Potentially Applicable Laws and Recommended Steps: MoodNote

Not legal advice. This report is general information, not legal advice, and it should not be relied on or treated as legal advice. It lists laws and rules that may potentially apply to the app, based on the answers given and any code reviewed. It does not state that any law does or does not apply, and it does not determine whether the app complies with any law. Using it does not create a lawyer-client relationship. Laws change, and how they apply depends on facts this report may not capture. Consult a qualified attorney before making legal decisions.

Facts marked *declared* were supplied by the app owner and were not independently verified. Code offered as a control is a starting point, not warranted. Test it in your own environment before relying on it.

Application	MoodNote
Description	Journaling and mood-tracking web app built with Lovable on Supabase. Users log daily mood and notes, can sync sleep data from Fitbit, tag entries with where they were for a 'mood map', and chat with 'Mo', an AI companion that remembers past conversations. About 800 registered users, no revenue yet.
Platform	supabase
Assessment date (as of)	2026-11-03
Scope	Consumer health and wellness apps, and apps built for health care providers, with US users, including their AI features
Rule library version	`d48c083bf67e` (git commit)
Prepared with	RuleAlign 0.1.0
Repository reviewed	none
Inputs fingerprint	`sha256:23a83e1c883c7e3ab68dbf7445d64da7 26cfffbd83666e77cd3266d0a59ae431`

At a glance

- **May apply:** FTC Health Breach Notification Rule, Washington My Health My Data Act, New York health-data protections (geofencing ban, abortion-referral reports, shield laws, police access)
- **Need more information:** Nevada consumer health data law (SB 370), Connecticut Data Privacy Act (including its health-data and minors' rules), California Confidentiality of Medical Information Act (CMIA), including the Genetic Information Privacy Act, Children's Online Privacy Protection Act (COPPA) and COPPA Rule
- **Considered, unlikely to apply:** HIPAA (covered entities and business associates), California Consumer Privacy Act (as amended by the CPRA)
- **Recommended steps:** 25, of which **1 to do first**

- **Technical controls recommended:** 8 (5 with code provided, 3 specification only); **3 cannot be added later**
- **Not included in this report:** 1 law still being added to RuleAlign (listed under "What was NOT assessed")
- **Questions to take to a lawyer:** 1 (see the section of that name)
- **If this happens:** what to do in 6 situations (see the section of that name)

1. Recommended steps

Recommendations to help the app align with the laws that may apply (section 2). They are not legal advice. Work through them in order.

Do first

Find out what each tag receives. Remove tags from screens and events that reveal health information, conditions or treatment, or get valid authorizations first.

- Tracking tags may be disclosing medical information (not ruled out).
- Relates to: California Confidentiality of Medical Information Act (CMIA), including the Genetic Information Privacy Act (`cmia-tracking-tags`)

Answer these open questions

"Which US states do your users live in, or which states do you market to or do business in?"

- Your answer decides whether the laws or obligations below may apply.
- Relates to: Nevada consumer health data law (SB 370); Connecticut Data Privacy Act (including its health-data and minors' rules)

"Do you know that any specific user is under 18?"

- Your answer decides whether the laws or obligations below may apply.
- Relates to: Connecticut Data Privacy Act (including its health-data and minors' rules)

"Is the app designed to keep users' health information so they can manage it, or to help diagnose, treat or manage a physical or mental health condition, or does it market itself as providing or supporting mental health, reproductive or sexual health, or other health services?"

- Your answer decides whether the laws or obligations below may apply.
- Relates to: California Confidentiality of Medical Information Act (CMIA), including the Genetic Information Privacy Act

"Will any of the app's users be under 13?"

- Your answer decides whether the laws or obligations below may apply.
- Relates to: Children's Online Privacy Protection Act (COPPA) and COPPA Rule

Get legal advice on these

Get legal advice: whether sending entries to your AI provider is an "unauthorized disclosure".

- The question to ask, and what to bring, are under "Questions to take to a lawyer".
- Relates to: FTC Health Breach Notification Rule (`hbnr-ai-provider-disclosure`)

Start now: these cannot be added later

Record each user's consent separately for each purpose (collecting health data, sharing it, sending it to an AI provider), with the exact policy version and time, in an append-only log.

- Code provided: `controls/consent-capture-versioned/supabase.sql` (tested on PostgreSQL). How to check it: Appendix C.

