TELEHEALTH AND MEDICINE TODAY

OPINIONS, PERSPECTIVES, COMMENTARY

When AI Becomes Care: Governance Gaps in Women's Health Technologies

Soribel Feliz MA/MPA[1,2,3,4]

[1]Personal Algorithms, LLC, Richmond, Virginia, USA; [2]DHS AI Corps; [3]U.S. Senator Bill Cassidy, Shreveport, Louisiana, USA; [4]AI Governance

DOI: https://doi.org/10.30953/thmt.v11.683

Corresponding Author: Soribel Feliz, Email: soribelfelix@gmail.com

Keywords: AI governance, care infrastructure, health technologies, women's health

Abstract

Women's health apps are increasingly treated as care infrastructure. They track cycles, predict fertility, assess pregnancy risk, and shape decisions using artificial intelligence (AI)-driven systems, often filling gaps left by a medical establishment that has long underinvested in women's health. At the same time, many of these tools operate with minimal AI governance and fragile privacy protections. Founders frequently point to compliance with the U.S. Health Insurance Portability and Accountability Act as reassurance, even when their products fall outside its scope or rely on automated inference that compliance alone does not address. This op-ed examines how women's health technologies became substitutes for care, where governance breaks down in practice, and why AI governance now functions as women's health policy in the United States. As legal and social conditions shift, the cost of weak governance is no longer abstract, and the people bearing that cost are rarely the ones building the products and systems.

Submitted: January 6, 2026; Accepted: April 29, 2026; Published: June 20, 2026

Women's health apps increasingly rely on artificial intelligence (AI) and machine learning systems to analyze user data and generate insights. These AI systems operate in several ways:

Predictive Algorithms analyze historical menstrual cycle data, symptoms, and behavioral patterns to forecast ovulation windows, period timing, and fertility likelihood. These predictions are probabilistic, not diagnostic, but users often treat them as medical guidance.

Inferential Models draw conclusions about health states users never explicitly disclosed. An app may infer pregnancy based on missed periods, a cluster of symptoms, or changes in activity patterns. It may categorize users into risk profiles based on age, weight, or search behavior.

Recommendation Systems suggest actions, products, or clinical pathways based on user data and cohort comparisons. These recommendations shape decisions about when to seek care, what symptoms to monitor, or which products to purchase.

Natural Language Processing analyzes symptom descriptions, mood entries, and open-text responses to extract sentiment, health indicators, or behavioral signals that feed back into prediction models.

From a user perspective, these systems feel seamless. From a governance perspective, they introduce significant complexity: data flow across multiple parties, inferences compound over time, and the boundary between support and surveillance becomes difficult to discern.[1]

This op-ed focuses primarily on AI governance: how these systems are built, what data they use, and who bears risk when they fail, while acknowledging that governance intersects with broader concerns around cybersecurity, research ethics, and equitable access. Those dimensions matter deeply but require separate analysis. Here, the focus is on governance gaps that directly affect user safety, autonomy, and trust.

This piece proceeds in three parts. First, how apps became substitutes for care. Second, where governance breaks down in practice, particularly around U.S. Health Insurance Portability and Accountability Act (HIPAA) misunderstandings, AI inference, and post-Dobbs legal risks. Third, a minimum governance standard for apps functioning as care infrastructure is proposed.

When Apps Start Doing the Work of Care

Women's health apps did not appear because the healthcare system was working well for women. They appeared because it was not. For decades, women have faced research gaps, dismissed symptoms, long wait times, affordability concerns, and limited access to providers who take their concerns seriously.

Health Apps Stepped Into That Vacuum

They promise pattern-finding, validation, reassurance, and a sense of control over one's body. In contrast to rushed clinical visits, an app listens constantly. It remembers. It responds without judgment. It offers explanations where doctors sometimes offer dismissal.

Over time, that attention turns into trust. Many users stop thinking of these tools as optional accessories and start treating them as part of how they manage their health.

