March 6, 2023

Travis Hall
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

I. Introduction

On January 20, 2023, the National Telecommunications and Information Administration (NTIA) issued a Request for Comment (RFC) on "the extent to which the collection, processing, sharing, and use of data can lead to higher risks for some communities, exacerbate structural inequities, or contribute to their erosion."[1] The Center for Health Law and Policy Innovation of Harvard Law School and the Harvard Cyberlaw Clinic submit this comment to highlight threats to privacy, equity, and civil rights posed by the use of health-related data in general, and reproductive health data in particular.

Traditionally, information about individuals' health has been held primarily by health care providers and insurers—entities that are governed by the Health Insurance Portability and Accountability Act Privacy Rule (HIPAA).[2] Now, as technology increasingly mediates individuals' relationship with health care, application developers, mobile service providers, and other technology companies have greater access to sensitive health care data. With increased access comes an increased risk of improper disclosure, whether accidental or intentional.

Beyond the harm implicit in exposure of private information, improper exposure of health data can cause financial, emotional, or physical harm to marginalized populations,

[1] National Telecommunications and Information Administration, Dept. of Commerce, *Privacy, Equity, and Civil Rights Request for Comment*, 88 Fed. Reg. 3714-20 (Jan. 20, 2023) [hereinafter "RFC"].
[2] *See* 45 C.F.R. § 160.102.

including older adults,[3] immigrants,[4] and members of the LGBT community.[5] Reproductive health care data, which is particularly sensitive data in today's legal landscape, exposes women and pregnant people to increased risk of coercion, violence, and even criminal liability. This comment describes several risks associated with improper disclosure of health care data in detail, explains the primary sources of such disclosures, and offers recommendations for addressing the disproportionate impact of disclosures on underserved and marginalized communities.

II. High-Risk Areas of Health Records and Marginalized Communities

Health data covers all aspects of individuals' lives. From chronic conditions to financial information used to pay for visits to personal struggles revealed to therapists,[6] health care data paints an intimate picture of a person's life. Disclosure of such data can lead to stigmatization, threats to safety and security, financial harm, and reputational harm in the workplace. Such harms can impact anyone but marginalized communities often suffer the most. This section responds to RFC Question 2.a by describing four ways in which collection and processing of health data, including reproductive health data, causes disproportionate harm to marginalized groups.

a. Health data can be used to defraud vulnerable individuals.

Health data often combines personally identifying information, such as a person's birthday or social security number, and billing information. This combination of data already makes health records an attractive target for identity thieves. Furthermore, health care data can be used in spear phishing attacks, a form of fraud in which criminals pose as a trusted source and send texts or emails containing malicious links or instructions.[7] In 2020 and 2021, the Department of Health and Human Services identified health sector-related attacks ranging from targeted LinkedIn messages to efforts by nation states to target medical researchers.[8]

---

[3] Jingjin Shao, Qianhan Zhang, Yining Ren, Xiying Li, & Tian Lin, *Why Are Older Adults Victims of Fraud? Current Knowledge and Prospects Regarding Older Adults' Vulnerability to Fraud*, 31 J. OF ELDER ABUSE & NEGLECT 225 (2019), DOI: 10.1080/08946566.2019.1625842.

[4] *Four Charged in $32 Million Health Care Fraud Scheme*, DEP'T OF JUSTICE OFFICE OF PUBLIC AFFAIRS (Mar. 2, 2021) https://www.justice.gov/opa/pr/four-charged-32-million-health-care-fraud-scheme.

[5] Alex Lemberg, *Hackers Made Me Lose My Job!: Health Data Privacy and Its Potentially Devastating Effect on the LGBTQ Population*, 47 GOLDEN GATE U. L. REV. 175 (2017), *available at* https://digitalcommons.law.ggu.edu/ggulrev/vol47/iss2/10.

[6] Mayo Clinic, *Personal Health Records and Patient Portals* (June 4, 2022), https://www.mayoclinic.org/healthy-lifestyle/consumer-health/in-depth/personal-health-record/art-20047273.

