UC BERKELEY

CENTER FOR LONG-TERM CYBERSECURITY

CLTC WHITE PAPER SERIES

Enhancing Cyber Resilience for Equitable Healthcare

ANALYSIS OF CYBERATTACKS TARGETING SEXUAL AND REPRODUCTIVE FACILITIES AND SERVICES

PAVLINA PAVLOVA

CLTC WHITE PAPER SERIES

Enhancing Cyber Resilience for Equitable Healthcare

ANALYSIS OF CYBERATTACKS TARGETING SEXUAL AND REPRODUCTIVE FACILITIES AND SERVICES

PAVLINA PAVLOVA

October 2025

This report was published as part of the Center for Long-Term Cybersecurity's 2025 Public Interest Cybersecurity Research Call for Papers and was presented in June at the 2025 Cyber Civil Defense Summit.

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

Contents

Abstract

Healthcare is among the most targeted and vulnerable sectors for cyberattacks. Sexual and reproductive health (SRH) facilities and services in particular face financially motivated ransomware attacks and data breaches, ideologically motivated punitive attacks, and commercialization and misuse of medical and personal data. This research spotlights the SRH sector's threat landscape through quantitative and qualitative analysis of cyberattacks, extending into the impacts of these incidents. The findings inform strategies for cyber resilience that can support the integrity and equity of the U.S. healthcare sector. Recommendations focus on developing effective legislation, regulation, and cybersecurity practices, as well as enhancing collaborative strategies and community-driven solutions to protect healthcare facilities, including their services, operations, staff, and patients.

Executive Summary

This paper focuses on the following question: How do cyberattacks impact sexual and reproductive health (SRH) facilities and services in the U.S., and what strategies can enhance their cyber resilience to protect both providers and patients, particularly those who are legally, socially, and economically vulnerable?

SRH patients, providers, and platforms are uniquely exposed to cyberattacks and cyber-enabled threats. This vulnerability is compounded for individuals facing legal and political risks (such as abortion seekers in restrictive states), social stigmatization (for example, patients seeking abortions or IVF, or LGBTQ+ individuals seeking gender-affirming care), and economic or geographic marginalization (including rural populations, minors, and low-income individuals). SRH service providers manage highly sensitive medical and personal data, making them attractive targets for financially and ideologically motivated threat actors.

This study uses a mixed-methods approach, combining data analysis and personal interviews. Data about cyberattacks was collected from public reports (such as those available through the U.S. Department of Health and Human Services Office of Civil Rights Data Breach Portal and HIPAA Journal) and open-source publications, focusing on attack types, perpetrators, tactics, motivations, and the impact on data and operations. Interviews were conducted with frontline defenders and practitioners from SRH facilities to provide context and insights into the lived experiences and challenges faced by SRH organizations and their clients.

KEY FINDINGS

Healthcare is among the most targeted critical infrastructure sectors for cyberattacks. Sexual and reproductive health (SRH) service providers manage highly sensitive medical and personal data. This high-value data, combined with the stigma and political controversy that leaks could cause, increases the risk and impact of cyberattacks and other technology-facilitated attacks. Perpetrators' motivation ranges from financial extortion to punitive attacks and hacktivism.

Recent legislative developments have impacted the threat perception regarding the privacy of SRH data. The 2022 *Dobbs v. Jackson Women's Health Organization* decision, overturning *Roe v. Wade*, has enabled restrictive state laws that can compel providers to share medical records with authorities, allow law enforcement to request data from data brokers, and potentially

facilitate cross-state data access to penalize people for legally seeking procedures. The uncertain legal environment increases fears of criminalization among patients and providers and infringes on personal and medical data privacy.

Financially motivated data beaches at SRH organizations largely follow cybercrime patterns observed in other healthcare sub-sectors. The analysis of ransomware attacks and hacking incidents has not evidenced systematic operational disruptions in the provision of patient care. However, the secondary consequences of exposed data are extremely worrying, as double and triple extortion (where perpetrators exfiltrate data, threaten to leak it, and pressure the victims) and data misuse (including unauthorized access, sharing, or exploitation of medical records) are increasingly common. Combined with growing volumes of purposefully leaked sensitive data, aggressive extortion practices are likely to become more frequent, with criminals potentially revisiting previously exploited data. The SRH data is further vulnerable to misuse in targeted attacks against patients and staff and potential legal actions against them.

Reputational harm is a significant concern for SRH organizations as it can lead to financial repercussions, especially when the post-attack scrutiny uncovers failure of compliance with cybersecurity standards. Ransomware attacks and data breaches underscore systemic negligence, including insufficient information security practices and threat monitoring, outdated infrastructure, and gaps in employee cybersecurity training. The exposure of medical information can lead to legal action and financial compensation for victims. The fear of reputational harm guides organizations' responses to incidents, recovery and communication efforts, and remediation provided to victims.

SRH facilities and services face ideologically motivated attacks from activists and hacktivists. Hack-and-leak operations, distributed denial of service (DDoS) attacks, digital harassment (doxxing, targeted intimidation, and surveillance), misinformation, and smear campaigns aim to be both punitive — by intimidating patients, staff, and providers, and disruptive — by interfering with the provision of services and information.

The sale and third-party sharing of location data by data brokers is an insidious trend, enabling harassment and misinformation targeting individuals visiting SRH clinics. Commodification of medical and personal information by data brokers places individuals at risk of exposure and legal action.

Technical, structural, legal, social, and individual factors create an environment of digital, psychological, and physical insecurity for SRH staff and patients. The downstream effects are disproportionately experienced by vulnerable groups already facing barriers to accessing healthcare. Data-exploiting attacks can traumatize victims and lead to long-term harms, including withdrawal from using SRH services.

RECOMMENDATIONS

Strengthen privacy regulation to protect medical data: Healthcare providers are responsible for how they collect, use, and store medical and personal data, while digital platforms, search engines, and other technology and service providers make structural decisions that shape data collection and flows. Stronger regulation and privacy for medical data at the federal level, improved data security practices, and updated definitions of informed consent are essential to ensure that SRH data is safeguarded from the outset.

Recognize SRH services as critical infrastructure: The complex and evolving SRH threat landscape calls for robust policy interventions that comprehensively address data protection and privacy, cybersecurity posture and preparedness, and incident response protocols. Federal policy must explicitly recognize SRH as an essential component of national critical infrastructure, ensuring its inclusion in national security frameworks and emergency preparedness plans, and prioritizing its protection.

Share information, implement baseline cybersecurity, and improve incident response: Frontline service providers emphasize the need for collaborative approaches, such as improved cooperation among large- and medium-sized organizations in sharing intelligence and indicators around attacks; achieving essential baseline cybersecurity practices, including resilience measures and anti-harassment protections, in small or underfunded SRH facilities; and ensuring adequate incident response planning and recovery. Post-attack recovery efforts must account for operational disruptions, reputational damage, and the psychological toll on staff and patients.

Introduction

Cyberattacks against critical infrastructure have been growing in the U.S. and globally. The ever-increasing connectivity of people, devices, and platforms has created a sprawling attack surface that extends across American society.[1] Healthcare and public health (HPH), one of the 16 critical infrastructure sectors designated by the U.S. government, is frequently targeted by malicious actors and prone to severe and long-lasting impacts. Medical facilities and services operate in a data-rich environment and depend on digital systems and third-party contractors and vendors in the healthcare supply chain.[2] Ransomware attacks and data breaches pose an acute threat to the sector; attacks are increasingly driven by financial and ideological motives and are adopting new extortion and punitive tactics. Moreover, healthcare organizations face a range of disruptive disinformation campaigns that can compromise provision of care and undermine public trust.[3]

Attacks against protected health information (PHI), such as medical records, treatment histories, health insurance information, and prescription details held by HIPAA-covered entities, have intensified, leaving millions of patients affected. Reports to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) show that the impacts of attacks have been growing in terms of breached healthcare data; they reached an all-time high in 2024, with 276 million records illegally accessed.[4] A 2024 report by Rubrik Zero Labs highlighted that ransomware attacks on healthcare organizations not only affect a larger number of files but disproportionately impact sensitive data, making health care a uniquely vulnerable sector in terms of data risk and impact. The ransomware blast radius, measured by the number of impacted files, is 23% larger in healthcare organizations than the global average, and the amount of sensitive data impacted by breaches is 394% greater than the global average. On

[1] U.S. Department of Homeland Security. "Secure Cyberspace and Critical Infrastructure." https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure.

[2] U.S. Cybersecurity and Infrastructure Security Agency. "Healthcare and Public Health Sector." https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/healthcare-and-public-health-sector.

[3] HIPAA Journal. "Healthcare Data Breach Statistics." May 26, 2025. https://www.hipaajournal.com/healthcare-data-breach-statistics/; CyberPeace Institute. "Cyber Incident Tracer #Health." https://cit.cyberpeaceinstitute.org; CyberPeace Institute. Playing with Lives: Cyberattacks on Healthcare Are Attacks on People. March 2021. https://cyberpeaceinstitute.org/report/2021-03-CyberPeaceInstitute-SAR001-Healthcare.pdf.