That shift matters. When apps begin doing the emotional and informational work of care, they also inherit expectations around responsibility, protection, and accountability. Expectations about privacy and data stewardship. Those expectations are rarely met.

Empowerment language fills the gap. Users are told they are taking control of their bodies and their health. What they are rarely told is how their most intimate data moves, how it is inferred, or what happens when contexts change.

When Governance Questions Become Uncomfortable

At a pitch competition I attended, a female founder was presenting a women's health product designed to collect and analyze deeply sensitive pregnancy data. The product was framed as empowering, data-driven, and innovative.

During the question and answer session, I asked a straightforward question: What happens to a user's data if she experiences a pregnancy loss in a state with abortion restrictions?

The response came quickly. "We're HIPAA compliant."

Then the founder turned her head and body away from me and immediately took the next question.

That moment was telling. Not because the founder was malicious or careless, but because the phrase "we're HIPAA compliant" functioned as a conversational off-ramp. It sounded reassuring. It moved things along. It shut the discussion down.

That response is common. It should not be. Because "HIPAA compliant" rarely means what users think it means.

The HIPAA Shield Illusion

HIPAA was signed into law in 1996, long before app stores, data brokers, and AI-driven analytics became part of everyday healthcare.[4] For most people, HIPAA is synonymous with health privacy. It appears on intake forms, consent notices, and patient portals. Over time, it has become shorthand for safety.

That familiarity creates a powerful assumption. If something deals with health, it must be protected by HIPAA.

Most Consumer Health Apps Are Not

Many women's health apps are not covered entities under HIPAA. Data brokers are not covered entities. Third-party analytics firms are not covered entities. Compliance with HIPAA does not prevent data sharing with advertisers, analytics providers, or partners. It does not block subpoenas or warrants. It does not anticipate how inferred data may be used later.[2]

To Understand the Gap, It Helps to Look at How Data Actually Flow

A user downloads a period or pregnancy app and enters information about symptoms, cycle timing, mood, or sexual activity. Those data are stored by the app, but the app also relies on third-party software development kits (SDKs) for analytics, performance monitoring, or engagement tracking. Those third parties may receive event-level data, timestamps, device identifiers, or inferred states. The app may then use this information to train or refine AI models that generate predictions and insights.

From the user's perspective, this feels like a single trusted relationship. From a governance perspective, it is an ecosystem with multiple actors, incentives, and exposure points.

HIPAA Does Not Automatically Apply to That Ecosystem

High-profile enforcement actions have already shown how pregnancy and fertility data have been shared with major platforms under the banner of compliance. Enforcement tends to arrive after harm has occurred. For users, that timing matters.

In 2021, the Federal Trade Commission (FTC) settled with Flo Health after the company shared pregnancy and period data with Facebook and Google Analytics despite promises of privacy. At the time, the app had 100+ million users.[3]

According to the FTC complaint, Flo disclosed sensitive health information, such as the fact of a user's pregnancy, to third parties in the form of "app events," which is app data transferred to third parties for various reasons. In addition, Flo did not limit how third parties could use these health data.

Fast-forward to 2024, a jury found Meta liable for intentionally recording protected health information from Flo app users without consent, violating California privacy laws. The pattern is clear: "HIPAA compliant" meant nothing when the app used third-party SDKs that treated intimate health data as marketing intelligence.

"HIPAA compliant" still means nothing.

Compliance Versus Governance

The difference between compliance and governance is subtle but important. Compliance refers to meeting the minimum requirements of a specific law. Governance refers to the choices companies make about how systems behave, how data flow, and who bears risk when something goes wrong.

A company can be compliant and still expose users to harm.

Governance shows up in decisions about what data are collected, how long it is retained, what inferences are allowed, who can access those inferences, and how systems respond when legal or social conditions change. Compliance answers the question, "Are we allowed to do this?" Governance answers the question, "Should we, and under what conditions?"

In women's health technology, too many teams stop at the first question, if they ask that first question at all.

