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

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

U.S. SENATE COMMITTEE ON HEALTH, EDUCATION, LABOR, AND PENSIONS

Request for Information Regarding Health Privacy

September 28, 2023

The Electronic Privacy Information Center (EPIC) submits these comments in response to the U.S. Senate Committee on Health, Education, Labor, and Pensions Request for Information (RFI) related to safeguarding patient privacy and health data posted on September 7, 2023.[1] Through this RFI, the Committee seeks to understand the privacy and data security implications of new technologies that create and expand the collection of health data, including contexts where such data is not protected by the HIPAA framework.[2]

EPIC is a public interest research center in Washington, D.C., established in 1994 to focus on public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[3] EPIC regularly advocates for health data privacy and security safeguards, both in HIPAA-covered and non-HIPAA-covered contexts.[4] Health data is a particularly sensitive category of personal data. The Committee should scrutinize the commercial surveillance systems that collect, process, and share health data because they pose unique and serious privacy and security risks for patients and consumers.

We have listed below each of the Committee's questions addressed in these comments, followed directly by our response. We have also provided additional references and resources in a bullet-point list after each response.

General Privacy Questions

3. Should any or all of these entities have a duty of loyalty to consumers/patients?

a. How could a duty of loyalty be imposed in a way that maximizes the safeguarding of consumer/patient data without creating burdensome implementation challenges? Should requirements of such a duty be based on the sensitivity of collected data? Please explain.

---

[1] U.S. Senate Committee on Health, Education, Labor, and Pensions, *Request for Information on Health Privacy* (Sept. 7, 2023), https://www.help.senate.gov/imo/media/doc/health_privacy_rfi.pdf.
[2] *Id*.
[3] EPIC, *About Us* (2023), https://epic.org/about/.
[4] *See* EPIC, *Health Privacy* (2023), https://epic.org/issues/data-protection/health-privacy/.

Health data is particularly sensitive, and its collection and storage pose heightened privacy and data security risks to consumers and patients. Entities collecting, retaining, and sharing health data should be subject to heightened obligations protect the privacy and security of health data. EPIC has advocated for the adoption of data minimization rules directing entities collecting health data (and other sensitive data) to restrict their collection, use, disclosure, and retention of that data to which is strictly necessary. One example of a duty of loyalty centered around data minimization principles is the proposed American Data Privacy and Protection Act (ADPPA).

- EPIC's Comments for FTC's ANPR on Commercial Surveillance & Data Security: *Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystems*[5]
  - Introduction (p. 1)
  - The Scope of Covered Data (p. 24)
  - Data Minimization (p. 30)
- Proposed American Data Privacy and Protection Act (ADPPA)[6]

Health Information Under HIPAA

3. Are existing safeguards on the disclosure of health care data to law enforcement official sufficient?

No, in the wake of *Dobbs v. Jackson Women's Health Organization*, the collection of reproductive health data—both within the HIPAA context and in non-HIPAA commercial settings—can lead to or facilitate criminal intervention. In recent comments to the Department of Health and Human Services (HHS) regarding proposed HIPAA Privacy Rule changes, EPIC applauded HHS's proposed amendment to prohibit regulated entities from disclosing Protected Health Information (PHI) for civil, criminal, or administrative investigations related to reproductive healthcare. Additionally, EPIC urged that law enforcement should be required to obtain a warrant supported by probable cause for PHI. EPIC also recommended that HHS extend this warrant requirement and/or provide other heightened protections for PHI related to gender-affirming care and hormone treatments.

[5] Comments of EPIC to the FTC Proposed Trade Regulation Rule on Commercial Surveillance & Data Security, https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf [hereinafter EPIC FTC Comments on Commercial Surveillance].
[6] H.R. 8152, 117th Cong. (2022), https://www.congress.gov/bill/117th-congress/house-bill/8152/text.

- EPIC's Comments to the Department of Health and Human Services on the Notice of Proposed Rulemaking regarding HIPAA Privacy Rule to Support Reproductive Health Care Privacy[7]
- The Rise of Pregnancy Criminalization: A Pregnancy Justice Report[8]
- Human Rights Crisis: Abortion in the United States After Dobbs[9]

Collection of Health Data

1. ***How should consumer/patient consent to an entity to collect information be structured to minimize unnecessary data gathering? When should consent be required and where should it be implied?***

Entities should be required to limit the collection and processing of health data to what is strictly necessary and proportionate to the specific purposes for which it was collected. Even the most sophisticated patient or consumer cannot fully understand the complex, extractive web of commercial surveillance practices touching on health data. Privacy policies and other disclosures "are only valuable in conjunction with substantive limits on data collection and use."[10]