[4] HIPAA Journal. "The Biggest Healthcare Data Breaches of 2024." March 19, 2025. https://www.hipaajournal.com/biggest-healthcare-data-breaches-2024/.

average, ransomware attacks affect 20% of a healthcare organization's total sensitive data, compared to 6% for organizations overall.[5]

SRH providers and platforms are custodians to some of the most sensitive and personal data, and are uniquely vulnerable due to perceived stigma around the care they deliver. These services include contraception and family planning; treatment of sexually transmitted diseases (STDs); pregnancy-related services; cancer screening and preventive care; infertility care; gender-affirming and inclusive care; counseling and support services; and preventive health and education. Many of these services are controversial and subject to intense political pressure and hostility. In addition to financially motivated ransomware and data breaches prevalent in the healthcare sector, SRH services face a higher incidence of ideologically motivated attacks by hacktivists and anti-abortion activists, as well as data brokers commercializing medical and personal data, with potential punitive or legal action for the victims. Not only do cybercriminals and activists seek to identify and target individual patients and staff, but they also try to influence them with misinformation that harms health outcomes and compromises medical trust.[6]

Despite acute vulnerabilities in the SRH digital infrastructure, a lack of understanding persists about the threat landscape, including SRH-specific cyber threats and the full scale of impacts on victims. Accounts of personal experiences remain anecdotal and captured in individual testimonies, often due to fear of reputational harm, secondary victimization, and potential legal repercussions. To close this gap, this research examines the threat landscape of cyberattacks impacting SRH facilities and services through a combination of quantitative and qualitative analysis, including interviews with frontline defenders and practitioners. This effort to promote evidence-based, community-driven solutions for improved resilience comes at a particularly fragile moment for women's health in the U.S., as the highly polarized political and policy climate places sensitive protected health information at the forefront of ideological battles.

Access to SRH care, particularly abortion, is a controversial political issue, and recent legislative developments have exposed the fragility of access to safe and legal services. Digital privacy risks for those seeking abortions have exponentially grown since the 2022 Supreme Court's decision in *Dobbs*, which overturned *Roe v. Wade* and ended the constitutional right to abortion. This ruling allowed states to regulate or ban abortion as they choose, triggering a wave of laws restricting access to medical procedures and imposing punitive measures, extending to

[5] Rubrik Zero Labs. "Healthcare Organizations Lose 20% of Their Sensitive Data in Every Ransomware Attack, Reports Rubrik Zero Labs." April 30, 2024. https://www.rubrik.com/company/newsroom/press-releases/24/healthcare-organizations-lose-sensitive-data-in-every-ransomware-attack.

[6] John, J. N., S. Gorman, D. Scales, and J. Gorman. "Online Misleading Information About Women's Reproductive Health: A Narrative Review." Journal of General Internal Medicine 40 No. 5 (April 2025): 1123–1131. https://pubmed.ncbi.nlm.nih.gov/39511120/.

civil actions and criminal indictments of patients who receive treatment and providers who administer it.[7] Additional efforts are under way to prevent pregnant women from seeking care outside their home state. These laws will influence how information is documented and accessed via electronic health records and how personal health applications are utilized in the consumer domain.[8] State laws increasingly compel providers to hand over medical records to law enforcement authorities in states where abortion is restricted or banned. Authorities might also be able to access records across state lines where abortion is legal, for example, when different electronic health record systems can share data.[9] The provision of IVF treatments has also experienced legal ambiguity with the ruling *LePage v. Mobile*, issued on February 16, 2024, by the Alabama Supreme Court. This decision concerns the legal rights around the custody, security, and destruction of genetic material and related medical data, and has raised questions about liability, regulation, and how patients' rights over their embryos and associated records are defined and protected.[10]

In the United States, medical data is regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which protects health information from being shared without a patient's consent. However, critical gaps persist in safeguarding SRH information. HIPAA is limited in terms of its application to data captured outside medical portals and does not extend to personal healthcare information exchanged or searched for outside of the formal healthcare setting, including online searches and commercial products, such as femtech (i.e., personal digital devices or apps designed for women, often for cycle and fertility tracking). Data from apps or pharmacy transactions often falls outside the scope of this federal law.[11] Although policies vary depending on the provider or application involved, companies that provide commercial or consumer-facing platforms and applications related to health can evade the legal obligation to keep collected and processed data private. HIPAA includes further exceptions for the use of data by law enforcement and in judicial proceedings. Even if an entity

[7] Huq, Aziz Z., and Rebecca Wexler. "Digital Privacy for Reproductive Choice in the Post-Roe Era." New York University Law Review 97 (2022): 1–93. U of Chicago, Public Law Working Paper No. 812. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4191990.

[8] Cohen, I. Glenn, and Andrea M. Crespo. "Dobbs and the Future of Health Data Privacy for Patients and Clinicians." Journal of the American Medical Informatics Association 29 No. 12 (2022): 2089–2091. https://doi.org/10.1093/jamia/ocac180.

[9] Zubrzycki, Carleen. "The Abortion Interoperability Trap." Yale Law Journal Forum 132 (2022): 197–227. https://ssrn.com/abstract=4147900.

[10] Smith-Ramakrishnan, Vina. "IVF Is the Latest Battleground in the War on Reproductive Justice." The Century Foundation. February 23, 2024. https://tcf.org/content/commentary/ivf-is-the-latest-battleground-in-the-war-on-reproductive-justice/.

[11] The Conversation. "How Abortion Providers Can Help Patients Navigate Threats to Digital Privacy." Fast Company. January 27, 2025. https://www.fastcompany.com/91266872/how-abortion-providers-help-patients-navigate-threats-digital-privacy.

is covered by HIPAA, the law does not provide absolute protection against having SRH records disclosed.[12]

HIPAA was updated with the 2024 HIPAA Privacy Rule to Support Reproductive Health Care Privacy, which prohibited the disclosure of personal health information for law enforcement-related activities in the context of legal reproductive health care.[13] The HIPAA Privacy Rule, issued in response to the *Dobbs* decision, filled a critical loophole in privacy protections afforded by HIPAA that would have permitted the release of sensitive data. The rule obliges HIPAA-regulated entities to obtain a signed attestation from the requestors (e.g., judicial officials, law enforcement officers, health oversight agencies, and medical examiners) confirming that the information is not being requested for a restricted purpose (such as punishing or targeting individuals simply for accessing lawful reproductive health services) before they can hand over reproductive health information. Several lawsuits have challenged the rule since then and in June 2025, the U.S. District Court for the Northern District of Texas vacated the rule nationally.[14] Moreover, HHS may seek to promulgate new privacy regulations that jettison or substantially weaken or even eliminate existing privacy protections, including the possibility of choosing not to enforce the amended Privacy Rule or initiate revoking or rolling back these protections.[15] Finally, legal provisions alone do not determine regulatory practices. Healthcare providers often comply in advance with perceived legal and regulatory expectations. Such anticipatory compliance can lead to reduced availability of services, for example when providers limit or withdraw services in response to uncertainty and restrictive legal environments, thus negatively impacting patient access to care.[16]

[12] Bushwick, Sophie, edited by Dean Visser. “Yes, Phones Can Reveal if Someone Gets an Abortion.” Scientific American. May 13, 2022. https://www.scientificamerican.com/article/yes-phones-can-reveal-if-someone-gets-an-abortion/.

[13] U.S. Department of Health and Human Services (HHS). “HIPAA and Reproductive Health: Final Rule HIPAA Privacy Rule to Support Reproductive Health Care Privacy.” https://www.hhs.gov/hipaa/for-professionals/special-topics/reproductive-health/index.html.

[14] Steve Alder. “Texas Judge Vacates Abortion Privacy Protections.” HIPAA Journal. June 23, 2025. https://www.hipaajournal.com/texas-judge-vacates-hippa-reproductive-healthcare-privacy-rule/.

[15] Guttmacher Institute. “How Project 2025 Seeks to Obliterate Sexual and Reproductive Health and Rights.” Factsheet, October 2025. https://www.guttmacher.org/fact-sheet/how-project-2025-seeks-obliterate-srhr.

[16] Personal interview.

Methodology

This research employed a mixed-method approach to analyze cyberattacks carried out on U.S.-based SRH facilities and services between 2020 and 2024. Limiting the analysis to this timeframe helps to establish potential correlations between the type, frequency, and impact of attacks and the legislative and political developments during that period.

The quantitative data collection focused on the types of attacks, perpetrators, tactics, and motivations (when known), along with an assessment of the impacts, based on the volume and nature of breached data and changes in the victims' operational capacity before and after the incidents. Geographic and demographic information about the facilities and the communities they serve is included when available to understand the effects on populations. The data pool primarily considers publicly available reports from the HHS Office of Civil Rights (OCR) Data Breach Portal, a publicly accessible database listing data breaches of protected health information reported by HIPAA-covered entities, and HIPAA Journal, an online publication providing news and analysis related to HIPPA, for coverage of data breaches reported to the HHS OCR. The data collection was supplemented by other materials obtained via open-source research methods, including court documents, investigative articles, and sector-specific reports. The limitations of this study include incomplete data, information that organizations withheld in reporting, and details not covered in publicly accessible sources.