[7] In a spear phishing attack, a criminal uses personal information (often obtained from a data breach) to gain a victim's trust. *See What is a Phishing Attack?*, CLOUDFLARE (Mar. 3, 2023), https://www.cloudflare.com/learning/access-management/phishing-attack/.

[8] Dep't of Health and Human Services Cyber Security Program, *Phishing Campaigns Demonstrate Importance of User Training and Awareness* (Sept. 2, 2021), https://www.hhs.gov/sites/default/files/phishing-analyst-note-tlpwhite.pdf.

Health care data is particularly hazardous in the wrong hands because many people assume anyone with medical information is a trusted actor. For example, an attacker could use prescription data to send a false email to the victim claiming to be a health provider and obtain additional personal information or financial records. Using this playbook and impersonating health care providers, criminals can use leaked data to gain the victims' trust after the initial data breach and further defraud them.

Spear phishing attacks using health data are likely to disproportionately impact older individuals, who interact with health care more frequently than the average individual.[9] In addition, some older adults struggle with interacting with computerized systems that are now critical to health care access.[10] Perhaps for these reasons, spear phishing attacks are especially common in Medicare fraud.[11]

b. Disclosure of reproductive health data can increase the risk of abuse.

In addition to financial and emotional harm, disclosure of health data—in particular, reproductive health data—creates significant risks for abuse or intimate partner violence. According to a 2014 study, between 6 and 22 percent of women who have abortions report recent violence from an intimate partner.[12] This is not limited to women who have obtained an abortion; an abortion turn-away study found that women who had not terminated a pregnancy suffered from higher rates of intimate partner violence from the male involved in the pregnancy.[13]

Intimate partner abuse can also take the form of reproductive coercion. Reproductive coercion is broadly defined as explicit behaviors by one partner to promote pregnancy that is unwanted by the birthing partner. Reproductive coercion can take many forms, including interference with contraception or threatening a partner who does not want to become pregnant.[14]

---

[9] INSTITUTE OF MEDICINE: THE NATIONAL ACADEMIES, *RETOOLING FOR AN AGING AMERICA BUILDING THE HEALTHCARE WORKFORCE* 39 (2008), https://www.ncbi.nlm.nih.gov/books/NBK215400/.
[10] Shao et al., *supra* note 3.
[11] Gema de las Heras, *Stay Away From Scams This Medicare Open Enrollment Period*, FED. TRADE COMM'N (Nov. 4, 2022), https://consumer.ftc.gov/consumer-alerts/2022/11/stay-away-scams-medicare-open-enrollment-period-0.
[12] Ellen Wright Clayton, Peter J Embí, & Bradley A Malin, *Dobbs and the Future of Health Data Privacy for Patients and Health Care Organizations*, 30 J. AM. MED. INFORMATICS ASS'N 155 (2022), https://doi.org/10.1093/jamia/ocac155.
[13] Sarah C.M. Roberts, M. Antonia Biggs, Karuna S. Chibber, Heather Gould, Corinne H. Rocca, & Diana Greene Foster, *Risk of Violence from the Man Involved in the Pregnancy After Receiving or Being Denied an Abortion*, 12 BMC MED. 144 (2014), DOI: 10.1186/s12916-014-0144-z.
[14] Karen Trister Grace & Jocelyn C. Anderson, *Reproductive Coercion: A Systematic Review*, 19 TRAUMA, VIOLENCE & ABUSE 371 (2018), DOI: 10.1177/1524838016663935.

Disclosure of reproductive health data, whether it suggests pregnancy, non-pregnancy, or abortion, can drastically increases the risk for individuals in abusive relationships. With more and more sources of such data, the risk that an abusive partner is able to discover information about a person's reproductive care and status is ever-growing.

c. Disclosure of reproductive health data can increase the risk of criminalization.

