manner required by 45 C.F.R. § 164.514;
495 (b) Personal information that is governed by and collected, used, or disclosed pursuant to
496 the following regulations, parts, titles, or acts, is exempt from this chapter:
497 (1) The Gramm-Leach-Bliley Act, approved November 12, 1999 (113 Stat. 1338;
498 15 U.S.C. § 6801 *et seq*..) and implementing regulations;
499 (2) Part C of Title XI of the Social Security Act, approved August 21, 1996 (110
500 Stat. 1936; 42 U.S.C. § 1320d *et seq*.);
501 (3) The Fair Credit Reporting Act, approved May 29, 1968 (82 Stat. 146; 15
502 U.S.C. § 1681 *et seq*.);
503 (4) The Family Educational Rights and Privacy Act, approved August 21, 1974
504 (88 Stat. 57; (20 U.S.C. § 1232g) and 34 C.F.R. Part 99.
505 (c) The obligations imposed on regulated entities and processors under this act do not
506 restrict a regulated entity's or processor's ability to collect, use, or disclose consumer health data
507 to prevent, detect, protect against, or respond to security incidents, identity, theft, fraud,
508 harassment, malicious or deceptive activities, or any activity that is illegal under District or
509 federal law; preserve the integrity or security of systems; or investigate,
510 report, or prosecute those responsible for any such action that is illegal under District or federal
511 law.

512 (d) If a regulated entity or processor processes consumer health data pursuant to
513 subsection (c) of this section, such entity bears the burden of demonstrating that such processing
514 qualifies for the exemption and complies with the requirements of this section.
515 Sec. 12. D.C. Official Code § 28-3904 is amended as follows:
516 (a) Subsection (kk) is amended by striking the word "or" at the end.
517 (b) Subsection (ll) is amended by striking the period at the end and inserting the phrase ";
518 or" in its place.
519 (c) A new subsection (mm) is added to read as follows:
520 "(mm) violate any provision of the Consumer Health Information Privacy Protection Act
521 of 2024.".
522 Sec. 13. Fiscal impact statement.
523 The Council adopts the fiscal impact statement in the committee report as the fiscal
524 impact statement required by section 4a of the General Legislative Procedures Act of 1975,
525 approved October 16, 2006 (120 Stat. 2038; D.C. Official Code § 1-301.47a).
526 Sec. 14. Effective date.
527 This act shall take effect following approval by the Mayor (or in the event of a veto by
528 the Mayor, action by the Council to override the veto), a 30-day period of congressional review
529 as provided in section 602(c)(1) of the District of Columbia Home Rule Act, approved December
530 24, 1973 (87 Stat. 813; D.C. Official Code § 1-206.02(c)(1)), and publication in the District of
531 Columbia Register.
532

GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE ATTORNEY GENERAL

BRIAN L. SCHWALB
ATTORNEY GENERAL

Legal Counsel Division

MEMORANDUM

TO: Candyce Phoenix
Deputy Attorney General for Policy and Legislative Affairs

FROM: Megan D. Browder
Deputy Attorney General
Legal Counsel Division

DATE: July 11, 2024

SUBJECT: Legal Sufficiency Review of Draft Bill the "Consumer Health Information Privacy Protection Act (CHIPPA) of 2024" (AE-24-294)

This is to Certify that this Office has reviewed the above-referenced legislation and has found it to be legally sufficient. If you have any questions regarding this certification, please do not hesitate to contact me at (202) 724-5524.

Megan D. Browder

1350 Pennsylvania Avenue, N.W., Suite 409, Washington, D.C. 20004 Phone: (202) 724-5524 Email: megan.browder@dc.gov

GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE ATTORNEY GENERAL

Brian L. Schwalb
Attorney General

Legal Counsel Division

PRIVILEGED AND CONFIDENTIAL
ATTORNEY-CLIENT COMMUNICATION

MEMORANDUM

TO: **Candyce Phoenix**
Deputy Attorney General for Policy and Legislative Affairs

FROM: **Megan D. Browder** MDB
Deputy Attorney General
Legal Counsel Division

DATE: **July 11, 2024**

SUBJECT: **Legal Sufficiency Review of Draft Bill the "Consumer Health Information Privacy Protection Act (CHIPPA) of 2024"**
(AE-24-294)

This memorandum responds to your request that the Legal Counsel Division conduct a legal sufficiency review of the "Consumer Health Information Privacy Protection Act (CHIPPA) of 2024 ("bill").

The bill would establish privacy protections for consumer health data provided to entities that are not covered by the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), approved August 21, 1996 (Pub. L. 104-191; 110 Stat. 1936). Among other things, it would require regulated entities to establish and make available a consumer health data privacy policy governing the collection, use, sharing, and sale of consumer health data. It would also require these entities to obtain the consumer's informed consent to the collection and sharing of consumer health data and require additional protections and consumer authorizations for the sale of protected data.

The Legal Counsel Division worked with OAG's Office of Consumer Protection to develop and draft the bill, and the attached version is legally sufficient.[1] I have therefore provided a Certificate of Legal Sufficiency, which you should include in your legislative package when you submit it to the Council. Please also remember that you must obtain a fiscal impact statement from the Chief Financial Officer to accompany the legislation.

[1] We have advised further clarity be added to the bill's section 4(i), which prohibits a regulated entity from "unlawfully discriminat[ing] against a consumer for exercising any rights" included in the law. It is unclear what unlawful discrimination means in this context. We will continue to work with OCP to draft amending language.

If you have any questions about this memorandum, please contact Laurie Ensworth, Senior Assistant Attorney General, Legal Counsel Division, at (202) 724-5537, or me at (202) 724-5524.

MDB/lae