The research also entailed conducting firsthand interviews with individuals on the frontlines of these cyber incidents, such as defenders, threat analysts, and affected organizations, to help explain the threat landscape and experienced harm. The interviews are largely anonymized to mitigate potential professional, organizational, and legal risks for participants. The seven testimonies given for this study enhance understanding of how the facilities and individuals prepared for and endured cyberattacks, how they managed the increased operational and psychological pressure that resulted from the attack, and how they designed their post-attack recovery efforts.

Threat Landscape

FINANCIALLY MOTIVATED RANSOMWARE ATTACKS AND DATA BREACHES

Ransomware attacks and data breaches pose a critical threat to the provision of healthcare and the integrity of medical and personal information, as perpetrators leverage the threat of operational disruptions, reputational damage, and legal consequences to pressure targeted organizations.[17] According to a senior healthcare cybersecurity analyst interviewed for this study, the rise of data leak extortion strategies by ransomware actors has made protected health information a tempting target for two reasons: "First, in the U.S., healthcare data is highly regulated, and any unauthorized leaks will create a regulatory and legal risk to the organization. Second, the high sensitivity of health information increases the value of the data for extortion because it pressures the victim organization to pay to avoid reputational impact."[18] In other words, the importance of maintaining patient trust and protecting sensitive data makes the healthcare sector a lucrative target for extortion-based cyberattacks.

Furthermore, personally identifiable information (PII) accessed through a data breach is valuable for cybercriminals, who can use it for resale, identity theft, and social engineering. A former security and compliance executive at a clinic for women's and family health underscored the unique sensitivity of SRH data, which she said is creating a specific threat landscape. In her words, "It is very different to protect a business versus a clinic." Financially motivated cybercrime is common, and business-side organizations tend to prioritize protecting business data and maintaining operations. Failure to prioritize individual patient privacy and data security often results in the exposure of unencrypted databases, further compromising patient trust and safety.[19]

The information available on the HIPAA data breach portal largely refrains from identifying the perpetrators. However, financially motivated cyberattacks are commonly performed by ransomware-as-a-service (RaaS) gangs, as exemplified by the August 2024 attack against Planned Parenthood of Montana, in which RansomHub, a RaaS group, claimed responsibility for compromising data belonging to 18,000 individuals.[20] Operating under a service-oriented model,

[17] Rosenbaum, J., M. Zegers, D. Bhatia, et al. "Ransomware Attacks on US Hospitals and Clinics and the Impact on Patient Care." JAMA Network Open 7, no. 5 (2024). https://msutoday.msu.edu/news/2025/msu-study-ransomware-drives-us-health-data-breaches.

[18] Personal interview.

[19] Personal interview.

[20] Alder, Steve. "Planned Parenthood Ransomware Attack Affects 18,000 Patients." HIPAA Journal, November 8, 2024. https://www.hipaajournal.com/planned-parenthood-ransomware-2024/.

cybercriminal enterprises lower the barriers to entry, thereby enabling a broad spectrum of actors to participate. Moreover, ransomware tactics are growing more aggressive. As a cybersecurity analyst from the healthcare intelligence-sharing community explained, “Ransomware threat actors are increasingly engaging in tactics known as triple extortion, which is based on locking data, threatening to leak it, and then targeting customers to pay a separate ransom as well.” The analyst stressed that ransomware groups have engaged in triple extortion of U.S. healthcare entities in individual cases, and direct extortion with patients can become more common.[21]

According to 2024 research on ransomware against healthcare organizations conducted by the Royal United Services Institute (RUSI), there is limited evidence that exfiltrated medical data from financially motivated cybercrime is systematically exploited for personalized fraud or further extortion of individuals. At the same time, developments in cybercrime extortion methods and a growing amount of leaked data are likely to impact criminal practices, with criminals potentially revisiting previously exploited data.[22] It is therefore probable that ransomware groups will engage in extorting individual patients after breaching their sexual and reproductive medical data and PII. According to a cybersecurity analyst observing the extortion methods in the healthcare sector, “ransomware-as-a-service threat actors claim to have their own ‘ethics,’ and some declare bans [i.e., self-imposed rules and informal pledges] on targeting healthcare providers.” However, when their affiliates violate these “ethics,” there are rarely ramifications within the group. Several cybercriminal groups have been “explicitly known to primarily target healthcare entities,” according to the same analyst.[23]

An analysis of 13 ransomware attacks, hacking incidents, and unauthorized access incidents affecting SRH organizations reported in the HIPAA Data Breach Portal indicates that there was an increase in the frequency and volume of data breaches between 2020 and 2024.[24] The targeted organizations include large multi-state and state-specific organizations, with several high-profile organizations, such as Planned Parenthood and various fertility centers, being recurrent targets, likely because of their size, data volume, visibility, and calculated ability to pay a ransom.

Attacks are not concentrated in a single state or region; rather, data breaches are distributed across the U.S., affecting both large, urban states such as California and Illinois and less populous, rural states like Montana. The pattern suggests that financially motivated attackers are opportunistic, seeking high-value data and visibility rather than focusing on a specific state or city.

[21] Personal interview.

[22] MacColl, Jamie, et al. The Scourge of Ransomware: Victim Insights on Harms to Individuals, Organisations and Society. Royal United Services Institute (RUSI), January 2024. https://static.rusi.org/ransomware-harms-op-january-2024.pdf.

[23] Personal interview.

[24] HHS OCR Breach Portal. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

The consequences of these incidents can be both localized to individual clinics, as in the cases of Southern Reproductive Health and the Midwest Fertility Group, or have a nationwide reach, as in the breach of Laboratory Services Cooperative, which affected more than 1.6 million individuals, as it is affiliated with Planned Parenthood centers in 31 states and the District of Columbia.

The 13 cyberattacks analyzed breached a wide range of medical and personal data, including patients' full names, addresses, dates of birth, social security numbers, medical diagnoses, treatment histories, insurance details, and reproductive histories, such as abortion or STD treatment records. In cases like the Planned Parenthood Los Angeles breach in October 2021, sensitive health data was potentially weaponized for blackmail or harassment. A class-action lawsuit filed in the U.S. District Court of Central California concerning the Planned Parenthood Los Angeles data incident alleged that the breach's sensitive nature was compounded by the timing of Supreme Court abortion debates.[25] Some of the breached facilities are located in politically polarized environments, deepening their vulnerability. For example, a ransomware attack against Planned Parenthood of Montana affected a provider in a region with ongoing political polarization over reproductive rights.[26]

SRH facilities impacted by ransomware attacks and data breaches largely continued their services, while a few experienced varying levels of operational disruption or constraints; for instance, Planned Parenthood of Montana took parts of its network offline to contain the damage while continuing to provide patient care. A February 2021 ransomware attack on Fertility Centers of Illinois (FCI) forced the clinic to temporarily restrict access to certain IT systems. A September 2020 ransomware attack against US Fertility (USF), the largest physician-owned fertility organization in the U.S., led to significant IT system outages across over 100 clinic locations and over two dozen IVF laboratories. In several instances, ransomware attacks involved legacy systems with outdated computer hardware, software, and IT infrastructure, exposing vulnerabilities in systems that no longer receive security updates or patches from vendors, such as in the case of Conceptions Reproductive Associates of Colorado in April 2024, which had vulnerabilities left unaddressed due to a lack of ongoing security support. Following the attacks, organizations implemented more robust cybersecurity frameworks, including firewall enhancements, multi-factor authentication, third-party forensic audits, and employee retraining. Several organizations delayed public disclosure of breaches and/or faced legal action. Regional Women's Health Group, LLC, doing business as Sincera Reproductive

[25] Alder, Steve. "Planned Parenthood Los Angeles Settles Class Action Data Breach Lawsuit for $6 Million." HIPAA Journal. April 8, 2024. https://www.hipaajournal.com/planned-parenthood-los-angeles-settlement-data-breach-lawsuit/.

[26] Vicens, AJ. "Planned Parenthood of Montana Confirms Cyberattack." CyberScoop. September 5, 2024. https://cyberscoop.com/planned-parenthood-of-montana-confirms-cyberattack/.

Medicine, was affected by a data breach between August and September 2020, resulting in more than 37,000 patients having their personal and health information compromised during a five-week period. The clinic faced legal action filed by a group of patients and eventually agreed to a $1.2 million settlement. In September 2020, US Fertility, which supports a network of fertility service providers, experienced a ransomware attack affecting nearly 900,000 individuals; in February 2024, the organization reached a $5.75 million settlement to resolve negligence allegations. In April 2024, Planned Parenthood Los Angeles agreed, with no admission of wrongdoing, to resolve a class-action lawsuit by agreeing to a $6 million settlement to recover documented losses by affected patients, to compensate for out-of-pocket costs and credit monitoring and identity theft protection, and to obtain statutory damages incurred as a result of the 2021 data breach.[27] Legal settlements provided some restitution for affected individuals, including credit monitoring and financial compensation. The systemic issues that enabled the attacks, such as underfunded IT infrastructures and insufficient cybersecurity preparedness, prompted many organizations to implement improved security measures following the incidents.