- Relates to: FTC Health Breach Notification Rule (`hbnr-authorized-disclosure`); Washington My Health My Data Act (`mhmda-new-purposes-need-consent`, `mhmda-consent-to-collect`, `mhmda-consent-to-share`, `mhmda-withdraw-consent`)

List every outside service that receives user data, and stop health-related data reaching any of them unless the user has agreed to that recipient and purpose.

- No code yet: Appendix C says what to build and how to check it.
- Relates to: FTC Health Breach Notification Rule (`hbnr-authorized-disclosure`); Washington My Health My Data Act (`mhmda-consent-to-share`)

Log who reads, changes or exports health data, without copying the data itself into the log, somewhere app users cannot alter.

- No code yet: Appendix C says what to build and how to check it.
- Relates to: FTC Health Breach Notification Rule (`hbnr-breach-discovery`); Washington My Health My Data Act (`mhmda-data-security`)

Then: changes in the app

Add a setting where each user can choose email as their primary contact method, store the choice with its date, and ask users who don't choose email for a postal address.

- No code yet: Appendix C says what to build and how to check it.
- Relates to: FTC Health Breach Notification Rule (`hbnr-contact-preference`)

Set up one place to log access, deletion, correction and consent-withdrawal requests, with deadlines taken from the laws that may apply.

- Code provided: `controls/data-subject-request-intake/supabase.sql` (tested on PostgreSQL). How to check it: Appendix C.
- Relates to: Washington My Health My Data Act (`mhmda-right-to-access`, `mhmda-withdraw-consent`, `mhmda-right-to-delete`, `mhmda-request-handling`)

Make account deletion remove every row the user owns, and their uploaded files, automatically.

- Code provided: `controls/deletion-cascade/supabase.sql` (tested on PostgreSQL). How to check it: Appendix C.
- Relates to: Washington My Health My Data Act (`mhmda-right-to-delete`)

Turn on row-level security for every table the app exposes, so each user can read and change only their own rows.

- Code provided: `controls/row-level-access-control/supabase.sql` (tested on PostgreSQL). How to check it: Appendix C.
- Relates to: Washington My Health My Data Act (`mhmda-restrict-access`, `mhmda-data-security`)

Keep health data in its own owner-only table, and remove any view or function that exposes it to other users.

- Code provided: `controls/sensitive-data-segregation/supabase.sql` (tested on PostgreSQL). How to check it: Appendix C.
- Relates to: Washington My Health My Data Act (`mhmda-restrict-access`, `mhmda-data-security`)

Do not set up a geofence within 2,000 feet of an in-person health care facility to identify or track people seeking care, collect health data, or send them health-related notifications or ads.

- No control for this in the library yet. It needs a safeguard designed for your app.
- Relates to: Washington My Health My Data Act (`mhmda-no-geofencing`)

Don't set up a geofence or similar virtual boundary (a radius of 1,850 feet or less, drawn with GPS, cell, Wi-Fi, IP address or any other location data) around any health care facility other than your own, to send digital ads, build consumer profiles, or infer anyone's health status, condition or treatment; and don't deliver digital ads to people at or inside such a facility through a geofence. 'Health care facility' covers any provider of medical care or related services, including licensed mental health and addiction programs.

- No control for this in the library yet. It needs a safeguard designed for your app.

- Relates to: New York health-data protections (geofencing ban, abortion-referral reports, shield laws, police access) (`ny-no-geofencing`)

Encrypt stored health data, including backups and exports, in line with NIST SP 800-111 as HHS's guidance specifies, and keep the encryption keys separate from the data.

- Recommended, not a duty under this law. This rule's duties cover only "unsecured" health information. Data encrypted as HHS's guidance specifies, with the keys kept on a device or at a location separate from the data and not themselves breached, is not unsecured, so losing it is not a breach you must report under this rule. It does not help when readable data is sent to someone else, such as through an ad tag, or when an attacker gets in through the app itself, because the app decrypts the data for them.
- Relates to: FTC Health Breach Notification Rule (`hbnr-encryption-safe-harbor`)

Add a place in the app to receive each user's age group (under 13, 13-15, 16-17, 18 and over) from the app store, operating system or age-verification service, with its source and date, and act on it: switch on parental consent and children's protections for users under 13, and age-appropriate settings for other minors. For Texas users, delete the app store's age data once the check is done and keep only the resulting protection settings. If you ask users their age yourself, ask neutrally: don't pre-fill or default to an age, and don't hint at the answer that unlocks the app.

