Data Privacy for Reproductive Health

This document is a companion guide to the webinar, "Data Privacy for Reproductive Health," (September 2025), hosted by Rhia Ventures, with panelists from Rhia Ventures, The Center for Democracy and Technology (CDT), Euki, and aboboTech.

This guide will:

- **Clarify** the legal landscape of health data protections, limitations of HIPAA, FTC oversight mechanisms, and state-level privacy laws.
- **Debunk** common misconceptions around data privacy.
- **Explain** shareholder advocacy as a tool for holding corporations accountable, including real examples of negotiated policy improvements.
- **Showcase** current privacy-first innovators in the reproductive health space.
- **Provide** actionable recommendations tailored to different stakeholder groups.

The Legal Landscape of Health Data Privacy: HIPAA Coverage and Limitations

- The Health Insurance Portability and Accountability Act (HIPAA) of 1996 established federal protections for sensitive health information, prohibiting disclosure without patient consent.
- HIPAA:
    - Defines Protected Health Information (PHI) collected by "covered entities": doctors, insurers, healthcare providers, and their associates
    - Limits how these entities can use PHI (generally restricted to provision of care and billing)
    - Prevents use of health information for non-health related purposes

Critical Limitation: HIPAA protections attach to the entity holding the data, not the data itself. If a company isn't a HIPAA-covered entity (like most apps, wearables, and consumer products) HIPAA doesn't apply at all.

- The FTC's Role
    - For non-HIPAA covered entities, the Federal Trade Commission provides oversight through:
        - Section 5 Authority: can bring enforcement actions against companies that mislead consumers about data practices.
        - Health Breach Notification Rule (updated 2024): requires companies managing personal health records to notify the FTC, consumers, and sometimes media about data breaches (including unintended sharing of health data).

- State-Level Data Privacy Protections
  - Washington State - “My Health My Data” Act
    - Limits collection and sharing of consumer health data to only what’s necessary
    - Gives residents more control over their data
    - Represents stronger protections than federal law
  - Other notable states: California, Connecticut, New York (pending governor’s signature)
  - Shield laws: some states have enacted laws specifically to protect residents seeking reproductive healthcare from investigations by other states.

A 2024 update to HIPAA privacy rules that limited law enforcement access to reproductive healthcare data was overturned by a Texas court in early 2025. This made it easier for law enforcement in hostile states to access health records for investigations and prosecutions.

Common Misconceptions about Data Privacy

- **Misconception #1: HIPAA means strong encryption**
  - Reality: HIPAA requires basic encryption meaning that data must be encrypted in transit and at rest. This is standard for modern applications, but it's fundamentally different from end-to-end encryption. With standard HIPAA encryption, the platform provider can still access your data. With end-to-end encryption, they cannot.
  - Why it matters: Many users assume HIPAA compliance means the provider can't see their data. That's not true. HIPAA-compliant means the provider promises to protect your data, not that they can't access it.
- **Misconception #2: Business Associate Agreements (BAAs) Ensure Data Protection**
  - Reality: BAAs are legal agreements platforms sign with any vendor that handles patient data to ensure HIPAA compliance. Those vendors often have their own vendors, who have their own vendors- creating what panelist and aboboTech founder Nancy Mandujano calls a "BAA conga line." Your data passes through multiple companies.
  - Why it matters: Each vendor in the chain is a potential breach point. Patients often receive notification of a data breach from a company they were not even aware had their data.

Shareholder Advocacy as a Tool for Change

- Shareholder Activism has been used since the late 1960s to influence corporate behavior on environmental and social issues. It is a pillar of ESG (Environmental, Social, and Governance) investing that is under threat from current administration’s policies.
- Key players include: ESG investing firms, progressive religious denominations, public pension funds, foundations, and individual investors.
- Shareholder advocates have frequently submitted proposals on a range of issues. Although nonbinding, they can lead to dialogue and negotiations with publicly-traded companies, which can lead to corporate policy changes or additional transparency. Those that proceed to a vote at annual shareholder meetings rarely receive high votes; their leverage is derived from companies’ interest in satisfying investors’ concerns.