IDEOLOGICALLY MOTIVATED ATTACKS AND DIGITAL SURVEILLANCE

Anti-abortion activists have for years targeted abortion and family planning facilities. In August 2023, New York Attorney General Letitia James filed a lawsuit[28] against members of Red Rose Rescue, an anti-abortion extremist group, for invading reproductive healthcare clinics, threatening staff and clinicians, and terrorizing patients.[29] According to Eva Galperin, director of cybersecurity at the nonprofit Electronic Frontier Foundation, which promotes digital rights, the current threat landscape for SRH services in the U.S. is characterized by "very real and ongoing threats, including court rulings, hostile legislation, and outright terrorist attacks such as the Palm Springs bombing."[30] As she emphasized, "These are not just theoretical risks; such attacks occur

[27] Alder, Steve. "Planned Parenthood Los Angeles Settles Class Action Data Breach Lawsuit for $6 Million." HIPAA Journal. April 8, 2024. https://www.hipaajournal.com/planned-parenthood-los-angeles-settlement-data-breach-lawsuit/.

[28] People of the State of New York, by Letitia James v. Red Rose Rescue, et al., No. 1:23-cv-04832 (S.D.N.Y. filed June 8, 2023). https://law.justia.com/cases/federal/district-courts/new-york/nysdce/7:2023cv04832/600073/55/.

[29] Attorney General James. "Attorney General James Sues Militant Anti-Abortion Group for Invading Clinics and Blocking Access to Reproductive Health Care." June 8, 2023. https://ag.ny.gov/press-release/2023/attorney-general-james-sues-militant-anti-abortion-group-invading-clinics-and.

[30] On May 17, 2025, a car bombing occurred at a reproductive center in Palm Springs, California, leaving one person near the vehicle, later confirmed to be the perpetrator, dead and four others injured. Press release by American Society for Reproductive Medicine, May 18, 2025: https://www.asrm.org/news-and-events/asrm-news/press-releasesbulletins/asrm-statement-on-palm-springs-bombing/.

regularly."[31] SRH services targeting can also intersect with domestic and sexual violence, from reproductive coercion in the form of preventing access to abortion services to individuals to threats or actual violence directed at medical service providers.[32] Policy efforts that include calls to drastically restrict access to abortion, contraception, family planning, and assisted reproductive services such as IVF can further exacerbate risks for individuals seeking health care.[33]

Ideology translates into the digital realm. According to a cybersecurity analyst in the healthcare sector interviewed for this study, perpetrators may carry out "hack and leak" operations, when they steal data from SRH service providers and then publish the information in a bid to harm the victim organization by mobilizing and gathering support from others who share their ideological beliefs. In addition, as a former security and compliance executive pointed out, hacktivists also present a threat from within: "There is a risk from insiders, especially due to high turnover in jobs, not just in IT but also in care roles. Someone could pretend to care about the job and gain access."

Hackers may also use cyberattacks to disrupt the availability of health care providers' websites, for example with distributed denial of service (DDoS) attacks, where organizers coordinate efforts to flood abortion providers' and abortion-rights groups' websites or internet-exposed infrastructure with traffic. Additionally, anti-abortion activists may initiate harassment campaigns and doxxing, coordinate online attacks, or impersonate target healthcare providers and staff. Leaked databases with home addresses, phone numbers, or emails and passwords can be published online to perpetuate such abuse. These attacks can be coordinated to maximize psychological harm and disruption. Between 2013 and 2016, such coordination against Whole Woman's Health, a major abortion provider, included malware infections and distributed denial of service (DDoS) attacks that shut down their website for weeks and disrupted patient access to services. These attacks led to severe operational and psychological harm and escalated when the organization publicly advocated for abortion.[34] As EFF's Eva Galperin explained: "Since the overturning of *Roe v. Wade*, these threats have worsened with recent changes in social media policies that implicitly or explicitly condone harassment.

[31] Personal interview.

[32] Silverman, Jay G., and Anita Raj. "Intimate Partner Violence and Reproductive Coercion: Global Barriers to Women's Reproductive Control." PLoS Medicine 11, No. 9 (2014): e1001723. https://pmc.ncbi.nlm.nih.gov/articles/PMC4165751/.

[33] Doctors of the World. "Project 2025: Sexual and Reproductive Health Rights." September 28, 2024. https://doctorsoftheworld.org/blog/project-2025-sexual-and-reproductive-health-rights/.

[34] Grant, Rebecca. "The Disturbing Rise of Cyberattacks Against Abortion Clinics." Wired, October 5, 2017. https://www.wired.com/story/cyberattacks-against-abortion-clinics/.

Several guardrails have been removed, exemplified in the rollback of gender-sensitive content moderation policies on platforms like Facebook and X (formerly Twitter)."[35]

Anti-abortion activists have engaged in aggressive tactics, such as wiretapping of abortion clinics, hacking provider networks to access patient information, and using phone location data to advertise anti-abortion materials to people who visit family planning clinics.[36] A lawsuit filed in September 2024 alleged that activists intercepted patients' exchanges with local abortion clinics in an effort to stop procedures.[37] In February 2024, a report on a pro-life political organization showed that a crisis pregnancy center obtained mobile phone location data from a broker and used it to target people who had visited clinics. According to the court document, in or around March 2024, the victimized woman mentioned in the lawsuit undertook efforts to seek reproductive health care. Through its online advertising, the crisis center, Attleboro Women's Health Center (AWHC), solicited an appointment under a false pretense and provided medically inaccurate information regarding abortions upon visit.[38]

In addition to trying to stop patients from visiting SRH providers, hackers may attempt to acquire and exploit personal data for commercial purposes, such as sale on the secondary market.[39] Location data brokers have been reported selling or sharing information about people who had visited abortion clinics, including where patients travelled before and after their visits.[40] Anti-abortion groups have utilized data brokers to target individuals visiting Planned

[35] Personal interview.

[36] Coutts, Sharona. "Anti-Choice Groups Use Smartphone Surveillance to Target 'Abortion-Minded Women' During Clinic Visits." Rewire News Group, May 25, 2016. https://rewirenewsgroup.com/article/2016/05/25/anti-choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits/; Stack, Liam. "A Brief History of Deadly Attacks on Abortion Providers." New York Times. November 29, 2015. https://www.nytimes.com/interactive/2015/11/29/us/30abortion-clinic-violence.html; Sabin, Sam. "'Lock It Down Right Now': Abortion Rights Advocates Prepare for a New Wave of Digital Security Threats." Politico. June 17, 2022. https://www.politico.com/news/2022/06/17/abortion-rights-advocates-digital-security-threats-00040654; Grant, Rebecca. "The Disturbing Rise of Cyberattacks Against Abortion Clinics." Wired. October 5, 2017. https://www.wired.com/story/cyberattacks-against-abortion-clinics/.

[37] Smalley, Suzanne. "Anti-abortion Group Accused of Electronically Intercepting Patients' Exchanges with Clinic." Recorded Future News. October 10, 2024. https://therecord.media/anti-abortion-group-massachusetts-accused-intercepting-messages.

[38] Four Women Health Services, LLC v. Abundant Hope Pregnancy Resource Center Inc., d/b/a Attleboro Women's Health Center, Catherine Roman, Nicole Carges, and Darlene Howard. No. 1:24-cv-12283 (D. Mass. filed Sept. 5, 2024). https://www.documentcloud.org/documents/25188991-01/; Smalley, Suzanne. "Anti-abortion Group Accused of Electronically Intercepting Patients' Exchanges with Clinic." Recorded Future News. October 10, 2024. https://therecord.media/anti-abortion-group-massachusetts-accused-intercepting-messages.

[39] Huq, Aziz Z., and Rebecca Wexler. "Digital Privacy for Reproductive Choice in the Post-Roe Era." New York University Law Review 97 (2022): 1–93. U of Chicago. Public Law Working Paper No. 812. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4191990.

[40] Cox, Joseph. "Location Data Firm Provides Heat Maps of Where Abortion Clinic Visitors Live." Vice. May 5, 2022. https://www.vice.com/en/article/location-data-firm-heat-maps-planned-parenthood-abortion-clinics-placer-ai/; Cox, Joseph. "Data Broker Is Selling Location Data of People Who Visit Abortion Clinics." Vice. May 3, 2022. https://www.vice.com/en/article/location-data-abortion-clinics-safegraph-planned-parenthood/.

Parenthood clinics with anti-abortion ads. For example, The Veritas Society, an anti-abortion nonprofit group funded by Wisconsin Right to Life, delivered 14.3 million ads in 2020 to people who had visited abortion clinics in Wisconsin alone.[41] A letter from Senator Ron Wyden (D-OR) detailed that Near Intelligence, a location data broker, tracked individuals' visits to nearly 600 Planned Parenthood locations to feed an anti-abortion ad campaign.[42]

Anti-abortion groups can use SRH data to identify women who seek out-of-state abortions, often in violation of applicable laws in their jurisdiction, or they can create "heat maps" that show in visual terms when individuals may have visited abortion clinics.[43] Such actions can have a chilling effect on patients and providers, as medical data could be used for harassment. Location data is extremely revealing when combined with SRH data, which can lead patients to limit their use of period- and fertility-tracking apps. Femtech developers and providers have been repeatedly shown to engage in widespread data misuse while handling highly personal data.[44] According to the Organization for the Review of Care and Health Apps, most period trackers share data with third parties.[45] This has been confirmed by Mozilla research.[46] In addition, a report by the International Digital Accountability Council found lack of transparency about data sharing policies and processing of intimate and gendered data, and showed that software development kits have been collecting lists of all apps installed on a user's device and transmitting these lists to

[41] Electronic Privacy Information Center. "Data Broker Helped Anti-Abortion Group Target Planned Parenthood Visitors, Wyden Letter Reveals." February 13, 2024. https://epic.org/data-broker-helped-anti-abortion-group-target-planned-parenthood-visitors-wyden-letter-reveals/.