After the decision in *Dobbs* permitting increased criminalization of abortion, privacy of reproductive health care data has become a national concern. A patch work of legislation has arisen, both in states that criminalize abortion and states seeking to protect their own residents from prosecution. Several articles from both medical and legal professionals have recognized legal risks that arise from this patch work of criminal law.[15] Many of these risks arise from exemptions in HIPAA permitting disclosure of protected health information by health care providers to law enforcement agencies.[16]

Other risks arise from entities that are not covered by HIPAA in the first place, including websites, search engines, and mobile service providers.[17] Even prior to *Dobbs*, internet search results have been used as evidence against individuals who have self-induced abortions.[18] Other forms of digital evidence that could be obtained from non-HIPAA covered entities include a person's location, call history, social media posts, or app usage information.[19] Such evidence is disproportionately likely to be obtained from younger, lower-income, and non-white individuals.[20] Members of these groups are more likely to depend on smartphones for internet access, use traceable payment systems like apps or Electronic Benefit Transfer cards, and have their devices seized during police interactions.[21] Moreover, this evidence is more likely to be used against lower income and Black women, who have consistently been disproportionately targeted in criminal proceedings involving reproductive choices.[22]

---

[15] Carmel Shachar, *HIPAA, Privacy, and Reproductive Rights in a Post-Roe Era*, 328 [J]AMA 417 (2022), doi:10.1001/jama.2022.12510; *see* Aziz Z. Huq & Rebecca Wexler, *Digital Privacy for Reproductive Choice in the Post-Roe Era*, 97 N.Y.U. L. REV., U. CHI. PUB. L. Working Paper No. 812 (2022), DOI: 10.2139/ssrn.4191990.
[16] *See* 45 C.F.R. § 164.512(f). While HIPAA reform is an essential element of safe, private access to reproductive health care, the authors acknowledge that such reform is beyond the scope of this comment.
[17] *See* Daly Barnett, *Security and Privacy Tips for People Seeking an Abortion*, ELEC. FRONTIER FOUND. (June 23, 2022), https://www.eff.org/deeplinks/2022/06/security-and-privacy-tips-people-seeking-abortion.
[18] Cynthia Conti-Cook, *Surveilling the Digital Abortion Diary*, 50 U. BALT. L. REV. 1, 48-51 (2020), DOI: 10.2139/ssrn.3666305.
[19] *See id.* at 51-56.
[20] *See id.* at 29.
[21] *See id.* at 29-34.
[22] *See generally* Lynn M. Paltrow & Jeanne Flavin, *Arrests of and Forced Interventions on Pregnant Women in the United States, 1973–2005: Implications for Women's Legal Status and Public Health*, 38 J. HEALTH POLITICS POL. & L. 299 (2013). DOI: 10.1215/03616878-1966324.

The pervasiveness of reproductive health data collection and the prevalence of government requests of user data from tech companies[23] puts users' reproductive health care information at risk. Companies subject to U.S. law are required to disclose this user data for legal purposes, regardless of where the company stores the data.[24] While some states have enacted shield laws to protect abortion providers from out of state litigation,[25] there are many unanswered legal questions related to the interstate transmission of reproductive health data. Until such questions are answered, individuals who seek, obtain, provide, or facilitate access to abortions are at risk of criminal liability.

d. Shared data can be used to infer—and reveal—private information, including reproductive health information.

While direct collection and disclosure of health data is a significant concern, even seemingly innocuous personal data can be used to infer sensitive health information. By combining such shared information with data from other sources, companies can infer information about users' health beyond what their families and doctors may know.