Where AI Changes the Risk Profile

These risks increase once AI systems enter the picture.

Women's health apps increasingly rely on algorithms to infer states users never explicitly disclosing pregnancy, fertility windows, mental health signals, risk categories, and behavioral predictions. These inferences are often probabilistic, undocumented, and difficult for users to see or challenge.

Telehealth and Medicine Today © 2026, 11: 683 - https://doi.org/10.30953/thmt.v11.683

AI creates new data through inference: pregnancy likelihood, fertility windows, and mental health signals, often without user knowledge or consent. Once inferred, these data can be logged, retained, and repurposed in ways users never anticipated. Models may be retrained. Outputs may change. New uses may emerge that were not part of the original product pitch.

This is what makes AI powerful. It is also what raises the stakes.

Without governance, inference becomes a blind spot rather than a feature.

Why the Stakes Are Higher Now

In the U.S., legal and social shifts have changed the consequences of weak governance. In a post-Dobbs era, data that once felt personal now carry legal weight in certain states.[5,6] Inferred health states can become evidence. The same systems designed to support users can expose them.

If a woman experiences a pregnancy loss in a state with abortion restrictions and authorities suspect she traveled across state lines to obtain care, data generated or inferred by a health app or data captured in another app on her phone (say, geolocation data captured by a gaming app) can become part of an investigation. A missed period logged in October. A location ping near a clinic in November. A search for "abortion pill" in December. Each data point alone means little. Together, they build a prosecutable narrative. That data may be accessed through subpoenas, warrants, or third-party intermediaries.[7]

Regardless of the outcome, the burden falls on the individual. Companies that build these products are rarely liable for the potential downstream harm caused by investigations or prosecutions. Governance failures do not distribute consequences evenly. They concentrate them.

Risk accumulates quietly and subtly in these products and systems. Users rarely know who has access to inferred health data, how long it is retained, or how it may be interpreted later. That uncertainty erodes trust in ways that are difficult to repair.[8]

AI Governance as Women's Health Policy

At this point, it becomes difficult to separate women's health outcomes from AI governance choices.

Questions founders avoid answering (and investors avoid asking!) are governance questions. Who can access inferred reproductive data? What happens when legal contexts change? How long is sensitive data retained? Can users meaningfully delete data that trained models, as well as back up data?

AI governance frameworks already exist in other high-impact domains. In finance, organizations are expected to document model purpose, assess downstream effects, and plan for misuse. In traditional healthcare settings, systems that shape care decisions are subject to oversight and accountability.

Women's health technologies have quietly crossed into similar high-risk territory. They influence decisions about care, behavior, and risk. Yet, they are rarely held to comparable governance standards.

AI governance here is not theory or ethics navel-gazing. It is concrete, tangible, operational work.

The Minimum Bar Going Forward

If women's health apps are going to function as care infrastructure, a minimum governance bar is no longer optional.

That bar must include:

1. Clear Limits on AI Inference

Apps should document what health states their AI systems are designed to infer, under what conditions those inferences are generated, and how users can access or challenge them. Inferred pregnancy, mental health signals, or risk categories should not be generated silently. Users deserve to know when an algorithm has drawn conclusions about their bodies.

2. Purpose Limitation and Data Minimization

Collect only the data necessary for the stated purpose. Retain it only as long as needed. Do not repurpose reproductive health data for advertising, engagement optimization, or model training without explicit, informed consent. These principles come from Privacy by Design frameworks and the General Data Protection Regulation's (GDPR's) data protection standards—proven models that already work in other high-risk domains.

3. Third-Party Accountability

If an app relies on third-party SDKs, analytics providers, or cloud infrastructure, those relationships must be disclosed and governed. Contractual agreements should prohibit repurposing health data. Regular audits should verify compliance. The Flo Health case shows what happens when third-party data flows are treated as invisible: user trust is violated, and liability arrives too late.