- Recommended, not a duty under this law. App stores, phone operating systems and age-verification services can now tell an app a user's age group. An app that receives that result knows when a user is under 13, which brings COPPA in for that user. Texas already requires apps offered there through an app store to use the store's age information and to delete it once the check is done (Tex. Bus. & Com. Code 121.054-121.055), and from 1 January 2027 California requires apps to request an age signal from the device's operating system or app store (Cal. Civ. Code 1798.501). The COPPA Rule requires a service aimed partly at children to ask ages neutrally, without defaulting to an age or encouraging false answers (16 CFR 312.2, mixed audience).
- Relates to: Children's Online Privacy Protection Act (COPPA) and COPPA Rule (`coppa-age-check-intake`)

Check what each analytics or session-recording tool receives, and strip health information from event names, page URLs and recordings, or get users' authorization first.

- Analytics or session-recording tools may receive health data.
- Relates to: FTC Health Breach Notification Rule (`hbnr-analytics-disclosure`)

Review your AI provider's data-use, retention and training terms; choose settings that bar training and limit retention where available, and tell users their entries are sent to it.

- User content is sent to an outside AI provider.
- Relates to: FTC Health Breach Notification Rule (`hbnr-ai-provider-disclosure`)

Outside the code: documents, processes and contracts

Prepare your breach response before you need it *(6 parts)*

- After discovering a breach of security, notify each affected individual who is a US citizen or resident without unreasonable delay and within 60 calendar days. A law-enforcement official can require a delay. You don't have to wait until you know everything: the rule lets you send the notice in more than one mailing as information becomes available.
- Notify the FTC, using the instructions on its website. If 500 or more people are affected, do it at the same time as notifying individuals. If fewer are affected, you may instead keep a log of such breaches and send the year's log to the FTC within 60 calendar days after the end of the calendar year.
- If the information of 500 or more residents of one state or jurisdiction is, or is reasonably believed to have been, acquired, notify prominent media outlets serving it, without unreasonable delay and within 60 calendar days after discovery.
- Prepare breach notice content in plain language that covers what the rule lists: what happened, with the date of the breach and of its discovery; who acquired the information, if known (for example the advertising platform); the types of information involved, which can include the fact that someone used a health app; steps individuals should take; what you are doing to investigate, limit harm and protect them; and at least two ways to contact you (toll-free number,

email, website, in-app or postal address). Drafting it for the first time during an incident makes omissions likely.

- Plan how a breach notice would reach every affected user. Notice by email must be clear and conspicuous and go with a text message, in-app message or banner. If contact details are missing or out of date for 10 or more people, post a substitute notice on your home page for 90 days or in major print or broadcast media, with a toll-free number that stays active for 90 days. If a user has died, notice goes to the next of kin they named and authorized you to contact. In urgent cases you may also phone people.
- Keep records showing that every notice you send under this rule (to individuals, the FTC and the media, or, as a service provider, to the business you serve) went out on time and by the required method, and the evidence for any delay, such as a law-enforcement request. The burden of proof is on you.
- Relates to: FTC Health Breach Notification Rule (`hbnr-notify-individuals`, `hbnr-notify-ftc`, `hbnr-notify-media`, `hbnr-notice-content`, `hbnr-notice-method`, `hbnr-notification-records`)

Put the required contracts in place with every vendor that handles the data *(2 parts)*

- Tell each service provider that handles the health data for you (hosting, analytics, advertising, AI, support tools) that your app may be a vendor of personal health records or a PHR related entity under this rule, As good practice, also name in your contract the person who should receive their breach notices; otherwise they go to a senior official. The rule requires vendors to tell service providers their status, and requires service providers to report a breach to the vendor within 60 calendar days, identify the affected customers and get the vendor's acknowledgment.
- Let processors (hosting, AI, analytics vendors acting for you) handle consumer health data only under a binding contract that sets processing instructions and limits what they may do, and only in ways consistent with your privacy policy.
- Relates to: FTC Health Breach Notification Rule (`hbnr-service-provider-terms`); Washington My Health My Data Act (`mhmda-processor-contracts`)

Publish a consumer health data privacy policy, prominently linked from your homepage, stating the categories of health data collected and why, the sources, the categories shared, who receives them, and how users exercise their rights. *(document)*

- Relates to: Washington My Health My Data Act (`mhmda-privacy-policy`)

