

California Adopts Privacy Protections for Digital Reproductive and Sexual Health Information

Article By:

Gayland O. Hethcoat II

Moyosore O. Koya

With the recent passage of Assembly Bill (AB) 254 and AB 1697, California's Confidentiality of Medical Information Act (CMIA) will extend privacy protections to reproductive and sexual health information on mobile applications and internet websites.

This expansion of CMIA's scope notably impacts digital health

companies and other entities that offer online reproductive or sexual health services in California. As the privacy regulatory landscape continues to evolve, these entities now must consider CMIA in their privacy compliance programs.

Defining “Reproductive or Sexual Health Application Information”

Considered California’s analogue to the federal Health Insurance Portability and Accountability Act (HIPAA), CMIA imposes restrictions on the use and disclosure of “medical information.” The recently enacted **AB 254** and **AB 1697** amend the law’s definition of “medical information” to include “reproductive or sexual health application information” collected by a “reproductive or sexual health digital service.” The bills define these terms as follows:

- **“Reproductive or sexual health application information”** is defined as “information about a consumer’s reproductive health, menstrual cycle, fertility, pregnancy, pregnancy outcome, plans to conceive, or type of sexual activity collected by a reproductive or sexual health digital service.” The term includes information from which one can infer someone’s pregnancy status, menstrual cycle, fertility, hormone levels, birth control use, sexual activity, or gender identity.
- **“Reproductive or sexual health digital services”** is defined as “a mobile-based application or internet website that collects reproductive or sexual health application information from a consumer, markets itself as facilitating reproductive or sexual health services to a consumer, and uses the information to facilitate reproductive or sexual health services to a consumer.”

Additionally, AB 254 states that any business offering a reproductive or sexual health digital service to allow a consumer to

“manage the individual’s information, or for the diagnosis, treatment, or management of a medical condition,” is considered a “provider of health care.” As such, a reproductive or sexual health digital service provider must comply with the same requirements of clinicians and health care institutions under CMIA and may be liable for penalties for the improper use or disclosure of medical information, including the sale or use of medical information for marketing purposes without an individual’s authorization.

By the same token, clinicians and health care institutions also may be impacted by AB 254 and AB 1697. For example, if a clinic integrates reproductive or sexual health application information into a patient’s electronic medical record, it must protect that information to the same extent as other medical information in the patient’s record. Use or disclosure of the reproductive or sexual health application information in violation of CMIA could result in direct liability for the clinic.

Taking effect on January 1, 2024, AB 254 and AB 1697 will formally codify how the California Attorney General (AG) has already been interpreting and enforcing CMIA. In a **May 26, 2022 press release** stressing “unprecedented threats to reproductive freedom,” the AG opined that CMIA “applies to mobile apps that are designed to store medical information, including some fertility trackers, and establishes privacy protections that go beyond federal law.” Consistent with that interpretation, in 2020 the AG entered into a **settlement with Glow Inc.**, the maker of an ovulation and fertility cycle tracker, in which the company agreed to pay \$250,000 in penalties, implement an information security program, and take other actions to remediate features of the app that allegedly compromised users’ information in violation of CMIA.

California Bills Echo Federal Commitment to Reproductive Health Privacy

In addition to aligning with the California AG's CMIA enforcement posture, AB 254 and AB 1697 parallel efforts by the federal government to safeguard reproductive health information privacy. Shortly after the US Supreme Court's 2022 landmark ruling in *Dobbs v. Jackson Women's Health Organization*, the US Department of Health and Human Services (HHS) Office for Civil Rights (OCR), which enforces HIPAA's privacy and security protections, **published guidance** noting that HIPAA's restrictions on the use and disclosure of "protected health information" apply to "information relating to abortion and other sexual and reproductive health care." In **separate post-Dobbs guidance**, OCR also advised on how individuals can protect the privacy and security of health information on cell phones, tablets, and associated apps. Yet, because HIPAA applies only to "covered entities," including health care providers and health plans, and their "business associates," OCR cautioned that HIPAA generally does "not protect the privacy of data you've downloaded or entered into mobile apps for your personal use, regardless of where the information came from."

Meanwhile, the Federal Trade Commission (FTC) has enforced Section 5 of the FTC Act and the Health Breach Notification Rule against businesses falling outside the scope of HIPAA that do not adequately protect their users' app-based reproductive and sexual health information. For example, the agency recently **settled a complaint against Easy Healthcare Corporation**, the developer of the fertility tracking app Premom, that alleged the company shared sensitive health information about users with third-party firms in violation of its privacy policies and without adequate encryption. Similar to the California AG's settlement with Glow, the FTC's settlement requires the app developer to obtain affirmative consent before sharing a user's personal health information and to maintain a comprehensive information security program, among

other corrective actions.

Key Takeaways

California's legislative action exemplifies a trend among states to protect digital reproductive and sexual health information. As we discussed in a **prior alert**, other states, including Nevada and Washington, have recently passed legislation to safeguard reproductive and sexual health information, as well as other broadly defined "consumer health data." These laws are a testament to the proliferation of digital health technologies among consumers, including apps to track menstrual cycles, monitor fertility, and manage contraception, which typically fall outside of OCR's oversight under HIPAA. Developers of these apps and other businesses that process reproductive and sexual health information should evaluate if and how CMIA and other state consumer health data privacy laws apply to them. Stakeholders should also consider the interplay between state privacy laws and federal laws that may protect reproductive and sexual health information, including HIPAA and the FTC Act.