epic.org

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

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

October 31, 2024

Chair Christina Henderson
DC Council Committee on Health
1350 Pennsylvania Avenue NW
Washington, DC 20004

Dear Chair Henderson and Members of the Committee:

Thank you for the opportunity to submit written testimony in support of Bill 25-0930, the Consumer Health Information Privacy Protection Act. The Electronic Privacy Information Center (EPIC) is an independent nonprofit research organization here in Washington, DC, established in 1994 to protect privacy, freedom of expression, and democratic values in the information age.[1]

EPIC commends the sponsors for crafting a bill that provides meaningful privacy protections for sensitive health data. For more than two decades, powerful tech companies have been allowed to set the terms of our online interactions. Without any meaningful restrictions on their business practices, they have built systems that invade our private lives, surveil our families, and gather the most intimate details about us for profit. But it does not have to be this way, and enacting CHIPPA would be a significant step toward securing privacy for health data.

This supplemental written testimony will build on EPIC's oral testimony during the October 17 hearing by discussing why it is urgent that the Council act now to protect health data privacy, providing an overview of the health data privacy risks that this bill will mitigate, and highlighting some of the most important aspects of CHIPPA.

[1] EPIC, *About EPIC*, https://epic.org/about/.

I. A Critical Moment to Protect Consumer Health Data

It is time for Council to act to meaningfully protect consumer health privacy. To set the stage: Congress has failed multiple times to pass a comprehensive federal privacy law or a law specifically aimed at protecting consumer health data. States are stepping in and enacting state-level comprehensive data privacy laws to fill this gap, as well as laws specific to consumer health data like Washington State's My Health My Data Act. By passing CHIPPA, the Council has the opportunity remain a leader in consumer protection and set the bar high for Congress to do the same.

a. Consumer Health Data Collection Falls Outside of HIPAA's Scope

Consumer health data collection has skyrocketed in recent years. The broad availability and convenience of smartphones and internet access has enabled "Americans to turn to apps and other technologies to track diseases, diagnoses, treatment, medications, fitness, fertility, sleep, mental health, diet and other vital areas[.]"[2] Our understanding of what constitutes health data has grown as data analysts and data brokers have demonstrated their ability to infer health-related insights from a widening range of data sources. For example, location data can become sensitive health data, like GPS data indicating that someone has visited a methadone or abortion clinic.[3] Location data can also reveal healthcare activity and related behavior.[4]

---

[2] Office of the Chair, *Statement of the Commission On Breaches by Health Apps and Other Connected Devices*, Fed. Trade Comm'n (Sept. 15, 2021), https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf.

[3] Leah R. Fowler, *8th Annual Symposium: Redefining & Regulating Health Data*, 21 Hous. J. Health L. &. Policy 1, 1-3 (2021), https://houstonhealthlaw.scholasticahq.com/article/31471-8th-annual-symposium-redefining-regulating-health-data.

[4] Kristen Cohen, Acting Associate Director, FTC Div. of Privacy & Identity Prot., *Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data*, Fed. Trade Comm'n Business Blog (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal.

Unbeknownst to many consumers, most of this health data collection is not regulated by the Health Information Portability and Accountability Act (HIPAA). Most of the apps, platforms, and companies that collect our most sensitive data fall outside of HIPAA's narrow scope because these companies are not HIPAA-covered entities.[5] For example, direct-to-consumer genetic testing companies like 23andMe are not HIPAA-covered entities and thus are not obligated under any federal law to safeguard highly sensitive consumer genetic data. In 2023, the company failed to protect the privacy of millions of users, exposing highly sensitive personal information in a massive data breach.[6]

Even in the context of a clearly HIPAA-covered entity like a hospital, data collection is not necessarily protected by HIPAA unless it is Protected Health Information (PHI) as defined by HIPAA. In other words, for HIPAA's protections to apply, both the collecting entity must be a HIPAA-covered entity *and* the type of data collected must be PHI. Currently, plenty of consumer health data is collected and maintained by HIPAA-covered entities like hospitals, but without HIPAA protections because the data is not considered PHI. For example, a 2023 study revealed that third-party tracking technologies, like cookies, collect data from 99% of hospital websites.[7] These third-party tracking technologies facilitate the profiling of visitors to the hospital websites, transferring data to other technology companies, advertisers, data brokers, or other entities without any regulatory oversight. This means that the vast majority of hospital websites were collecting consumers' personal information to use for unrelated purposes, like selling it to data brokers or using