- EPIC Analysis: Data Minimization: Centering Reasonable Consumer Expectation in the FTC's Commercial Surveillance Rulemaking[11]
- EPIC Data brokers comments[12]
  - The unavoidability of the data trade (p. 16)
  - Recommendation to ban disclosure and purchase of sensitive data (p. 74)
- EPIC Analysis: Data Minimization: Bolstering the FTC's Health Data Privacy Authority[13]

---

[7] EPIC, Comments to HHS on HIPAA Privacy Rule to Support Reproductive Health Care Privacy, 88 Fed. Reg. 23,506 (June 16, 2023), https://epic.org/documents/comments-of-epic-on-hhs-proposed-rulemaking-to-modify-hipaa-privacy-rule-to-support-reproductive-health-care-privacy/.
[8] Pregnancy Justice, *The Rise of Pregnancy Criminalization* (2023), https://www.pregnancyjusticeus.org/rise-of-pregnancy-criminalization-report/.
[9] Human Rights Watch, *Human Rights Crisis: Abortion int he United States After Dobb*s, (Apr. 18, 2023), https://www.hrw.org/news/2023/04/18/human-rights-crisis-abortion-united-states-after-dobbs.
[10] EPIC FTC Comments on Commercial Surveillance, *supra* note 5 at 3.
[11] Suzanne Bernstein, *Data Minimization: Centering Reasonable Consumer Expectation in the FTC's Commercial Surveillance Rulemaking*, EPIC Analysis (Apr. 20, 2023), https://epic.org/data-minimization-centering-reasonable-consumer-expectation-in-the-ftcs-commercial-surveillance-rulemaking/.
[12] EPIC, Comments to CFPB on RFI Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information, 88 Fed. Reg. 16, 951 (July 14, 2023) https://epic.org/wp-content/uploads/2023/07/EPIC-CFPB-data-brokers-RFI-comments-071423.pdf [hereinafter *EPIC CFPB Comments on Data Brokers*].
[13] Suzanne Bernstein, *Data Minimization: Bolstering the FTC's Health Data Privacy Authority*, EPCI Analysis (July 13, 2023), https://epic.org/data-minimization-bolstering-the-ftcs-health-data-privacy-authority/.

- EPIC FTC Comments on Commercial Surveillance[14]
  - Data Minimization (p. 30).
- EPIC Analysis: Reproductive Privacy in the Age of Surveillance Capitalism[15]

Biometric Data

1. To what extent should biometric data be considered health care information when not used for health care purposes?

Biometric data that reveals health information in commercial settings is frequently created, collected, retained, and shared without meaningful oversight. Some examples of biometric data that can reveal health information are more obvious, like heart rate monitors and blood oxygen trackers found in smartwatches and fitness trackers. Other biometric data technologies that can lead to inferential health information include iris authenticators, voice and facial recognition, and "emotion detection" systems. The mismanagement of health information drawn from biometric data can pose significant risks to consumers, from security breaches to stigma and humiliation to financial and reputational injuries.

- EPIC FTC Comments on Commercial Surveillance[16]
  - Biometric technologies for commercial surveillance (p. 98)

Genetic Information

1. How should genetic information collected by commercial services be safeguarded?

The Direct to Consumer (DTC) genetic testing market has continued to expand and diversify into different types of testing, including evaluating health risks such as carrier screening or cancer predisposition, determining ancestry, and pharmacogenomic purposes. There should be heightened privacy and data security requirements for personal data processed in the course of DTC genetic testing. Because DTC genetic testing is usually a commercial activity unlike the genetic testing done in hospital or healthcare settings, the genetic and sensitive health information implicated is typically not protected by HIPAA privacy safeguards.

- EPIC Vitagene Comment letter[17]

[14] EPIC FTC Comments on Commercial Surveillance, *supra* note 5.
[15] Sara Geoghegan & Dana Khabbaz, *Reproductive Privacy in the Age of Surveillance Capitalism*, EPIC Analysis (July 7, 2022), https://epic.org/reproductive-privacy-in-the-age-of-surveillance-capitalism/.
[16] EPIC FTC Comments on Commercial Surveillance, *supra* note 5.
[17] EPIC, Comments on FTC's Proposed Order & Settlement with Vitagene, Inc., FTC File No. 192-3170 (July 24, 2023), https://epic.org/documents/comments-of-epic-in-re-the-federal-trade-commissions-proposed-order-settlement-with-vitagene-inc/.

- Consumer Reports: The Privacy Problems of Direct-to-Consumer Genetic Testing[18]

Location Data

1. ***How should location data that is being collected at a health care facility or website or other digital presence maintained by a health care entity be treated? For example, location data could potentially disclose a patient's health condition or treatment plan. Should this data be treated differently from the same data collected by non-health care entities?***

Location data can reveal health information about a consumer or patient. On its own, location data can yield health-related inferences like the fact that someone has visited an abortion clinic or a dialysis center. Combined with other personal information, location data can be used by brokers to reveal even more—and more sensitive—health information.