Run an appeal process for refused requests. Respond in writing with reasons, and if the appeal is denied, give the user a way to contact the Washington Attorney General. *(process)*

- Relates to: Washington My Health My Data Act (`mhmda-appeals`)

Don't treat people worse because they used any right under the Act, for example by cutting features or refusing service after they ask to see, delete or withdraw their data. *(process)*

- Relates to: Washington My Health My Data Act (`mhmda-no-discrimination`)

2. Laws and rules that may apply

Based on the answers given and the code reviewed, each of these may apply. This is not a statement that it does apply. Full detail for each (all duties, notes, sources and the parts of the law not covered) is in Appendix B.

FTC Health Breach Notification Rule

16 CFR Part 318 (as amended, effective 29 July 2024; 89 FR 47028); 42 U.S.C. 17937 · Private right of action: no · Confidence: medium

Why it may apply

- **No**: The operator is a HIPAA covered entity, so its health data is protected health information under HIPAA *(declared)*
- **Yes**: The app holds identifiable information about users' physical or mental health (the rule treats apps that track mood, sleep, symptoms, fitness, diet, fertility and similar as health care services) *(declared)*
- **Yes**: People use the app for themselves, so the health record is managed primarily for the individual *(declared)*

- **Yes**: The app has the technical capacity to draw information from more than one source (for example user entries plus a wearable, a health platform, the phone's calendar or another API) *(declared)*
- **Yes**: The app collects location from the device, which the FTC treats as a second source of information (2024 rule, 89 FR 47036, Example 3) *(declared)*

Duties that fit your app: 10, built into the recommended steps above. 1 other duty does not fit your answers.

Washington My Health My Data Act

RCW 19.373 · Private right of action: yes · Confidence: high

Why it may apply

- **Yes**: The app collects data that identifies a person's past, present or future physical or mental health status (defined broadly, including wellness data and health status inferred from other data) *(declared)*
- **No**: HIPAA applies, so the app's health data is protected health information, which this Act exempts *(assessed: unlikely to apply)*
- **Yes**: People use the app for themselves, rather than a clinic, employer or insurer running it for them *(declared)*
- **No**: The operator is a HIPAA covered entity, so all its health data is protected health information *(declared)*
- **Yes**: The app has users in Washington, or markets to Washington consumers *(declared: CA, IL, NY, OH, TX, WA (list may be incomplete))*

Duties that fit your app: 14, built into the recommended steps above. 3 other duties do not fit your answers.

New York health-data protections (geofencing ban, abortion-referral reports, shield laws, police access)

N.Y. Gen. Bus. Law 394-e to 394-i · Private right of action: yes · Confidence: medium

Why it may apply

- **Yes**: The app collects precise location *(declared)*
- **Yes**: The app has users in New York, or does business there *(declared: CA, IL, NY, OH, TX, WA (list may be incomplete))*

Duties that fit your app: 1, built into the recommended steps above. 1 other duty does not fit your answers.

3. Laws and rules that need more information

These could not be assessed either way. Answering the open questions in the recommended steps decides them.

Nevada consumer health data law (SB 370)

NRS 603A.400 to 603A.550 (added by SB 370, 2023) · Private right of action: no · Confidence: medium

- **Unknown**: The app has users in Nevada, or markets to Nevada consumers *(declared: CA, IL, NY, OH, TX, WA (list may be incomplete))*

If it does apply, it brings 17 principal duties (Appendix B).

Connecticut Data Privacy Act (including its health-data and minors' rules)

Conn. Gen. Stat. 42-515 to 42-526 and 42-529 to 42-529e, as amended by P.A. 23-56 and P.A. 25-113 · Private right of action: no · Confidence: medium

- **Unknown**: The app has users in Connecticut, or targets Connecticut residents *(declared: CA, IL, NY, OH, TX, WA (list may be incomplete))*
- **Unknown**: The operator knows that specific users are under 18 *(answered unknown)*

If it does apply, it brings 35 principal duties (Appendix B).

California Confidentiality of Medical Information Act (CMIA), including the Genetic Information Privacy Act

Cal. Civ. Code 56-56.37 · Private right of action: yes · Confidence: medium

- **Unknown**: The app is designed to help people manage their health information or a health condition, or markets itself as offering health services *(answered unknown)*

If it does apply, it brings 18 principal duties (Appendix B).