When a Fortune 500 company changes policies, it can raise standards across entire sectors.

aboboTech CENTER FOR DEMOCRACY & TECHNOLOGY Euki Rhia VENTURES

Rhia Ventures' Corporate Engagement on Data Privacy

- Target sectors: Retail, pharmacies, financial services, data brokers, travel/hospitality
- 20 shareholder proposals filed at 18 companies over the past three proxy seasons
- Negotiated successes include:
  - Tightened policies on releasing customer data to law enforcement
  - Tracking systems for law enforcement requests
  - Notifications to consumers when they are subject to investigations
  - Expansion of data deletion rights

Principle of Least Privilege:
A process should only be granted minimum access rights necessary to perform its required tasks, reducing security risks.

Privacy-First Innovation in Practice: Euki & aboboTech

- **Euki App- Designing from the Margins**
  - Menstrual tracker app built in 2017 based on research about people facing the most significant barriers to reproductive healthcare access - before Dobbs made these threats mainstream concerns.
  - Co-designed with real users who have exceptional privacy concerns- young people, people of color, transgender folks, and others with marginalized identities.
  - **Innovative Approach:**
    - User data autonomy: All data stored on device only, giving users control of who has access to their data and how long the data is stored.
    - No servers means no data to subpoena
    - Works offline (accessible in rural areas with poor internet connectivity)
  - **Business model impact**
    - Pregnancy data is among the most valuable consumer data. Euki deliberately chose not to monetize it, operating as a nonprofit to maintain this commitment.

- **aboboTech- End-to-end Encryption for Clinic Management**
  - Builds privacy-first clinic management tools for abortion providers and allied organizations
  - True end-to-end encryption: PHI is encrypted so that even aboboTech cannot access it- unprecedented in software.
    - Single-use form links: if someone checks browser history and clicks on a link, they see a non-descript page that neither confirms nor denies a form ever existed.
    - Strategic legal protection: incorporated in New York state to leverage expanded protections for electronic reproductive health data.
    - Single data subprocessor: avoids the "BAA conga line"
  - **Philosophy: "This is the software of our collective dreams- it's a reimagining of what healthcare tech should be, not just what it currently is." -Nancy Mandujano, aboboTech founder**

aboboTech CENTER FOR DEMOCRACY & TECHNOLOGY Euki Rhia VENTURES

Best Practices for Companies

- **Data Minimization**
  - **Collect** only what's absolutely necessary
  - **Retain** data only as long as needed
    - Scrutinize data retention policies; make sure data is only retained as long as purposefully needed
- **User Rights**
  - **Provide** meaningful access and deletion rights
  - **Be transparent** about data practices in plain language
  - **Do not mislead** consumers about how data will be used
- **Post-Dobbs Urgency**
  - **Recognize** that law enforcement and civil rights litigants will increasingly seek data to prove someone sought, received, aided, or provided abortion or reproductive healthcare. This reality demands proactive protection measures.

> ***"The best answer when law enforcement comes asking for that type of information is for a company to say: 'Thank you for asking; pursuant to our policies, we don't have any data to reply.'"***
> ***-Andy Crawford, CDT***

Actionable Recommendations by Stakeholder Type

- **For Organizations and Program Leaders**
  - Audit your data practices
    - Why are specific data being collected? Is each piece of data truly necessary?
    - What's your data retention schedule?
    - Where is your data stored and who has access?
  - Implement data hygiene
    - Clean data regularly
    - Delete information you don't need
  - Question before collecting data

- **For Tech Innovators and Developers**
  - Challenge the status quo
    - Break out of the "growth-at-all-costs" mindset
  - Consider your business model
    - Can you operate without monetizing user data?
  - Prioritize real privacy
    - Implement true end-to-end encryption
    - Design for the most vulnerable users (not just edge cases)

- **For Investors and Funders**
  - Invest in organizations that build privacy-first solutions
  - Reconsider success metrics
    - In the current political climate, not having data can be more valuable than having it.
    - Consider benefit versus risk of requiring detailed reporting, particularly for vulnerable communities being served.

abobTech CDT CENTER FOR DEMOCRACY & TECHNOLOGY Euki Rhia VENTURES

Actionable Recommendations by Stakeholder Type (cont.)