- EPIC Data brokers comments[19]
  - The Participants and victims of the data broker market (p 6)
  - Health data collection (p. 16)
- N.Y. Times: In a Post-Roe World, the Future of Digital Privacy Looks Even Grimmer[20]

Sharing of Health Data

1. ***Should there be an opt-in method of data collection for health data outside of the HIPAA framework versus and opt-out method? Please Explain.***

As noted above, the most important step Congress could take to safeguard personal health information is imposing an across-the-board data minimization standard that limits the collection and processing of health information (and indeed, all sensitive personal data) to what is strictly necessary. Placing this obligation on businesses and health care providers—rather than on overwhelmed consumers—would provide meaningful, systemic privacy protection rather than an endless parade of unintelligible consent requests. However, in exceptionally risky processing contexts—such as the transfer of personal health data to a third party—this minimization standard could backstopped with a requirement to obtain affirmative opt-in consent from the consumer.

[18] Catherine Roberts, *The Privacy Problems of Direct-To-Consumer Genetic Testing*, Consumer Report (Jan. 14, 2022), https://www.consumerreports.org/health/dna-test-kits/privacy-and-direct-to-consumer-genetic-testing-dna-test-kits-a1187212155/.
[19] EPIC CFPB Comments on Data Brokers, *supra* note 12.
[20] Natasha Singer & Brian X. Chen, *In a Post-Roe World, th Future of digital Privacy Looks Even Grimmer*, N.Y. Times (June 22, 2023), https://www.nytimes.com/2022/07/13/technology/personaltech/abortion-privacy-roe-surveillance.html.

Even with informed consent, many of the downstream risks of health data collection (or other data collected that reveals health information) are unavoidable due to the largely unregulated data broker ecosystem. For example, "health insurance companies can purchase and use information collected by data brokers to determine healthcare rates. 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 to make an insurance policy decision, is largely beyond the control of consumers."[21]

In comments to the FTC, EPIC applauded the FTC's recent effort to expand the Health Breach Notification Rule (HBNR) to cover mobile apps and other digital service providers. The proposed Rule clarifies that a breach of security under the HBNR includes the unauthorized acquisition of covered health data that occurs because of a data breach or unauthorized disclosure. In addition to intentionally sharing health data with an unauthorized party, EPIC encouraged the FTC to further clarify that a breach of security also includes a scenario in which an entity collects more identifiable health information than necessary to provide the product requested by the consumer.[22]

- EPIC Analysis: Data Minimization: Bolstering the FTC's Health Data Privacy Authority[23]
- ProPublica: Health Insurers are Vacuuming Up Details About You – And It Could Raise Your Rates[24]
- Comments of EPIC, FTC Proposed Rulemaking to Amend the Health Breach Notification Rule[25]

[21] Suzanne Bernstein, *Data Minimization: Bolstering the FTC's Health Data Privacy Authority*, EPCI Analysis (July 13, 2023), https://epic.org/data-minimization-bolstering-the-ftcs-health-data-privacy-authority/.
[22] EPIC, Comments to the FTC on Proposed Rulemaking to Amend the Health Breach Notification Rule, 88 Fed. Red. 37,819 (Aug. 8, 2023), https://epic.org/documents/epic-comments-to-the-ftc-on-proposed-rulemaking-to-amend-the-health-breach-notification-rule/.
[23] Suzanne Bernstein, *Data Minimization: Bolstering the FTC's Health Data Privacy Authority*, EPCI Analysis (July 13, 2023), https://epic.org/data-minimization-bolstering-the-ftcs-health-data-privacy-authority/.
[24] 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.
[25] EPIC, Comments to the FTC on Proposed Rulemaking to Amend the Health Breach Notification Rule, 88 Fed. Red. 37,819 (Aug. 8, 2023), https://epic.org/documents/epic-comments-to-the-ftc-on-proposed-rulemaking-to-amend-the-health-breach-notification-rule/.

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

Conclusion

We applaud the Committee's attention to the important issues shaping health privacy for consumers and patients. The ongoing and often unregulated collection, retention and sharing of sensitive personal data like health information poses serious privacy and data security risks. More can be done to protect patient privacy both within and beyond the HIPAA framework. We are eager to engage with the Committee further on the issues raised in our comment, including health data privacy, data minimization, data security, automated decision-making, and the data broker ecosystem.

Respectfully submitted,

/s/ *John Davisson*
John Davisson
EPIC Director of Litigation & Senior Counsel

/s/ *Suzanne Bernstein*
Suzanne Bernstein
EPIC Law Fellow