[42] Ng, Alfred. "A Company Tracked Visits to 600 Planned Parenthood Locations for Anti-Abortion Ads, Senator Says." Politico. February 13, 2024. https://www.politico.com/news/2024/02/13/planned-parenthood-location-track-abortion-ads-00141172; Wyden, Ron. "Wyden Reveals Phone Data Used to Target Abortion Misinformation at Visitors to Hundreds of Reproductive Health Clinics." U.S. Senate. February 13, 2024. https://www.wyden.senate.gov/news/press-releases/wyden-reveals-phone-data-used-to-target-abortion-misinformation-at-visitors-to-hundreds-of-reproductive-health-clinics.

[43] Cox, Joseph. "Location Data Firm Provides Heat Maps of Where Abortion Clinic Visitors Live." Vice. May 5, 2022. https://www.vice.com/en/article/location-data-firm-heat-maps-planned-parenthood-abortion-clinics-placer-ai/; Cox, Joseph. "Data Broker Is Selling Location Data of People Who Visit Abortion Clinics." Vice. May 3, 2022. https://www.vice.com/en/article/location-data-abortion-clinics-safegraph-planned-parenthood/; Pavlova, Pavlina. "Gendered Harms of Data Weaponization: Historical Patterns, New Battlefields, and the Implications for Democracy and National Security." Future Security. New America. Last updated November 14, 2024. https://www.newamerica.org/future-security/reports/gendered-harms-of-data-weaponization/.

[44] Kemp, Katharine. "Popular Fertility Apps Are Engaging in Widespread Misuse of Data, Including on Sex, Periods and Pregnancy." UNSW Newsroom. March 22, 2023. https://www.unsw.edu.au/newsroom/news/2023/03/popular-fertility-apps-are-engaging-in-widespread-misuse-of-data; Paul, Kari. "How Private Is Your Period-Tracking App? Not Very, Study Reveals." The Guardian. August 17, 2022. https://www.theguardian.com/world/2022/aug/17/pregnancy-period-tracking-apps-privacy.

[45] BBC. "Period Trackers to Be Reviewed over Data Concerns." September 7, 2023. https://www.bbc.com/news/technology-66740184.

[46] Boyd, Ashley. "Why Mozilla is Scrutinizing the Privacy of Pregnancy Apps." Mozilla Foundation. August 17, 2022. https://foundation.mozilla.org/en/blog/why-mozilla-is-scrutinizing-the-privacy-of-pregnancy-apps.

third parties.[47] This data, especially in an unencrypted form, is vulnerable to breaches, leaks, commercial de-anonymization, publication, and exploitation. A report by the University of Cambridge's Minderoo Centre for Technology and Democracy shows that most cycle tracking apps are targeted at women attempting to get pregnant, and the download data about the app installation alone is of high commercial value. Few life events are linked to such dramatic shifts in consumer behavior, and the report assesses data on pregnancy as over 200 times more valuable in digital marketing than data on age, gender, or location for targeted advertising.[48]

Social media platforms curate content for their users based on collected data. When individuals install femtech apps and social media apps on the same device, providers can share or cross-reference respective data. Additionally, large-scale anonymized data collected from these apps can be resold through intermediaries such as advertisers and data brokers and combined for commercial purposes to create detailed user profiles. Such data-sharing practices make it more likely that users will receive tailored misinformation through personalized social media feeds, as the platforms use this information-dense data to target content specifically suited to individual users' behaviors. Users of femtech apps are at heightened risk of being exposed to misleading or harmful content precisely because of the overlap and flow of sensitive health data within the digital ecosystem.[49]

The risk posed by law enforcement requests or third-party subpoenas for digital health records is high, especially in states where abortion is criminalized, or where reproductive health care is limited. App providers may be requested to share this data with the authorities, or to provide information about individuals accessing online health services. When combined with location data indicating proximity to sexual and reproductive health facilities, this information may be monitored by law enforcement to track and prosecute individuals.[50] The Surveillance

[47] Holden Williams, Ginny Kozemczak, and Dan Kinne. "Digital Health is Public Health: Consumers' Privacy & Security in the Mobile Health App Ecosystem." International Digital Accountability Council (IDAC). December 15, 2021. https://digitalwatchdog.org/wp-content/uploads/2022/01/Digital-Health-is-Public-Health-Consumers-Privacy-and-Security-in-the-Mobile-Health-App-Ecosystem.pdf; International Digital Accountability Council (IDAC). "SDKs Collecting Installed App Lists." Trend Report. https://digitalwatchdog.org/trend-report-sdks-collecting-installed-app-lists/.

[48] Felsberger, Stefanie. "The High Stakes of Tracking Menstruation, " Minderoo Centre for Technology and Democracy, June 11, 2025, https://www.mctd.ac.uk/femtech-high-stakes-tracking-menstruation/. See also "Menstrual tracking app data is a 'gold mine' for advertisers that risks women's safety." University of Cambridge. https://www.cam.ac.uk/research/news/menstrual-tracking-app-data-is-a-gold-mine-for-advertisers-that-risks-womens-safety-report.

[49] Shires, James, Bassant Hassib, and Amrit Swali. "Gendered Hate Speech, Data Breach and State Overreach: Identifying the Connections between Gendered Cyber Harms to Shape Better Policy Responses," Chatham House Research Paper, International Security Programme, May 2024, https://www.chathamhouse.org/sites/default/files/2024-05/2024-05-24-gendered-cyber-harms-shires-et-al_0.pdf.

[50] Gollan, Jennifer. "Websites Selling Abortion Pills Are Sharing Sensitive Data With Google." Ms. Magazine, January 18, 2023. https://msmagazine.com/2023/01/18/google-abortion-pills-privacy-data/; James Shires, Bassant Hassib, and Amrit Swali, "Gendered Hate Speech, Data Breach and State Overreach: Identifying the Connections between Gendered Cyber Harms to Shape Better Policy Responses," Chatham House Research Paper, International Security Programme, May 2024, https://www.chathamhouse.org/sites/default/files/2024-05/2024-05-24-gendered-cyber-harms-shires-et-al_0.pdf.

Technology Oversight Project report explains how governments and private entities surveil women's search history, location data, and social media content.[51] According to the report, once reported to authorities, activities conducted on devices, such as browsing, purchasing, tracking and communication, can become evidence in prosecutions. In a personal interview, Rebecca Nall, Executive Director and Founder at I Need An A (ineedana.com), a project that helps people get an abortion in post-Roe America, cautioned that the most important thing a patient can do is be careful with whom they share their experiences. People who have been arrested for self-managed abortions without direct clinical supervision, such as those using abortion medications at home or undergoing miscarriages, have been reported to the police by healthcare professionals, family, and friends. As Nall explains, "It is often only after being reported that digital evidence is used to build a case against them."[52]

Authorities have shown a willingness to subpoena records from personal accounts and seek access to medical information for women who received legal out-of-state abortions.[53] As a sign of how far law enforcement surveillance has reached to access electronic evidence, 404 Media reported that a sheriff's office in Texas searched data from automated license plate reader (ALPR) cameras across the nation to trace an individual suspected of an abortion. The search concerned camera networks maintained by surveillance technology company Flock Safety, including those located in states where abortion access is protected by law.[54] In the words of a senior-level CISO at a SRH organization interviewed for this report: "In a post-Roe era, we are witnessing the erosion of digital safe spaces. Technologies originally designed for public safety, like license plate readers, data brokers, and search history tools, are now being used to monitor, intimidate, or even prosecute people seeking reproductive care. Until we address the surveillance infrastructure itself, we must empower individuals with the tools and knowledge to protect their digital footprints."[55]

[51] Surveillance Technology Oversight Project. "S.T.O.P. Releases Report on Abortion Surveillance After Roe." May 24, 2022. https://www.stopspying.org/latest-news/2022/5/24/stop-releases-report-on-abortion-surveillance-after-roe.

[52] Personal interview.

[53] McDonald, Nora. "Reproductive Health Care Faces Legal and Surveillance Challenges Post-Roe – New Research Offers Guidance." The Conversation. January 24, 2025. https://theconversation.com/reproductive-health-care-faces-legal-and-surveillance-challenges-post-roe-new-research-offers-guidance-246869; Greig, Jonathan. "Lab Provider for Planned Parenthood Discloses Breach Affecting 1.6 Million People." Recorded Future News. April 11, 2025. https://therecord.media/lab-provider-planned-parenthood-breach.

[54] Alajaji, Rindala. "She Got an Abortion. So a Texas Cop Used 83,000 Cameras to Track Her Down." Electronic Frontier Foundation. May 30, 2025. https://www.eff.org/deeplinks/2025/05/she-got-abortion-so-texas-cop-used-83000-cameras-track-her-down; Marcus, Josh. "Texas Police Used Nationwide License Plate Reader Network to Track Woman Who Had Self-Managed Abortion." The Independent. May 30, 2025. https://www.independent.co.uk/news/world/americas/crime/texas-abortion-license-plate-camera-b2760411.html.