- **For Shareholders**
  - Activate your holdings
    - Determine how your mutual funds/investment firms vote on shareholder proposals
    - Consider taking back voting rights (see resource asyousow.org for more on this)
    - Support ESG-focused funds that vote conscientiously
    - Engage with Shareholder advocates (like Rhia Ventures) for insights and recommendations for best practices.
- **For Healthcare Organizations**
  - Vet vendors thoroughly
    - What are their data retention policies?
    - Do they use third party analytics?
    - Where and how is data stored?
    - What happens in a breach scenario?
  - Minimize data vulnerabilities

Key Takeaways

- Stakeholders at every level- from individual consumers to institutional investors- have concrete tools to push for greater data privacy protections.
- The current landscape is fragmented and insufficient, but through actions like shareholder advocacy, supporting privacy-first technology, demanding corporate accountability, and implementing data minimization principles, meaningful change is possible.
- **Privacy is not just a technical feature- it's a fundamental right that requires intentional design, sustained advocacy, and collective responsibility to protect.**

Thank You to Our Panelists

- **Andrew "Andy" Crawford, Senior Counsel, Privacy and Data, Center for Democracy and Technology**
    - Andrew Crawford is a Senior Counsel with CDT's Data and Privacy Project. In addition to advocating for comprehensive federal privacy legislation, Andrew's work focuses on the intersection of technology, health data, and privacy. He led the development of CDT's Consumer Privacy Framework for Health Data along with the associated paper that identifies and suggests ways that privacy protections can benefit everyone, including underrepresented and overlooked communities harmed by current health data practices.
- **Ana Ramirez, Co-Founder and Co-Executive Director, Euki**
    - Ana is a co-founder and co-executive director of Euki. She is passionate about breaking down barriers to sexual and reproductive healthcare by building robust, privacy-forward tools that put people in control of their own bodies. She leads the design of the Euki app and brings over a decade of research experience on abortion care, menstruation, and HIV/AIDS to her work.
- **Nancy Mandujano, Founder & Senior Geek, aboboTech**
    - Nancy is former social worker and teacher who pivoted to tech over a decade ago as a way to create sustainable, scalable change. Since then, She has co-created software for nonprofits and social justice organizations across NYC, built human-centered solutions with Stanford's AI and Educational Studies Labs (tackling COVID-19 remote learning challenges), and collaborated with Stanford's Computational Policy Lab on media representation projects with the BBC.
- **Shelley Alpern, Director of Corporate Engagement, Rhia Ventures**
    - Shelley brings over two decades experience leading and participating in shareholder advocacy campaigns on a wide range of social and environmental issues, which has resulted in numerous negotiated agreements to advance more progressive corporate policies and practices. She also serves currently as a board member for RMH Compass, an organization that provides tools and data insights to employers to evaluate and benchmark their maternal and reproductive health benefits.

aboboTech CENTER FOR DEMOCRACY & TECHNOLOGY Euki Rhia VENTURES

Resources

- **As You Sow**
  - An organization helping retail and institutional investors vote on their proxies.

- **Open Mic**
  - Nonprofit working with shareholders to develop corporate accountability in digital technology.

- **Center for Democracy and Technology (CDT)**
  - Report: Data after Dobbs: Best Practices for Protecting Reproductive Health Data
  - Consumer Privacy Framework for Health Data and associated paper

- **The Age of Surveillance Capitalism**
  - Book by Shoshana Zuboff

- **Rhia Ventures Health Equity Assessment and Rating Tool (HEART) Framework**
  - A framework to help companies, investors, and organizations develop their policies and practices with an equity lens.