News and Perspectives

More Should Be Done to Protect Reproductive Health Data in FemTech Apps

Jenny Castillo Cato, JMIR Correspondent

Abstract

FemTech apps enable women to track their own data and better understand their own health, but are the data always used for the purposes we'd expect? In this *News and Perspectives* op-ed, JMIR Correspondent Jenny Castillo Cato reports on how reproductive health data could be misused, arguing for stronger data privacy and security protections.

Key Takeaways:

- Despite empowering women, FemTech apps may lack sufficient data privacy and security protections.
- These apps may expose women to both privacy and legal risks: FemTech data could be used to prosecute women seeking reproductive health care in areas with legal restrictions.

Jenny Castillo Cato, MD, a board-certified emergency medicine physician, continues her series on FemTech with this op-ed exploring tensions around data privacy and liability in FemTech.

Over the past decade, FemTech—technology designed for women's health—has helped to increase access to information and promote awareness of women's health issues, improving understanding of historically understudied conditions such as endometriosis. However, as these technologies continue to evolve, they have become central to an ethical dilemma: the balance between empowerment and liability.

While FemTech apps can empower women, major fears about data privacy, security, and misuse are surfacing and becoming reality. Both regulators and app developers should be doing more to protect reproductive health data.

Lack of Privacy Protections

Within the medical community, protecting patient confidentiality and personal health information is a fundamental ethical and legal responsibility. The Health Insurance Portability and Accountability Act (HIPAA) establishes US federal protections for sensitive health information. Health care professionals and organizations must comply with its requirements, and violations can result in serious consequences. However, health app data collected by app developers not affiliated with health care plans, clearinghouses, or providers typically do not fall under this act. As a result, the sensitive information collected by FemTech apps—for example, menstruation, fertility, and pregnancy status—are not protected.

Many FemTech companies rely on collecting, analyzing, and sharing user data to generate revenue, support targeted advertising, or develop commercial insights. This information is a valuable commodity—one that some companies will commit privacy violations to trade in. When personal reproductive health data are treated as a resource, it puts users' privacy at risk and raises critical questions about informed consent, corporate accountability, legal compliance, and the extent to which FemTech companies should be responsible for protecting their users' privacy.

Potential Monitoring and Misuse

Without comprehensive regulations, sensitive information collected through these increasingly popular apps may also be vulnerable to misuse, surveillance, or access by government authorities. Precedence for the systematic collection, monitoring, and scrutinization of women's reproductive choices or statuses already exists. In 2019, the US Senate Committee on Health, Education, Labor, and Pensions investigated the Office of Refugee Resettlement for maintaining a spreadsheet that tracked "private reproductive health information for pregnant minors, some as young as 12- and 13-years old."

These concerns are further illustrated by legislative efforts to monitor pregnancies; for example, in Missouri, Bill HB 807 proposed establishing a "central registry of each expecting mother who is at risk for seeking an abortion." Although the proposed legislation did not pass, it illustrates how reproductive health data could potentially be repurposed for uses that extend far beyond the original intentions of the individuals who provided it.

These theoretical concerns are a real possibility.

A 2022 report by the Organization for the Review of Care and Health Apps (ORCHA) found that 67% of the period-tracking apps it assessed shared data for reasons related to "legal obligations." This broad category raises concerns about the circumstances under which companies may disclose sensitive

information; geolocation data, for example, could be used to establish whether an individual or their device was present at a particular location, such as an abortion clinic. Another study examining 23 popular women's mobile health apps found that the apps permitted location tracking (61%), shared collected data with third parties (87%), collected personal health information (100%), and enabled behavioral tracking (100%). Combined with menstrual cycle records and fertility information, such data could be used in jurisdictions where abortion is criminalized or legally restricted with serious implications for individuals seeking reproductive health care.

In an evolving, frequently contentious legal and political landscape, why has the safeguarding of women's digital reproductive health information not become a more urgent public policy priority?

According to Sara Geoghegan, JD, Director of the Consumer Privacy Program and Senior Counsel at the Electronic Privacy Information Center (EPIC) in Washington, DC, the lack of progress in reproductive health data privacy protections is simple. "The current US administration and Federal Trade Commission have not made it a priority."

Safeguarding Efforts

Some organizations have taken their own steps to offer more privacy-conscious alternatives. In July 2026, an in-depth evaluation of 6 popular FemTech apps gave Euki, an open-source application managed by a nonprofit organization, a perfect privacy score of 10 out of 10. Euki is designed to store users' health information locally on their devices rather than on company servers and allows individuals to use the app without creating an account. It also includes a decoy feature that displays misleading information to someone attempting to access a user's private data without authorization. Privacy can be incorporated into an app's design, rather than treated as an afterthought.

However, according to the same evaluation, even apps that adopt privacy-conscious practices may expose users to risks through external websites or integrated services. For example, Planned Parenthood's Spot On app purports not to track or share users' information within the app itself. However, accessing certain features, such as the Roo chatbot or the health care provider search tool, may redirect users to Planned Parenthood's website. If those external services employ third-party tracking technologies, information about users' interactions may be shared with companies such as Google, Microsoft, TikTok, and Pinterest without the users' knowledge.

Geoghegan highlights the work of the Digital Defense Fund, an organization originally focused on reproductive rights but whose mission has expanded to support "autonomy and liberation" more broadly. Through practical account security resources and data management, the Digital Defense Fund aims to help individuals strengthen their digital privacy and protect sensitive information.



Privacy can be incorporated into an app's design, rather than treated as an afterthought.

Efforts to address these privacy concerns are also emerging at the federal legislative level. In November 2025, Senator Bill Cassidy introduced the Health Information Privacy Reform Act, which seeks to extend federal privacy protections to entities not currently regulated by HIPAA, including health apps, wearable devices, and consumer-based genetic testing services. Seventeen states have also enacted shield laws addressing reproductive health and gender-affirming care, with 8 of those states extending protections to telehealth services. However, existing shield laws do not explicitly address or provide protections for reproductive health information collected, stored, or shared through FemTech platforms.

FemTech has provided enormous advances in women's reproductive health information and access, but these advances could be undermined if users cannot trust that their most sensitive information is safe. Individual users can take proactive steps to protect their privacy. These include familiarizing themselves with social media privacy settings, determining which accounts should remain private versus public, and exercising caution when sharing location information. Region-specific FemTech consumer guidance—like this guide developed by European researchers, along with international experts—could be highly beneficial in this context. As FemTech continues to expand, however, the onus should not rest solely with users to protect themselves.

App developers must protect reproductive health data, balancing legal obligations to comply with lawful disclosure requests with their responsibility to implement appropriate data privacy safeguards: providing transparency around legal and commercial third-party data sharing practices, minimizing unnecessary data collection, strengthening encryption and anonymization, and limiting IP address tracking. If voluntary industry practices fail to provide adequate safeguards, comprehensive legislation may be necessary to establish enforceable privacy standards, increase corporate accountability, and protect individuals from the potential misuse of their reproductive health data.

Keywords: data privacy; data security; reproductive health; mobile apps; confidentiality; legal regulation; health information management; FemTech

Please cite as:
Cato JC
More Should Be Done to Protect Reproductive Health Data in FemTech Apps
J Med Internet Res 2026;28:e116574
URL: https://www.jmir.org/2026/1/e116574
doi: 10.2196/116574

© JMIR Publications. Originally published in the Journal of Medical Internet Research (https://www.jmir.org), 13.Nov.2026