[55] Personal interview.

Impacts on Patients, Staff, and Organizations

IMPACTS ON PATIENTS

When SRH data is breached and weaponized, victims face psychological, physical, financial, legal, reputational, and social harm. Individuals may suffer trauma, a sense of violation, and insecurity, as well as fear of re-victimization. Such incidents undermine privacy, personal security, and fundamental rights, affecting individuals' autonomy, agency, and self-development. When combined with health information, PII can lead to unauthorized charges, identity theft, and other fraudulent transactions made without the consent or knowledge of the victim, and can add to fear of blackmail or harassment. SRH data, including information about pregnancy, abortion, sexual health, and STDs, is uniquely sensitive. Exposure of such data can harm individuals' health, well-being, and access to services, while also threatening their social, physical, and psychological security. The weaponization of data can target and victimize individuals for their reproductive health choices, leading to deep and lasting harm.[56] According to a former security and compliance executive interviewed for this study, "people do not always realize how misused data can have downstream effects, for example, affecting eligibility for health insurance, job opportunities, or personal relationships."[57]

In states where abortion is illegal, abortion-seekers and medical practitioners may face criminal charges and other legal actions. As such, the perception of threats concerning SRH data has increased as access to abortion has become more restrictive.[58] Data from healthcare providers, family, and friends could be used to identify abortion seekers to law enforcement, and information kept on personal devices, including search history, pose privacy risks and raise the threat of potential prosecution.[59] Abortion seekers, particularly those living in states that prohibit traveling across state lines for legal abortion care, are concerned that their personal

[56] Pavlova, Pavlina. "Gendered Harms of Data Weaponization: Historical Patterns, New Battlefields, and the Implications for Democracy and National Security." Future Security. New America. Last updated November 14, 2024. https://www.newamerica.org/future-security/reports/gendered-harms-of-data-weaponization/.

[57] Personal interview.

[58] MacColl, Jamie, et al. The Scourge of Ransomware: Victim Insights on Harms to Individuals, Organisations and Society. Royal United Services Institute (RUSI), January 2024. https://static.rusi.org/ransomware-harms-op-january-2024.pdf.

[59] McDonald, Nora. "Reproductive Health Care Faces Legal and Surveillance Challenges Post-Roe – New Research Offers Guidance." The Conversation. January 24, 2025. https://theconversation.com/reproductive-health-care-faces-legal-and-surveillance-challenges-post-roe-new-research-offers-guidance-246869.

medical information could be shared, misused, and disclosed without their consent. Fear of surveillance and criminalization, loss of trust in the healthcare system, and legal and policy uncertainty can significantly impact patient behavior by deterring individuals from seeking or accessing lawful abortion care.[60] Unauthorized sharing of personal information related to SRH can further lead to distress, for example from fertility advertising inappropriately targeting miscarriage victims or increased exposure to misinformation aimed at those seeking abortions. This fallout is possible when advertisers use sensitive health data without consent to push targeted ads that assume or exploit these experiences and emotionally trigger users.

Financially motivated data breaches also cause direct harm to victims, as they can result in purposeful or negligent publishing of sensitive and personal information on the dark web and online platforms, and in the coercion of the target organizations and victims through extortion.[61] Once SRH information is obtained, there is no assurance that it will not be eventually misused. Compromised data may be carelessly stored by hackers or revisited for further victimization, highlighting the permanent harm caused by data breaches.[62] Not only the type of exposed data but also the individual's identity can determine the scale and nature of inflicted harm. Data leaks can put people of diverse gender identities, expressions, and sexualities at risk of being involuntarily outed, potentially leading to family rejection, societal ostracization, loss of employment, or exposure to further stigmatization and violence.[63] Potential consequences for victims of domestic or intimate partner abuse are dire since abusers could use leaked data to locate, intimidate, or further control their targets, exacerbating their vulnerability and undermining their safety and efforts to seek health care.[64]

Data breaches, disruptive and punitive attacks, and misinformation prevent patients from accessing needed services. Limited or restricted access undermines the individual's rights to

[60] U.S. Department of Health and Human Services. "The Biden-Harris Administration Issues New Rule to Support Reproductive Health Care Privacy Under HIPAA." Press release. April 22, 2024. https://www.hhs.gov/about/news/2024/04/22/biden-harris-administration-issues-new-rule-support-reproductive-health-care-privacy-under-hipaa.html.

[61] Madnick, Stuart E. "The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase." Apple Newsroom. December 2023. https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf.

[62] Pavlova, Pavlina. "Gendered Harms of Data Weaponization: Historical Patterns, New Battlefields, and the Implications for Democracy and National Security." Future Security. New America. Last updated November 14, 2024. https://www.newamerica.org/future-security/reports/gendered-harms-of-data-weaponization/.

[63] Tiwari, Divya. "Data Breach Affects Women More, Has Chilling Effect on Their Online Participation." BehanBox. December 6, 2023. https://behanbox.com/2023/12/06/data-breach-affects-women-more-has-chilling-effect-on-their-online-participation/; U.S. Department of Health and Human Services. "The Biden-Harris Administration Issues New Rule to Support Reproductive Health Care Privacy Under HIPAA." Press release. April 22, 2024. https://www.hhs.gov/about/news/2024/04/22/biden-harris-administration-issues-new-rule-support-reproductive-health-care-privacy-under-hipaa.html.

[64] Electronic Privacy Information Center. "Data Broker Harms: Domestic Violence Survivors." Fact sheet. 2024. https://epic.org/documents/data-broker-harms-domestic-violence-survivors/.

have access to quality healthcare services and make informed decisions about their care, and negatively impacts health outcomes.[65] Privacy risks are the highest for vulnerable patients, including minors, individuals seeking gender-affirming care, and those in abusive relationships.[66] The external, downstream effects of cyberattacks intersect with structural inequalities, affecting communities based on gender, race, and geographic access. People of diverse gender identities and sexual orientations, as well as Black and Indigenous women, migrants, persons with disabilities, people who are low-income or living in poverty, and rural residents, all of whom typically experience poorer health outcomes compared to other populations, are disproportionately impacted by interference with their access to essential SRH services, further deepening existing health disparities and social inequities.[67]

IMPACTS ON STAFF AND ORGANIZATIONS

Psychological and physical harm to staff caused by cyberattacks and other technology-facilitated attacks is significantly overlooked, both in wider reporting and in organizational responses to incidents.[68] According to available surveys, abortion providers and those providing other SRH services report being subjected to a wide range of hostilities, from online harassment to threats to personal safety and physical violence. With hostility amplified by conservative media and anti-abortion groups, frontline staff members face frequent antagonism, yet the gravity of reprisals against providers is scarcely recognized.[69] Ideologically motivated attacks can be intended as both punitive — by punishing healthcare workers who

[65] Pavlova, Pavlina. “Gendered Harms of Data Weaponization: Historical Patterns, New Battlefields, and the Implications for Democracy and National Security.” Future Security. New America. Last updated November 14, 2024. https://www.newamerica.org/future-security/reports/gendered-harms-of-data-weaponization/.

[66] McDonald, Nora, Alan Luo, Phoebe Moh, Michelle L. Mazurek, and Nazanin Andalibi. “Threat Modeling Healthcare Privacy in the United States.” ACM Transactions on Computer-Human Interaction 32, No. 1 (2025): Article 8, 1–37. https://doi.org/10.1145/3704634; McDonald, Nora. “Reproductive Health Care Faces Legal and Surveillance Challenges Post-Roe – New Research Offers Guidance.” The Conversation. January 24, 2025. https://theconversation.com/reproductive-health-care-faces-legal-and-surveillance-challenges-post-roe-new-research-offers-guidance-246869.

[67] Ehrlich, Shoshanna. “HIPAA’s Reproductive Privacy Rule Under Siege: Legal Attacks and a Trump Administration Loom.” Ms. Magazine. January 31, 2025. Updated February 10, 2025. https://msmagazine.com/2025/01/31/abortion-privacy-healthcare-data-shield-law-ban-state/; Joh, Elizabeth E. “Dobbs Online: Digital Rights as Abortion Rights.” UC Davis Legal Studies Research Paper No. 604. September 5, 2022. https://ssrn.com/abstract=4220828; Pavlova, Pavlina. “Gendered Harms of Data Weaponization: Historical Patterns, New Battlefields, and the Implications for Democracy and National Security.” Future Security. New America. Last updated November 14, 2024. https://www.newamerica.org/future-security/reports/gendered-harms-of-data-weaponization/; Shires, James, Bassant Hassib, and Amrit Swali. “Gendered Hate Speech, Data Breach and State Overreach: Identifying the Connections between Gendered Cyber Harms to Shape Better Policy Responses.” Chatham House Research Paper. International Security Programme. May 2024. https://www.chathamhouse.org/sites/default/files/2024-05/2024-05-24-gendered-cyber-harms-shires-et-al_0.pdf.

[68] Personal interview.