Reproductive health information is no exception to this concern. In 2012, Target analyzed historical buying data for individuals who signed up for baby registries to identify products that individuals who were likely to be pregnant would buy.[26] By applying this data to new purchases, Target could predict not only if a shopper was pregnant, but how late in their pregnancy the shopper was. For instance, when someone suddenly starts buying scent-free soap and cotton balls, it "signals they could be getting close to their delivery date."[27] Target used this data to send coupons for baby products to pregnant shoppers, timed to very specific stages of their pregnancy.[28] This resulted in gross violations of privacy, such as when Target sent coupons for baby clothes and cribs to a teenage girl at the place where she lived with her father—who did not know she was pregnant.[29]

This kind of inferential invasion of privacy shows how "big data" and automated decision-making can result in harmful outcomes to specific populations of users.[30] It is not hard to

---

[23] For the period of 2013-2020, the U.S. government made at least 23,972 user data requests from Apple, which is 56% of the total requests that the tech giant had received. *See* Antanis Rimeikis, *The Data Flows: How Private Are Popular Period Tracker Apps?*, SURFSHARK BLOG (Feb. 28, 2023), https://surfshark.com/blog/period-track-app-data-privacy.

[24] *Id.*

[25] David S. Cohen, Greer Donley, & Rachel Rebouché, *The New Abortion Battleground*, 123 COLUM. L. REV. 1 (2022), DOI: 10.2139/ssrn.4032931.

[26] Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=4fde15bc6668.

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *See* RFC at 3718.

imagine a father reacting poorly to finding out his daughter was pregnant via a Target mailing. Decisions to reveal pregnancy, abortion, and other reproductive health information to family members should be left up to individuals, not third parties.

III. Sources of Reproductive Health Data That Increase Vulnerability

Health data can be pulled (and, as described above, inferred) from a variety of sources. Importantly, much of this data is not governed by federal privacy and security standards for protected health information.

Understanding these sources of reproductive health data is vital to answering question 1.e., concerning the development of effective proposals to improve privacy protections and mitigate disproportionate harms of privacy invasions on marginalized communities. In response to RFC Question 3.b, this section describes two technologies that warrant particularly rigorous scrutiny for their potential to invade privacy and enable discrimination.

a. Smartphone-Based Apps

Smartphone apps provide a wealth of personal data, often far beyond what users expect. Apps for contraception, period tracking, and fertility tracking collect copious amounts of sensitive information about the length and specific dates of users' menstrual cycles and ovulation, sexual activity, and potential abortions, miscarriages, and pregnancies.[31] A study of 20 popular period tracking apps revealed that all of the studied apps collected an "above-average amount of data," beyond information about menstrual cycles, and nearly half made user data available for third-party advertising.[32] Through techniques such as tracking pixels and app-to-app integrations, this health data is often connected with other personal data, such as users' names, email usage, location, purchase histories, advertising profiles, and more.[33]

Some, but not all, of these apps are subject to regulatory control. FDA-regulated apps for contraception are defined as devices that provide "user specific fertility information for preventing a pregnancy" and include "an algorithm that performs analysis of patient-specific data (e.g., temperature, menstrual cycle dates) to distinguish between fertile and nonfertile days", then provide "patient-specific recommendations related to contraception."[34] FDA regulations require contraception app developers to provide a

---

[31] Cat Zakrzewski, *Abortion Rights Advocates Turn to Digital Privacy Tools to Fight Restrictive Laws*, WASH. POST (May 4, 2022), https://www.washingtonpost.com/technology/2022/05/04/abortion-digital-privacy/.
[32] Rimeikis, *supra* note 23.
[33] *Id.*
[34] Leah R. Fowler & Michael R. Ulrich, *Femtechnodystopia*, 21-22 (Forthcoming 2023), DOI: 10.2139/ssrn.4099764.

documented cybersecurity vulnerability and management process to assure software functionality.[35]

On the other hand, apps for period and fertility tracking, which collect similar data, are rarely regulated in the same way. In fact, the majority of period and fertility tracking apps are not FDA regulated at all because, according to the FDA, these apps are simply designed to maintain or encourage "a healthy lifestyle."[36] Accordingly, there is increased risk that developers will maintain insufficient security practices and, ultimately, of improper disclosure of reproductive health data.