[5] Office of Civil Rights, *Health Information Privacy: Covered Entities and Business Associates*, U.S. Dep't of Health and Human Serv., https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html (last updated Aug. 31, 2024).
[6] Jonathan Stempel, *23andMe settles data breach lawsuit for $30 million*, Reuters (Sept. 13, 2024), https://www.reuters.com/technology/cybersecurity/23andme-settles-data-breach-lawsuit-30-million-2024-09-13/.
[7] Ari B. Friedman et al., *Widespread Third-Party Tracking on Hospital Websites Poses Privacy Risks for Patients and Legal Liability for Hospitals*, 42 Health Affairs 508, 508-15 (Apr. 2023), https://doi.org/10.1377/hlthaff.2022.01205.

it to target consumers with advertising. Although the U.S. Department of Health and Human Services published guidance in response to the study outlining "HIPAA compliance obligations for regulated entities when using tracking technologies,"[8] the guidance is limited to HIPAA-covered PHI, and a federal court vacated a critical portion of the guidance soon after.[9]

Relatedly, CHIPPA should ensure any exemptions to its coverage are as narrow as possible, including making clear that the HIPAA exemption is data-level, not entity-level. While the intent of Section 11(a)(1)(A) was to exempt only the data that is covered by HIPAA, Section 11(a)(2)(A) muddies these waters. As it is currently written, this provision could function as an entity-level HIPAA exemption. CHIPPA exempts information "originating from, and intermingled to be indistinguishable […]"[10] from PHI maintained by a HIPAA-covered entity. Without further defining "intermingled" and/or "indistinguishable," it could be used as a loophole for HIPAA-covered entities to claim that any non-PHI consumer health data that is collected is "intermingled" and "indistinguishable" from other PHI retained by the HIPAA-covered entity. This reading could, in practice, allow HIPAA-covered entities like hospitals or insurance companies to avoid complying with CHIPAA for the non-PHI consumer health data that they collect. To avoid creating this loophole, CHIPPA should make clear what constitutes intermingled PHI and non-PHI consumer health data to the extent that it is "indistinguishable." If CHIPPA includes any exemptions at all, they should be limited to data-level exemptions. Exemptions should be limited to the *data* covered

[8] Office of Civil Rights, *Guidance: Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. Dep't of Health and Human Serv., https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last updated June 26, 2024).
[9] *See* Am. Hosp. Ass'n v. Becerra, — F. Supp. 3d ----, No. 4:23-cv-1110, 2024 WL 3075865 (N.D. Tex. June 20, 2024).
[10] Consumer Health Information Privacy Protection Act of 2024, §11, as introduced on July 12, 2024 (Bill 25-0930) [hereinafter *CHIPPA*].

by existing federal laws rather than exempting an entire entity simply because some personal data they handle falls under an existing law.

b. CHIPPA Can Address Significant Consumer Health Data Privacy Risks

The current gap in the regulation of consumer health data poses significant risks to consumers. The mismanagement or breach of sensitive health data can result in a range of privacy injuries, from stigma and humiliation to financial and reputational injuries. What's more, the largely unregulated data brokerage ecosystem that constantly collects, analyzes, and sells health data without consumer knowledge or consent poses stark privacy and data security risks to consumers. Data brokers sell health data, including mental health information,[11] to willing buyers including commercial entities, health insurance companies, law enforcement, and nearly any interested individual.

While the collection and sale of health data are only one piece of the enormous commercial surveillance ecosystem,[12] they pose unique risks to consumers. For example, health insurance companies can purchase and use information collected by data brokers to determine aspects of healthcare rates.[13] Health, demographic, and "lifestyle" information collected from any online activity—like purchasing plus-sized clothing or posting about feeling anxious or depressed from a recent divorce—can yield inferences for predicting health costs. All of this, from the surveillance and data collection to the sale and use of health data, is largely beyond the control of consumers.

---

[11] Joanne Kim, *Data Brokers and the Sale of Americans' Mental Health Data*, Duke University Cyber Policy Program (Feb. 2023), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/02/Kim-2023-Data-Brokers-and-the-Sale-of-Americans-Mental-Health-Data.pdf.
[12] *Id*.
[13] Marshall Allen, *Health Insurers Are Vacuuming Up Details About You – and It Could Raise Your Rates*, ProPublica (July 17, 2018), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates.

