# THE TECH POLICY STACK OF CONSUMER HEALTH

**Discussion Lead: Jordan Wrigley**

## SESSION DESCRIPTION

This roundtable will explore the practical and policy realities of complying with health and sensitive data restrictions. This is an opportunity to examine the technical "how-to" of data segmentation, focusing on current practices, emerging practices, and policies for distinguishing "consumer health data" from broader sensitive categories. The discussion will also tackle high-stakes implementation challenges, including the DOJ's Final Rule on Bulk Sensitive Data. By bridging the gap between policy and technical, this session provides a space to trade emerging thoughts on the practicalities of meeting today's fragmented regulatory standards.

## KEY DISCUSSION QUESTIONS

1. **Operationalizing Broad Definitions:** How are organizations technically executing data segmentation to account for broad definitions of "consumer health data" under non-HIPAA state laws?
2. **DOJ Bulk Sensitive Data Rule:** What compliance workflows and technical safeguards are organizations building to comply with the DOJ's Final Rule on Bulk Sensitive Data, specifically regarding the heavy restrictions on transferring bulk human genomic, biometric, and health data to "countries of concern"?
3. **Pixel Tracking & Algorithmic Surveillance:** Following major FTC enforcement actions against digital health platforms in past years (e.g., GoodRx, BetterHelp, and Premom), how are companies structuring policies and technical safeguards in this new FTC administration? Is a "deregulatory" outlook short-term?
4. **Geofencing Prohibitions:** How are legal and technical teams collaborating to implement the strict bans on geofencing around sensitive/health data locations (mandated by Washington, Nevada, Connecticut, and California) to ensure consumer health data is not collected, tracked, or targeted for advertising without appropriate consent?

## NOTES ON CONTENT

- With the absence of a unified federal standard, state legislatures are aggressively filling the gaps left by HIPAA. States have instituted stringent rules requiring prior opt-in consent for health data collection, separate consents for sharing, and strict 1-year standalone written authorizations for data sales.
- The FTC has relied on the Health Breach Notification Rule (HBNR) and Section 5 of the FTC Act to prosecute digital health apps. The FTC has treated the unauthorized transmission of individually identifiable health data to third-party ad networks (via SDKs or tracking pixels) as a data breach. This seems unlikely to be similar in the current administration but what about the future?
- Effective April 2025, this rule introduces high-stakes implementation challenges by placing outright prohibitions on transferring specific categories of bulk sensitive data to entities affiliated with countries like China, Russia, and Iran. This forces entities to adopt rigorous vendor diligence, auditing practices, and CISA-promulgated cybersecurity standards.
- Plaintiffs are leveraging wiretap laws, such as the California Invasion of Privacy Act (CIPA), to target commercial websites whose marketing SDKs and pixels load and transmit data prior to obtaining explicit user consent, highlighting a critical intersection of technical operations and legal exposure