[69] Boydell, Victoria, et al. “Hostilities Faced by People on the Frontlines of Sexual and Reproductive Health and Rights: A Scoping Review.” BMJ Global Health 8 (2023): e012652. https://gh.bmj.com/content/8/11/e012652.

provided reproductive health care — and disruptive, by hindering staff from operations and leading to increased workload under pressure.[70] Breaches of sensitive medical data can erode trust in healthcare services and hinder the capacity of organizations to protect patient data. Other (punitive) attacks and data brokers' practices can lead patients to withdraw from using SRH facilities and services. If patients believe their sensitive health information may be misused, a climate of insecurity may endanger their relationships with healthcare providers.[71] Surveillance practices, exemplified in gathering and publishing location data about SRH facilities, put both patients and providers at risk, hampering the equitable provision of healthcare services.[72]

Online harassment and doxxing of people working for SRH organizations are pervasive. "The technology-facilitated abuse is so widespread that it is often not discussed openly," according to Galperin. There is also significant shame and a lack of knowledge about mitigating the psychological effects of harassment. The public discourse often overlooks the scale and normalization of abuse, as well as the psychological toll it takes on individuals.[73] There is a lack of attention to how providers can mitigate these effects, for example, by delegating online account monitoring to others rather than handling it themselves to help reduce trauma. Campaigns against healthcare workers have severe psychological and organizational impacts, including burnout and trauma. Online attacks also increase exposure to real-world physical violence or confrontations targeting healthcare staff.[74]

Reputational harm is a major concern for healthcare organizations. Data breaches of sensitive medical information regularly lead to legal action and financial compensation for victims. The fear of reputational harm often guides incident responses, communication efforts, and services offered to victims, such as identity theft monitoring services. This dynamic is understandable, as poor external communication practices — for example, when an organization delivers late notice to people affected by a cyber incident — may have significant reputational consequences, especially if a breach leads to further data misuse. Reputational harm is also tightly interconnected with the sensitivity of the provided services. Organizations holding SRH

[70] MacColl, Jamie, et al. The Scourge of Ransomware: Victim Insights on Harms to Individuals, Organisations and Society. Royal United Services Institute (RUSI). January 2024. https://static.rusi.org/ransomware-harms-op-january-2024.pdf.

[71] Huq, Aziz Z., and Rebecca Wexler. "Digital Privacy for Reproductive Choice in the Post-Roe Era." New York University Law Review 97 (2022): 1–93. U of Chicago, Public Law Working Paper No. 812. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4191990.

[72] Pavlova, Pavlina. "Gendered Harms of Data Weaponization: Historical Patterns, New Battlefields, and the Implications for Democracy and National Security." Future Security. New America. Last updated November 14, 2024. https://www.newamerica.org/future-security/reports/gendered-harms-of-data-weaponization/.

[73] Personal interview.

[74] Personal interview.

information are more susceptible to reputational harm, which can translate into financial harm in the form of lawsuits, regulatory scrutiny, and financial liabilities.[75]

Essential baseline cybersecurity practices are frequently missing. Lack of investment in cybersecurity and ineffective allocation of budget are persistent in SRH facilities of all sizes. Additionally, large health care providers often struggle with challenges posed by legacy computer systems and a lack of cybersecurity due diligence during mergers. Smaller clinics are at risk due to limited resources for cybersecurity and the potentially devastating financial consequences if a breach occurs. Healthcare systems serving marginalized and vulnerable populations typically have even fewer resources. SRH facilities at large prioritize delivery of care and deprioritize cybersecurity and harassment mitigation, which leaves them vulnerable to attacks and psychological harm.[76]

[75] MacColl, Jamie, et al. The Scourge of Ransomware: Victim Insights on Harms to Individuals, Organisations and Society. Royal United Services Institute (RUSI). January 2024. https://static.rusi.org/ransomware-harms-op-january-2024.pdf.

[76] U.S. Department of Health and Human Services, Office for Civil Rights. "Cybersecurity Best Practices for Small Healthcare Providers." https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html; Personal interview.

Recommendations: Law and Practice, Collaborative Strategies, and Community-Driven Solutions

LAW AND PRACTICE

Strengthen federal-level data protection: Data privacy laws at the federal level need strengthening, especially for medical data. Current policies vary by state; some states have strong privacy laws while others do not, creating a patchwork that complicates protection efforts. Vulnerable populations — especially in rural areas, states with abortion bans, or areas where SRH care is limited — are disproportionately affected by weak data privacy regulation. In addition, the future application of the 2024 HIPAA Privacy Rule to Support Reproductive Health Care Privacy depends on court decisions. Federal legislative action should shield medical data from restrictive law enforcement and civil plaintiffs to extend strong safeguards.

Hold companies accountable for data practices: The privacy of users is shaped by several factors, including how applications and devices collect and share information, how companies decide to retain data, how they respond to regulatory demands, and whether they provide privacy-protective infrastructure that allows individuals to access accurate information securely and confidentially.[77] The vulnerability of users' data, therefore, depends on the choices made by those who develop and deploy software and applications. PPI, protected health information, and other medical data should not be collected unless absolutely necessary. When collecting sensitive data is a hard requirement, providers should have clear and accessible options in place to ensure effective data deletion and prevent unauthorized disclosure once the data in question is no longer required.

Close loopholes exploited by data brokers: The risks associated with data brokers exposing geolocation data can be mitigated legislatively by banning secondary uses of collected data and, technically, by enhancing data security and limiting data sharing. Anonymized location data can

[77] Huq, Aziz Z., and Rebecca Wexler. "Digital Privacy for Reproductive Choice in the Post-Roe Era." New York University Law Review 97 (2022): 1–93. U of Chicago, Public Law Working Paper No. 812. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4191990; Center for Democracy and Technology, "CDT Releases Best Practices for Companies to Protect Reproductive Health Data." Press release. May 31, 2023. https://cdt.org/press/cdt-releases-best-practices-for-companies-to-protect-reproductive-health-data/.

still be de-anonymized if enough data points are available, making comprehensive protections necessary. Legal loopholes used by data brokers to collect and monetize location information must be closed to prevent data misuse and protect patients and staff.[78]

Design secure infrastructure: Data protection must be addressed on the infrastructure and software layers on which SRH servers and networks operate, which are typically developed by third-party vendors. Technology vendors and companies that build software need to ensure their products and services are designed, developed, and tested to limit the number of exploitable flaws. The U.S. Cybersecurity and Infrastructure Agency (CISA) launched the Secure by Design initiative in April 2023 to encourage technology manufacturers to integrate security as a core requirement throughout the software development lifecycle. Since the introduction of this initiative, over 300 technology companies have pledged their support.[79] However, this framework is only voluntary and should be mandated to ensure consistency, accountability, and protection for critical infrastructures and sensitive data environments.

Expand cooperation with private providers: Government agencies, such as CISA and HSS, play a supportive role in cybersecurity and infrastructure protection for healthcare facilities, which are largely privately owned and operated. Improved outreach and assistance by the government should extend to smaller providers facing capacity constraints. Additional support must also account for diverse SRH providers, including under-resourced companies that lack the means to pay for incident detection and response, and consider the specific SRH landscape.

Recognize SRH services as critical infrastructure: SRH infrastructure and services must be protected at the federal level to support equitable access and comprehensive care. SRH should

[78] In January 2025, the Federal Trade Commission (FTC) finalized enforcement orders against selected data brokers for unlawfully selling sensitive location data, reinforcing the FTC's stance that selling or sharing sensitive personal data requires safeguards and consumer consent. This includes prohibiting Gravy Analytics and its subsidiary Venntel from tracking and selling data about consumers' visits to healthcare-related locations. Source: Federal Trade Commission "FTC Finalizes Order Prohibiting Gravy Analytics, Venntel from Selling Sensitive Location Data." January 14, 2025. https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-order-prohibiting-gravy-analytics-venntel-selling-sensitive-location-data.

Starting January 2025, California requires data brokers to register with the California Privacy Protection Agency (CPPA). The annual registration fee substantively increased to fund the Delete Request and Opt-Out Platform (DROP), allowing consumers to submit opt-out or deletion requests to all registered data brokers through a single mechanism. Source: California Privacy Protection Agency. "Proposed Regulations on Accessible Delete Mechanism – Delete Request and Opt–out Platform (DROP) System Requirements." April 25, 2025. https://cppa.ca.gov/regulations/drop.html.

The Consumer Financial Protection Bureau (CFPB) is advancing a proposed rule to limit the sale of sensitive personal and financial data by data brokers. The rule would classify certain data brokers as consumer reporting agencies under the Fair Credit Reporting Act (FCRA), require explicit consumer authorization for data sales, and protect against the misuse of social security numbers and other sensitive information. Source: Consumer Financial Protection Bureau. "CFPB Proposes Rule to Stop Data Brokers from Selling Sensitive Personal Data to Scammers, Stalkers, and Spies." December 3, 2025. https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-rule-to-stop-data-brokers-from-selling-sensitive-personal-data-to-scammers-stalkers-and-spies/.