Consumers are becoming more aware of these issues, fueling momentum to enact stronger consumer health data privacy safeguards. On the state level, Washington, Nevada, and Connecticut have enacted laws similar to CHIPPA aimed at protecting consumer health data that falls outside of HIPAA's scope.[14] States have also passed more shield laws to protect consumer, patient, and provider privacy in areas like reproductive healthcare and gender-affirming healthcare.[15] Comprehensive data privacy laws on the state level also provide additional protections for categories of sensitive data, like health data.[16] On the federal level, the Federal Trade Commission has ramped up its health data privacy enforcement actions in recent years,[17] but these apply only after a privacy or data security violation has already occurred. With CHIPPA, DC can provide consumers with preventative safeguards for their consumer health data, mitigating potential risks or harms before they materialize.

II. The Council Should Maintain CHIPPA's Strong Provisions

CHIPPA would provide important safeguards for consumers' health data privacy in DC. This section will illustrate why provisions like the private right of action and geofence prohibition are central to CHIPPA's overall efficacy.

[14] SB 370, 82nd Sess. (Nev. 2023), https://www.leg.state.nv.us/App/NELIS/REL/82nd2023/Bill/10323/Text; Wash. Rev. Code § 19.373 (2023), https://app.leg.wa.gov/RCW/default.aspx?cite=19.373&full=true; 2023 Conn. Pub. Acts 23-56, https://www.cga.ct.gov/2023/act/Pa/pdf/2023PA-00056-R00SB-00003-PA.PDF.
[15] Southern California Alliance for Reproductive Justice, *State Shield Law Guide*, UCLA Law https://law.ucla.edu/academics/centers/center-reproductive-health-law-and-policy/shield-laws-reproductive-and-gender-affirming-health-care-state-law-guide (last visited Oct. 28, 2024). *See* David S. Cohen et al., *Abortion Shield Laws*, 2 NEJM Evid 1, 1-4 (Mar. 28, 2023), https://evidence.nejm.org/doi/10.1056/EVIDra2200280.
[16] *See* Keir Lamont & Jordan Francis, *The Expanding Scope of "Sensitive Data" Across US State Privacy Laws*, Tech Policy Press (Mar. 7, 2024), https://www.techpolicy.press/the-expanding-scope-of-sensitive-data-across-us-state-privacy-laws/.
[17] Suzanne Bernstein, *Data Minimization: Bolstering The FTC's Health Data Privacy Authority*, EPIC (July 13, 2023), https://epic.org/data-minimization-bolstering-the-ftcs-health-data-privacy-authority/.

a. CHIPAA's Private Right of Action is Necessary for Effective Enforcement

CHIPPA's private right of action rightly ties into DC consumer protection law.[18] As CHIPPA makes clear, a privacy violation should not be treated differently than any other unfair and deceptive trade practice. Individuals and groups of individuals who use online health services are in the best position to identify privacy issues and bring actions to vindicate their interests. Allowing consumers to enforce their own privacy rights preserves DC's resources, and statutory damages ensure that companies will face real consequences if they violate the law. During the October 17 hearing, the DC Attorney General's staff testified that a private right of action in CHIPPA is key for effective enforcement.

The inclusion of a private right of action is the most important tool a Legislature can give to their constituents to protect their privacy. A private right of action would impose enforceable legal obligations on companies. As Northeastern University School of Law Professor Woody Hartzog recently wrote with regard to a private right of action in the Illinois biometric privacy law:

> So far, only private causes of action seem capable of meaningfully deterring companies from engaging in practices with biometrics based on business models that inevitably lead to unacceptable abuses. Regulators are more predictable than plaintiffs and are vulnerable to political pressure. Facebook's share price actually rose 2 percent after the FTC announced its historic $5 billion fine for the social media company's privacy lapses in the Cambridge Analytica debacle. Meanwhile, Clearview AI specifically cited BIPA as the reason it is no longer pursuing non-government contracts. On top of that, Clearview AI is being sued by the ACLU for violating BIPA by creating faceprints of people without their consent. […] In general, businesses have opposed private causes of action more than other proposed privacy rules, short of an outright ban.[19]

[18] CHIPPA, *supra* note 10 at §3(c).
[19] Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI Now Institute (2020), https://ainowinstitute.org/regulatingbiometrics-hartzog.pdf.