Ultimately, with regulated and unregulated apps alike, users are vulnerable to having their sensitive information disclosed further by the app company. For example, when clicking through an app's terms of service, users may unwittingly "agree" that their information can be shared with company partners, used by advertisers, and even sold to brokers. And, even where reproductive health data is not shared commercially, it remains available to government entities that may seek to police people's pregnancies.[37]

b. Mobile and Internet Usage Data

Another avenue of unregulated access to reproductive health data comes from users' mobile network and internet usage. Modern smartphones track data about individuals' calls, texts, and location.[38] Calls and texts are generally only accessible to law enforcement agents—or someone with physical access to a phone.[39] However, location data is often shared via apps, and can be used to target users with advertisements.[40] Anti-abortion groups and crisis pregnancy care centers have already used this technique, called geofencing, to disseminate anti-abortion messaging to mobile devices in and around reproductive health clinics that offer full-spectrum care.[41]

An individual's internet activity can also be a source of reproductive health data. A search history with questions concerning pregnancy, abortions, or menstrual cycles provides insight into a person's reproductive health, including their intention to become pregnant or obtain an abortion.[42] If this information is discovered by an abusive partner, it can lead

---

[35] *See* 21 C.F.R. § 884.5370.
[36] Fowler & Ulrich, *supra* note 34, at 6.
[37] *Id.* at 18.
[38] *Keep Your Abortion Private and Secure*, DIGITAL DEFENSE FUND, https://digitaldefensefund.org/ddf-guides/abortion-privacy/#history.
[39] Kendra Albert, Maggie Delano, & Emma Weil, *Fear, Uncertainty, and Period Trackers*, MEDIUM (June 28, 2022), https://medium.com/@Kendra_Serra/fear-uncertainty-and-period-trackers-340ab8fdff74.
[40] *Keep Your Abortion Private and Secure*, *supra* note 38.
[41] *See In re Copley Advertising, LLC,* No. 1784- CV-01033 (Mass. Super. Ct. Apr. 4, 2017).
[42] *See* Albert et al., *supra* note 39.

to serious physical risk.[43] Moreover, internet usage information can be—and has been—used in prosecutions against women who have miscarried.[44]

Location, search history, and other usage data is increasingly easy for both private and public actors to obtain. A person who stops by a reproductive health clinic or explores abortion options online might find themselves targeted by unwanted advertising, harassment, or even law enforcement investigations. Conversely, a person who wishes to avoid such unwanted attention may forego obtaining important, even life-saving, health information.

IV. Principles for Regulatory Reform

The discussion above highlights significant shortcomings in the current regulatory framework with respect to protecting health data and how those shortcomings pose risks of serious harm to individuals. In response the RFC Question 5, this section offers four principles to guide the development of regulatory frameworks that address the disproportionate harms experienced by marginalized communities due to the collection, creation, processing, use, and disclosure of reproductive and other health data.

a. Health data should be treated as distinct from commercial data.

With the proliferation of medical apps for smartphones, real-time health data is increasingly available to health care providers. This market is poised for rapid growth, and apps linked directly to health care are likely to be an important part of patient care in the next decade. However, there are currently no regulations that prohibit non-health care providers from tapping into the same source of data. As a result, some app developers have created a business model where health data is collected and then sold directly to advertisers.

The FTC's recent action against GoodRx is a leading example of an app company inappropriately collecting and selling health data.[45] However, the FTC's complaint is limited to GoodRx's violation of the Health Breach Notification Rule, because GoodRx sent out customer data to third parties without approval. If GoodRx had informed its customers, it might have gotten away with profiting off of health data without regard to consumer harm. Regulatory reforms must more directly address the privacy, equity, and civil rights concerns posed.

---

[43] *See supra* Section II.b.

[44] *See* Conti-Cook, *supra* note 18.

[45] Press Release, Fed. Trade Comm'n, *FTC Enforcement to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising* (Feb. 1, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising.

b. Meaningful transparency is central to equitable informed consent.