[79] The U.S Cybersecurity and Infrastructure Security. "Secure by Design Pledge." https://www.cisa.gov/securebydesign/pledge.

be explicitly recognized as critical infrastructure.[80] Some states have already taken measures to provide this protection. For example, the State of New York has identified the need for critical infrastructure updates for reproductive healthcare facilities.[81] Planned Parenthood, along with a coalition of nearly 80 organizations behind the Blueprint for Sexual and Reproductive Health, Rights, and Justice — a comprehensive federal policy agenda that promotes integrating SRH equity into federal processes — advocate for treating these services as fundamental to national health and well-being and establishing permanent governmental structures and dedicated funding to ensure SRH equity is integrated into public health strategies.[82]

COLLABORATIVE STRATEGIES AND COMMUNITY-DRIVEN SOLUTIONS

Pool resources to counter SRH-specific threats: Both formal and informal cooperation among large, medium, and small organizations to share intelligence and indicators around attacks is essential. For example, seeking to advance a political cause, ideological actors or hacktivists may openly and publicly coordinate their attacks. Ideologically motivated campaigns can be monitored, whether through keyword alerts (tracking the names of individual facilities), or by monitoring social media, messaging platforms, or forums on the dark web. Many larger organizations employ vendors and analysts to monitor the internet for signs of reputationally damaging campaigns, and to alert victims to social media smear campaigns and potential attacks. Diverse SRH organizations should share sector-specific threat intelligence around both financially and ideologically motivated attacks, provide backchannels, and manage trust groups, such as H-ISAC and other industry-specific cybersecurity working groups and alliances, to prevent and reduce the impact of cyberattacks and coordinated campaigns.

Expand collaborative models to serve smaller and under-resourced clinics: Establishing ISAC-like services for local clinics can match the specific needs of this sector and accommodate many diverse SRH operators and services. Especially for smaller organizations, sharing a Chief

[80] SRH is not formally recognized as part of the U.S. federally designated critical infrastructure at the national level. While healthcare broadly is included, SRH facilities and services are not specifically listed as a protected subcategory. The U.S. Department of Homeland Security (DHS) defines critical infrastructure as systems and assets that are so vital that their incapacity would have a debilitating impact on security, the economy, or public health and safety. Source: Cybersecurity and Infrastructure Security Agency (CISA). "Healthcare and Public Health Sector." https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/healthcare-and-public-health-sector.

[81] The state is investing in security, modernization, and capital improvements to ensure these services' availability and safety. Governor Hochul's policies and funding highlight a commitment to treating reproductive health care as essential for equitable access. Source: Governor Kathy Hochul. "2025 State of the State." January 9, 2024. https://www.governor.ny.gov/sites/default/files/2025-01/2025StateoftheStateBook.pdf.

[82] "Blueprint for Sexual and Reproductive Health, Rights, and Justice." October 2023. https://reproblueprint.org/wp-content/uploads/2023/10/Blueprint-for-Sexual-Reproductive-Health-Rights-Justice_October-2023.pdf.

Information Security Officer (CISO) among several entities can also be an effective practice to address cybersecurity challenges through expert leadership without incurring full-time costs. Other collaborative models, such as the Cyber Resilience Corps, a program that mobilizes cybersecurity expertise and resources from a range of organizations, can be leveraged to support under-resourced healthcare providers. These models must be implemented with acute awareness of the sensitivity of SRH data and the heightened risks of potential compromise from within.

Limit data collection, adjust informed consent, and offer privacy guidance: Care providers must ensure that vulnerable populations they cater to are protected, including by limiting the collected data that could be misused for financial or ideological exploitation, for example, patient records, appointment metadata, or location data. SRH facilities need to prioritize data security practices, such as revised protocols for access privileges that limit misuse stemming from unauthorized access or breach. Approaches to informed consent in SRH also need to account for the growing data privacy challenges. Consent practices must clearly inform patients about how their data may be processed, stored, and potentially shared, and to what aims, and provide patients with transparent options to exert control over their data. By incorporating digital privacy and threat modeling into their care, clinics can help patients navigate a complex landscape of threats in an environment of pervasive surveillance.[83] SRH organizations should also implement accessible tools and protocols that reinforce patient trust and access to care, and that are effective without being intimidating. Providers should consider the diversity of patient technology literacy and avoid overly complex tools that could confuse or deter patients from using services. Importantly, healthcare staff is uniquely positioned to offer critical privacy guidance.[84] This is not uncharted territory, as publicly available resources, including the Digital Defense Fund's Privacy Toolkit, the Electronic Frontier Foundation's Surveillance Self-Defense, and the platform offered by I Need An A (ineedana), are designed to help users to safely navigate their options.[85]

Implement facility-specific protocols and trauma-informed support: SRH incident response protocols should be tailored to the unique operational and privacy needs of

[83] The Conversation. "How Abortion Providers Can Help Patients Navigate Threats to Digital Privacy." Fast Company. January 27, 2025. https://www.fastcompany.com/91266872/how-abortion-providers-help-patients-navigate-threats-digital-privacy.

[84] McDonald, Nora, Alan Luo, Phoebe Moh, Michelle L. Mazurek, and Nazanin Andalibi. "Threat Modeling Healthcare Privacy in the United States." ACM Transactions on Computer-Human Interaction 32 No. 1 (2025): Article 8, 1–37. https://doi.org/10.1145/3704634.

[85] Digital Defense Fund. "Keep Your Abortion Private & Secure." https://digitaldefensefund.org/ddf-guides/abortion-privacy; Electronic Frontier Foundation. "Surveillance Self-Defense: Tips, Tools and How-Tos for Safer Online Communications." https://ssd.eff.org; Ineedana.com. "Release Notes #7 - I Need An A Chat." https://www.ineedana.com/blog/release-notes-7.

each facility. Stronger measures often come only in the aftermath of an attack. Firewall enhancements, implementation of multi-factor authentication, third-party forensic audits, and employee retraining must be applied proactively. Building operational resilience through practicing coordinated responses and ensuring timely communication are crucial to protect patient safety and trust throughout incidents. Addressing the psychological impact of a cyberattack and other technology-facilitated attacks on staff needs to be at the center of responses to an incident. This requires not only raising awareness of potential psychological harm, but also ensuring that crisis management focuses on mitigating such harm.[86] Effective support structures addressing cyber harassment and doxing campaigns against SRH staff should include delegating harassment monitoring to others to minimize personal trauma, providing psychological support to affected staff, and signing up for data broker deletion services to reduce personal data exposure. Staff training and trauma-informed support systems are also important as part of prevention and post-incident mitigation. Publicly available resources supporting these efforts include the Digital Safety Kit for Public Health, developed by the Harvard T.H. Chan School of Public Health's Center for Health Communication, which aims to help public health workers and researchers navigate hostile online experiences.[87]

[86] MacColl, Jamie, et al. The Scourge of Ransomware: Victim Insights on Harms to Individuals, Organisations and Society. Royal United Services Institute (RUSI). January 2024. https://static.rusi.org/ransomware-harms-op-january-2024.pdf.

[87] Harvard T.H. Chan School of Public Health's Center for Health Communication. "Digital safety kit' offers guidance for public health workers dealing with online harassment." January 31, 2024. https://hsph.harvard.edu/news/digital-safety-kit-offers-guidance-for-public-health-workers-dealing-with-online-harassment/.

Conclusion

The study finds that cyber threats targeting SRH facilities and services come in complex combinations, driven by financial extortion, ideologically motivated attacks, data commercialization, and misuse. Cybercriminal gangs breach sensitive medical records in ransomware bids. Anti-abortion activists harass patients and providers, interfere with access to healthcare services, and lead coordinated campaigns to discourage individuals from seeking essential care. Data brokers sell location data that can expose individuals' visits to specialized clinics and femtech shares personal and medical information with third parties. The downstream impacts of these actions impact vulnerable communities and societal trust in health care and SRH applications.

This research calls for an urgent expansion of efforts to improve resilience across SRH facilities, particularly as these organizations become increasingly targeted, disputed, and politicized. Current data and cybersecurity practices concerning sensitive and personal medical data and healthcare infrastructure are in most cases inadequate and unsustainable. A variety of factors — including extensive data collection, weak SRH-specific data privacy and protection regimes, fragmented regulation that varies by state, lack of government and private-sector coordination that harms especially smaller and under-resourced providers, and gaps in cybersecurity preparedness and resource allocation — translate into an insecure environment. As pressure on the SRH sector grows, strengthening policy and legal frameworks as well as digital defenses through collaborative approaches will be critical to safeguarding patient rights, safety of SRH staff, and the integrity and equity of provided healthcare.

About the Author

Pavlina Pavlova is a policy expert with a cross-cutting perspective on international cybersecurity and transnational cybercrime. Her experience spans technology, security, governance, and human rights in civil society and at national, regional, and international institutions, and she leads stakeholder engagement in UN cyber-related processes. Pavlova's research examines the societal and human impacts of cyber incidents on critical infrastructure to advance evidence-based approaches to cyber resilience.

Acknowledgments

I am deeply grateful for the support of the UC Berkeley Center for Long-Term Cybersecurity team, including Ann Cleaveland, Sarah Powazek, Shannon Pierson, and Audrie Francis. I also extend my sincere appreciation to the philanthropy, industry partners, and individual donors whose contributions make the Public Interest Cybersecurity Research Call possible and propel CLTC's mission. Finally, I am indebted to the individuals who shared their lived expertise during the interviews.

CLTC

Center for Long-Term Cybersecurity

UC Berkeley

Center for Long-Term Cybersecurity | cltc.berkeley.edu | @CLTCBerkeley