The ACLU's suit against facial recognition company Clearview AI settled, with Clearview agreeing not to sell its face surveillance system to any private company in the United States.[20] Private rights of action are an effective mechanism to ensure that the rights in privacy laws are meaningful.

b. CHIPPA Can Help Ensure Access to Healthcare in DC for All, Including Reproductive Healthcare and Gender-Affirming Care

The privacy risks posed by underregulated consumer health data collection can hinder access to healthcare. Many people travel to the District to access all types of healthcare, including categories of healthcare that are under attack in other jurisdictions like reproductive and gender-affirming healthcare. There are two provisions in CHIPPA that would go a long way toward safeguarding access to all kinds of healthcare services in DC. First, the geofencing prohibition is central to limiting the collection of revealing location data. Geofencing is the use of technology like Wi-Fi or cell tower data to create a boundary around a physical location or to locate or collect data about a consumer within that boundary. Geofencing prohibitions are also central components of Washington,[21] Nevada,[22] and Connecticut's[23] health data privacy laws and an aspect of Maryland's comprehensive data privacy law.[24] CHIPPA prohibits geofencing within 2,000 feet from the perimeter of an entity that provides in-person health care services.[25]

This is an important provision because location histories—collected by many apps or websites on our phones or other devices—collect and retain location information without consumer

[20] Ryan Mac & Kashmir Hill, *Clearview AI Settles Suit and Agrees to Limit Sales of Facial Recognition database*, N.Y. Times (May 9, 2022), https://www.nytimes.com/2022/05/09/technology/clearview-ai-suit.html.
[21] Wash. Rev. Code § 19.373.080 (2023), https://app.leg.wa.gov/RCW/default.aspx?cite=19.373&full=true.
[22] SB 370, 82nd Sess. §31 (Nev. 2023), https://www.leg.state.nv.us/App/NELIS/REL/82nd2023/Bill/10323/Text.
[23] 2023 Conn. Pub. Acts 23-56 §2(a)(1)(C), https://www.cga.ct.gov/2023/act/Pa/pdf/2023PA-00056-R00SB-00003-PA.PDF.
[24] H.B. 567, 2024 Gen. Assemb., 446th Sess. §14-1604(3) (Md. 2024), https://mgaleg.maryland.gov/2024RS/Chapters_noln/CH_455_sb0541e.pdf.
[25] CHIPPA, *supra* note 10 at §9.

knowledge. If a person is at a hospital or a health clinic specializing in certain types of care like dialysis, methadone treatment, or reproductive care, that location information can immediately become health information. Consumers in DC should feel safe to seek healthcare without commercial surveillance tracking their every move to and from a health clinic.

Although abortion and gender-affirming care are legal and accessible in DC, this provision will play an important role in limiting the collection and use of location data for criminalizing reproductive healthcare or gender-affirming care for people visiting from out of state.[26] It will also provide safety and peace of mind for any person seeking in-person healthcare in DC. Consumer health data derived from location data should not be used to profile consumers or contribute to other health data privacy and security risks.

Second, CHIPPA should maintain its "consumer" definition to include any person "whose consumer health data is collected in the District."[27] Although the idea of narrowing the scope of the definition to DC residents was raised during the October 17 hearing, CHIPPA should maintain its current definition of consumer to be most effective. Not only would limiting CHIPPA's protections to DC residents weaken the overall efficacy of the law, but it would specifically kneecap the geofence provision. It may be even *more* critical for a person seeking healthcare in DC that may be otherwise illegal in their home state to have the protection of CHIPPA's geofence provision. Washington, DC is a welcoming city for tourists, residents, and frequent visitors from the broader mid-Atlantic and northeast region. This Committee should proudly ensure that CHIPPA's

[26] *See* Suzanne Bernstein, *The Role of Digital Privacy in Ensuring Access to Abortion and Reproductive Health Care in Post-Dobbs America*, American Bar Association Human Rights Magazine (June 3, 2024), https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/technology-and-the-law/the-role-of-digital-privacy-in-ensuring-access-to-reproductive-health-care/.
[27] CHIPPA, *supra* note 10 at § 8.

protections apply to anyone whose consumer health information is collected in DC, not just those who live within its city limits.