A common thread for many of the instances of harm discussed above is that an individual's reproductive health care data was used or shared in a way that led to adverse effects to the individual—ways the individual likely would not have consented to if they had known such uses or disclosures were going to happen.[46] To minimize the risk of such harms, individuals must be informed of how apps, websites, and service providers will use their health data before they decide whether to share their information. For this to happen, entities that collect health data must provide meaningful transparency about their data practices.

As an initial step, entities that collect health data should be subject to stringent transparency requirements, including disclosures that individuals can realistically read, understand, and use to make informed decisions. Too often, individuals are presented with privacy policies that are impossible to comprehend[47] or are simply far too long to actually read and digest before signing up for a service.[48] Such privacy policies may satisfy current laws and regulations that simply mandate disclosure, but cannot be considered meaningful transparency. Regulations should require meaningful transparency—for example, by requiring a succinct and non-technical representation of data practices at the top of any privacy policy, so that users can understand an entity's privacy practices at a glance.[49]

This recommendation comes with an important caveat: while transparency is necessary to protect reproductive health data, by itself it is not enough. In today's ever-connected world, it is virtually impossible to go about our daily lives without disclosing some sensitive information—like location—to some third party.[50] Further, when asked for information in a health care or related setting, individuals may feel obligated or pressured to reveal information even if they do not feel that the information is directly relevant to the service they are seeking. In cases where individuals have limited ability to opt out (real or perceived), transparency is inadequate to protect individuals from harm.

---

[46] *See supra* Section II.
[47] *See* Kevin Litman-Navarro, *Opinion: We Read 150 Privacy Policies. They Were an Incomprehensible Mess.*, NY TIMES (June 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.
[48] *See* Geoffrey A. Fowler, *I Tried to Read All My App Privacy Policies. It Was 1 Million Words.*, WASH. POST (May 31, 2022), https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/.
[49] For instance, California requires that businesses subject to the California Consumer Privacy Act provide notice to consumers at the point of data collection and that the notice use plain language, be in a format that draws attention, be available in languages in which the business ordinarily provides information to consumers, and be accessible to consumers with disability. CAL. CODE REGS. tit. 11, § 999.305(a)(2) (2023).
[50] *See Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018) (noting that cell phones are "indispensable in participating in modern society" and that there is no realistic way of not creating a trail of location data).

c. Regulations should focus on reasonably foreseeable risks from the use and sharing of data.

In many of the examples discussed above, data is collected for legitimate reasons connected to health care, health promotion, and health services, only to be improperly used or shared. For instance, GoodRx customers presumably shared their health information to utilize the services GoodRx offers, such as buying prescription drugs.[51] GoodRx could have limited the use of customer data to these purposes; instead, it shared sensitive information with advertisers, a gross invasion of its users' privacy. This case serves as a reminder that, to minimize the risk of harm, regulations should consider not only what data is collected and created, but how that data is used and shared. In other words, regulations should take an outcome-based approach.

An outcome-based approach also helps to recognize that even seemingly innocuous data can lead to privacy and equity harms when used to infer health status. In other words, those violations of health privacy that can occur even without data that is, at face value, health data. Consider the Target anecdote described above.[52] Target used historical buying data—which most privacy frameworks would not treat as sensitive personal information—to infer sensitive health information, namely pregnancy status.[53] Regulations that aim to protect reproductive and other forms of health privacy must account for both health data and other data that can indirectly reveal facts about a person's health.

This principle is especially important to equity considerations. If strong baseline privacy protections are not established for all, privacy will become a luxury,[54] with users who cannot afford "privacy premiums" paying with personal data instead of subscriptions.[55] Regulations that hope to address disproportionate harms experienced by underserved communities should, therefore, be especially sensitive to how data use may lead to adverse outcomes for individuals and seek to provide strong protections so that these adverse outcomes do not occur.

d. Data minimization is necessary to protect individuals from extractive data practices and the risk of exploitation.