4. Adversarial Scenario Planning

Governance cannot assume best-case conditions. It must account for worst-case scenarios: subpoenas, warrants, data breaches, and legal contexts shifting overnight. Apps should build data retention policies, encryption standards, and user deletion workflows with these risks in mind. Finance and traditional healthcare already do this. Women's health apps should follow.

5. Transparency and User Control

Users should know what data their app collects, what it infers, who has access, and how long it is retained. They should be able to delete their data—including inferred data and model training contributions—without penalty. Transparency is not a legal nicety. It is foundational to trust.

6. Regulatory Models from Adjacent Domains

Several governance frameworks offer adaptable models:

GDPR (EU): Requires purpose limitation, data minimization, and user rights to access, correct, and delete data. These principles translate directly to reproductive health apps.

FDA Medical Device Oversight: High-risk health technologies already face pre-market review, post-market surveillance, and adverse event reporting. Apps making medical claims or shaping clinical decisions should be subject to similar scrutiny.

Financial Services Model Risk Management: Banks and insurers must document AI model purposes, validate outputs, and assess downstream effects. Women's health apps influencing reproductive decisions operate in comparable risk territory.

The question is not whether governance models exist. They do. The question is whether the industry will adopt them voluntarily or wait for enforcement to force the issue.

Conclusion

Women's health apps can expand access and insight. AI can do pattern recognition and inferencing that would take a human age. But without governance, these health apps, which women trust with their most sensitive personal data, can also amplify harm. And the people bearing that harm are rarely the ones building the products.

The difference lies in whether builders treat governance as infrastructure or an afterthought. Right now, most are choosing the latter.

Women deserve better.

Funding

None.

Financial and Non-Financial Relationship and Activities

None.

Data Availability Statement (DAS), Data Sharing, Reproducibility, and Data Repositories

Not applicable.

Application of AI-Generated Text or Related Technology

Contact the author.

References

1. Frasco v. Flo Health, Inc. Class Action Settlement [Internet]. New York (NY): Labaton Sucharow LLP. [cited 6 Jan 2026]. Available from: https://www.labaton.com/cases/frasco-v-flo-health-inc
2. Matsakis L. Most period apps say they protect your data. They don't. ProPublica [Internet]. 2022 May 23 [cited 6 Jan 2026]. Available from: https://www.propublica.org/article/period-app-privacy-hipaa
3. Federal Trade Commission. Developer of popular women's fertility tracking app settles FTC allegations it misled consumers about privacy [Internet]. Washington (DC): FTC. 2021 Jan 13 [cited 2026 Jan 6]. Available from: https://www.ftc.gov/news-events/news/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc-allegations-it-misled-consumers-about
4. U.S. Department of Health and Human Services. HIPAA privacy laws and regulations [Internet]. Washington (DC): HHS. [updated 2024; cited 6 Jan 2026]. Available from: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
5. U.S. Department of Health and Human Services. HIPAA Privacy Rule and reproductive health information: final rule fact sheet [Internet]. Washington (DC): HHS. 2024 Apr [cited 2026 Jan 6]. Available from: https://www.hhs.gov/hipaa/for-professionals/special-topics/reproductive-health/final-rule-fact-sheet/index.html
6. Hill K. Should you be worried about your period-tracking app after Roe? NPR [Internet]. 2022 May 10 [cited 2026 Jan 6]. Available from: https://www.npr.org/2022/05/10/1097482967/roe-v-wade-supreme-court-abortion-period-apps
7. Pregnancy Justice. Pregnancy as a crime: an interim update on the first two years after Dobbs [Internet]. New York (NY): Pregnancy Justice; 2024 [cited 2026 Jan 6]. Available from: https://www.pregnancyjusticeus.org/resources/pregnancy-as-a-crime-an-interim-update-on-the-first-two-years-after-dobbs/
8. Hao K. Why US women are deleting their period tracking apps. The Guardian [Internet]. 2022 Jun 28 [cited 2026 Jan 6]. Available from: https://www.theguardian.com/world/2022/jun/28/why-us-woman-are-deleting-their-period-tracking-apps