III. The Committee Should Strengthen CHIPPA by Improving Key Definitions and Incorporating Data Minimization Principles, Including a Ban on the Sale of Consumer Health Data

The Committee should strengthen key definitions like "consumer health data," "consumer," and "sharing," to effectively safeguard consumer health data in DC. Additionally, CHIPPA's structure should be grounded in a data minimization framework. In this way, the bill could both address the consent fatigue issue and provide stronger safeguards for consumer health data privacy.

a. "Consumer Health Data" Definition is Necessarily Broad

Another important aspect of CHIPPA is the definition of consumer health data. The bill defines consumer health data as "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."[28] The expansive scope of health data and health-related inferences that can be drawn from data collection require a broad definition like this one for CHIPPA's protections to be effective.

There are multiple ways that the Committee can address the valid concerns about consent fatigue stemming from such a necessarily broad definition of consumer health. First, the Committee should consider mirroring language from Nevada[29] and Connecticut's[30] consumer health data laws by adding the bolded language: "personal information that is linked or can reasonably be linked to a consumer **and that a covered entity uses to identify** the consumer's past, present, or future physical or mental health status." Adding this language maintains the necessary breadth of the

[28] CHIPPA, *supra* note 10 at §2(9).
[29] SB 370, 82nd Sess. §8 (Nev. 2023), https://www.leg.state.nv.us/App/NELIS/REL/82nd2023/Bill/10323/Text.
[30] 2023 Conn. Pub. Acts 23-56 §1(9), https://www.cga.ct.gov/2023/act/Pa/pdf/2023PA-00056-R00SB-00003-PA.PDF.

consumer health data definition while incorporating a more targeted evaluation of how that data is being used. For example, the purchase of a toothbrush may not be consumer health data on its own, but if a covered entity uses the information of that toothbrush purchase in an effort to "identify the consumer's past, present or future physical or mental health status"—through actions like profiling the consumer to reveal dental health patterns, selling or sharing it to a third party for dental advertising purposes, or combining data sets to reveal broader health information—the purchase of the toothbrush would then be considered consumer health data.

Relatedly, the Committee should strongly consider including inferences in the consumer health data definition. While the definition of "collect" includes reference to inferences, CHIPPA should mirror similar language in Washington[31] and Nevada's[32] consumer health data privacy laws that explicitly covers information extrapolated or inferred from other non-consumer health data. For example, Nevada's consumer health data definition (which is nearly identical to Washington's) includes "[a]ny information described in paragraph […] that is derived or extrapolated from information that is not consumer health data, including, without limitation, proxy, derivative, inferred or emergent data derived through an algorithm, machine learning, or any other means."[33]

b. Data Minimization Will Address Consent Fatigue and Disclosure Loophole

The Committee should include data minimization principles in CHIPPA to limit consent fatigue to consumers, more effectively and clearly outline data management requirements for covered operators, and close the disclosure loophole.

[31] Wash. Rev. Code § 19.373.010 (8)(b)(xiii) (2023), https://app.leg.wa.gov/RCW/default.aspx?cite=19.373&full=true.
[32] SB 370, 82nd Sess. §8(1)(d) (Nev. 2023), https://www.leg.state.nv.us/App/NELIS/REL/82nd2023/Bill/10323/Text.
[33] Wash. Rev. Code § 19.373.010 (8)(b)(xiii) (2023), https://app.leg.wa.gov/RCW/default.aspx?cite=19.373&full=true.

When consumers interact with a business online, they reasonably expect that their data will be collected and used for the limited purpose and duration necessary to provide the goods or services that they requested. For example, a consumer using a map application to obtain directions would not reasonably expect that their precise location data would be disclosed to third parties and combined with other data to profile them. And indeed, providing this service does not require selling, sharing, processing, or storing consumer data for an unrelated secondary purpose. Yet these business practices are widespread. Nearly every online interaction can be tracked and cataloged to build and enhance detailed profiles and retarget consumers.

A data minimization provision would also limit the ability of covered operators to list a seemingly endless number of "specified purposes" in disclosures to consumers. Tying the permitted use of consumer health data to the service or good requested by the individual would close this loophole that, as is it currently written in Section 4(a), would allow covered operators to use, retain, share, or sell consumer health data for any reason that it discloses as a "specified purpose."[34] Although the section later uses data minimization language to prohibit use inconsistent with the "specified purpose" without additional consent, the strength of that provision is weakened by not imposing limits on what can be a "specified purpose," nor tying that purpose to the service or good requested by the consumer. In other words, the prohibition on out-of-context uses of consumer health data is largely ineffective without limits on what a covered operator can disclose as a "specified purpose."