When service providers collect data that is not strictly necessary to further an agreed-upon purpose, they create the risk that such data will be used or shared in a way that is unrelated to the purpose. The principle of data minimization seeks to reduce this risk by

---

[51] *See supra* Section IV.a.
[52] *See supra* Section II.d.
[53] *Id.*
[54] *See* Julia Angwin, *Opinion: Has Privacy Become a Luxury Good?*, N.Y. TIMES (Mar. 3, 2014), https://www.nytimes.com/2014/03/04/opinion/has-privacy-become-a-luxury-good.html.
[55] For example, Apple offers Private Relay, a feature that allows individuals to browse the web without any entity knowing both the identity of the individual and the website they are visiting, as part of a premium subscription. *See About iCloud Private Relay*, APPLE, https://support.apple.com/en-us/HT212614.

requiring that only information necessary to complete a specific purpose should be collected. Data minimization is an established principle of privacy protection and incorporated in many privacy frameworks (including HIPAA, through the law's minimum necessary provisions).[56]

However, too often, exceptions provided in the frameworks and/or a lack of accountability in minimum necessary determinations effectively undermine the principle. For instance, disclosures required by law are not subject to HIPAA's minimum necessary standard.[57] In many jurisdictions across the country, state law mandates reporting of abortion care furnished by health care providers to state departments of health.[58] The stated purpose of these laws is generally to obtain de-identified, aggregated *statistical* information on abortion care.[59] However, state-issued reporting forms often ask extensive questions about the patient's demographic information—enough that, according to the Electronic Frontier Foundation, "it would not take great skill to identify the individual, particularly in a small town."[60] Because these forms may be subject to disclosures as public records, they become "fodder in the continuing pro-choice/anti-abortion battles, with violation of patients' privacy as collateral damage."[61] This problem is not theoretical; in Seattle, abortion care providers and an anti-abortion activist are currently in a legal battle over whether the anti-abortion activist can access abortion reporting forms with demographic information that may lead to re-identification.[62] If this information were not collected by the state in the first place, in contravention of at least the spirit of HIPAA's minimum necessary principle, the threat of patient identification and subsequent harm therefrom would be greatly decreased.

Any regulation seeking to mitigate privacy and equity harms caused by disclosures of health data must be rooted firmly in the principle of data minimization with minimal exceptions and processes in place that promote accountability to the principle.

V. Conclusion

In today's world, an individual's health data, including reproductive data, is collected, used, and disclosed by various commercial entities through a number of different ways. Without proper protection, misuse of this data may lead to serious harms for the individual. Further, these harms will not be evenly distributed; underserved communities

---

[56] *See Minimum Necessary Requirement*, DEP'T OF HEALTH AND HUM. SVCS., https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html.
[57] *See id.*
[58] *Abortion Reporting,* ELEC. FRONTIER FOUND., https://www.eff.org/issues/abortion-reporting.
[59] *Report of Induced Abortion*, NEB. VITAL RECS. OFFICE, https://www.nebraska.gov/nesos/rules-and-regs/regtrack/proposals/00000000000001071.pdf.
[60] *Abortion Reporting*, *supra* note 58.
[61] *Id.*
[62] *Id.*

are likely to be more seriously affected. There is a great need for principled privacy regulations to minimize the risks of harm.

***

We applaud NTIA for its commitment to reviewing current privacy frameworks with specific attention to equity and civil rights. We appreciate this opportunity to share urgent concerns regarding health data, particularly reproductive data. Please feel free to reach out to Mason Kortz (mkortz@law.harvard.edu) and Rachel Landauer (rlandauer@law.harvard.edu) should you have any questions.[63]

Sincerely,

Mason A. Kortz, JD
Clinical Instructor and Lecturer on Law

on behalf of

Cyberlaw Clinic at the Berkman Klein Center of Internet and Society at Harvard Law School

Rachel Landauer, JD, MPH
Clinical Instructor and Lecturer on Law

on behalf of

Center for Health Law and Policy Innovation of Harvard Law School

[63] The commenters thank Harvard Health Law and Policy Clinic student Christina Lee and Cyberlaw Clinic students Vincent Wroble and Sarah Zahedi for their invaluable contributions to this comment.