Data minimization offers a practical solution to a broken internet ecosystem by shifting the paradigm away from insufficient safeguards that rely on user consent and providing clear limits on how companies can collect and use data. Because consumer health data is widely considered to be

[34] CHIPPA, *supra* note 10 at §4(a).

sensitive data, CHIPPA should set a baseline requirement that entities only collect, use, and transfer consumer health data that is "strictly necessary and proportionate" to provide or maintain a product or service requested by the individual (or pursuant to certain enumerated purposes) and prohibit use of consumer health data for targeted advertising. Alternatively, the Committee could employ a "reasonably necessary" standard. A data minimization framework better aligns business practices with what consumers expect. It would also address the consent fatigue issue by effectively protecting consumer health data without requiring repeated authorizations.

Data minimization is essential for both consumers and businesses. Data minimization principles set much-needed standards for data management, providing clear guidance to businesses when designing and implementing systems for data collection, storage, use, and transfer. And data security will be improved because personal data that is not collected in the first place cannot be at risk of a data breach.

c. CHIPPA Should Prohibit the Sale of Consumer Health Data

One of the best ways to prevent consent fatigue for consumers is to put clear rules in place prohibiting particularly harmful data practices. For example, Maryland passed a comprehensive privacy law earlier this year that implements a ban on the sale of sensitive data, which includes consumer health data.[35] DC Council should adopt a similar approach and include a ban on the sale of consumer health data in CHIPPA. This prohibition would directly prevent some of the most egregious abuses of consumers' health information while still allowing legitimate uses of health information to continue uninterrupted, as long as the entity complies with CHIPPA's other provisions.

[35] H.B. 567, 2024 Gen. Assemb., 446th Sess. §14-4607(A)(2) (Md. 2024), https://mgaleg.maryland.gov/2024RS/Chapters_noln/CH_455_sb0541e.pdf.

Banning the sale of consumer health data would also limit the number of prompts consumers receive asking for their consent for various data practices. Consumers would no longer be asked to consent to the sale of their health information—a practice consumers would be unlikely to consent to in the first place if they felt they had any real choice, which is often not the case in a digital world that requires consumers to either consent or forfeit access to a website or app. Because there would be fewer consent pop-ups with a ban on the sale of health data in place, consumers may be more conscious and careful when companies do ask for their permission to use their data for other purposes. This type of provision also sets clear expectations for both businesses and consumers, which ensures companies understand their legal obligations in collecting and using consumer health data and enables consumers to know what to expect when a covered entity is collecting their consumer health data.

d. CHIPPA Must Protect Against Downstream Data Use

For CHIPPA's restrictions on downstream data uses to be most effective, the bill should reflect the reality of the personal data ecosystem. For example, companies often "share" data and then purchase advertisements based on that "sharing"[36] through arrangements that would not qualify as "selling" under CHIPPA. If the bill defines "sharing" and "selling" separately, it should make clear that both are included in subsequent, relevant sections. For example, Section (8)(a) requires consumer authorization prior to selling consumer health data, but it omits "sharing," which can be just as harmful for privacy.[37] The section also omits "sharing" from the requirements in (8)(f) related

[36] *See* Suzanne Bernstein, *GoodRx Enforcement Action Signals FTC's Invigorated Commitment to Health Privacy*, EPIC (Feb. 9, 2023) ("The complaint illustrated how GoodRx further exploited the personal information it shared with Meta, using Meta's ad targeting program to target advertisements to GoodRx users based on their health information.").
[37] CHIPPA, *supra* note 10 at §8(a).

to contractual requirements for selling consumer health data.[38] Those requirements should extend to contracts where consumer health data is "shared" with third parties, not limited to selling.

IV. Conclusion

Thank you for the opportunity to further contribute to the record. CHIPPA is a meaningful and timely step towards consumer health data privacy in DC. EPIC is happy to serve as a resource to the Committee on these issues. Please contact Suzanne Bernstein at bernstein@epic.org with any questions.

Respectfully submitted,

/s/ *Suzanne Bernstein*
Suzanne Bernstein
EPIC Counsel

/s/ *Kara Williams*
Kara Williams
EPIC Law Fellow

[38] *Id*. at §8(f).