Children's Online Privacy Protection Act (COPPA) and COPPA Rule

15 U.S.C. 6501-6506; 16 CFR Part 312 (as amended 2025) · Private right of action: no · Confidence: high

- **Unknown**: Some of the app's users are under 13 *(answered unknown)*

If it does apply, it brings 9 principal duties (Appendix B).

4. Laws and rules considered and unlikely to apply

Each was considered and, on the facts shown, is unlikely to apply, for the reasons listed. If a fact is wrong, the result may change. Full detail: Appendix B.

- **HIPAA (covered entities and business associates)**: **No**: The organization offering the app is a HIPAA covered entity (a health plan, a health care clearinghouse, or a health care provider that conducts standard electronic transactions such as insurance billing); **No**: The app creates, receives, keeps or transmits health information on behalf of a HIPAA covered entity, directly or as a subcontractor of one of its vendors (a business associate role)
- **California Consumer Privacy Act (as amended by the CPRA)**: **No**: Annual gross revenue last year was more than $26,625,000 (the threshold as adjusted from 1 January 2025); **No**: The operator sells personal information; **No**: The app or its site uses advertising tags, which the CCPA treats as sharing for cross-context behavioural advertising; **No**: The personal information of 100,000 or more California consumers or households is handled each year; **No**: 50% or more of annual revenue comes from selling or sharing personal information; **No**: The company handles health or wellness data for another business's app or service, as its vendor; **No**: The app handles patients' data for a HIPAA covered entity; **No**: The operator is a HIPAA covered entity

5. Questions to take to a lawyer

RuleAlign can't settle these: the answer depends on how a lawyer reads the law against your facts. Bring this list, and what each item asks you to bring, to keep the consultation short.

1. Whether sending entries to your AI provider is an "unauthorized disclosure" (FTC Health Breach Notification Rule)

- **What this is about:** Under the FTC rule, sharing identifiable health information without the user's authorization counts as a breach. A provider that processes data only to deliver your feature, under contract, may be treated differently from one that keeps it or uses it for its own purposes, such as training models.
- **Ask:** Is sending users' entries to our AI provider an unauthorized disclosure under the FTC Health Breach Notification Rule, given the provider's terms, and what should we tell users?
- **Bring:** your AI provider's data-use, retention and training terms; what you send: whole entries or parts; what your privacy policy and consent screens say about it
- **Why it matters:** If it is unauthorized, it can be a reportable breach, with notice duties to users and the FTC.

6. If this happens

Situations that can't be assessed in advance. If one happens, do this, and contact a lawyer.

If police or another law enforcement official asks you to delay a breach notice (FTC Health Breach Notification Rule)

- Ask for the request in writing, stating how long the delay should be; then delay for that period.
- If the request is only spoken, write down what was said and who said it; you may then delay for no more than 30 days unless a written request follows.
- Keep the request with your breach records: you must be able to show why notices were delayed (16 CFR 318.4(c)).
- Contact a lawyer, and keep preparing the notices so they're ready when the delay ends.
- *16 CFR 318.4(d)*

If you buy a company, or its assets, that holds Nevada consumer health data (Nevada consumer health data law (SB 370))

- You take on all of that company's duties under Nevada's consumer health data law for that data.
- Before using the data, find out what consents, sale authorizations and open requests come with it, and keep to them.
- Contact a lawyer before the deal completes.
- *NRS 603A.490(2)*

If Connecticut's Attorney General contacts you about your data practices (Connecticut Data Privacy Act (including its health-data and minors' rules))

- Contact a lawyer before answering in substance.
- The Attorney General may ask for your data protection or impact assessments, and for any plan to reduce risks to minors; a requested minors' plan is due within 90 days of the notice.
- The Attorney General may, but no longer has to, give you a chance to fix a violation before acting. Ask whether one is available.
- Keep every relevant record, and don't delete or change anything.
- *Conn. Gen. Stat. 42-522(d); Conn. Gen. Stat. 42-525; Conn. Gen. Stat. 42-529b(f); Conn. Gen. Stat. 42-529e*

If New York police ask for, or offer to buy, users' health data without a warrant (New York health-data protections (geofencing ban, abortion-referral reports, shield laws, police access))

- New York law bars police from buying or obtaining health data, including inferences about health and location near a health facility, without a warrant.
- Ask for the warrant, and don't sell or hand over health data without one.
- Contact a lawyer before responding.
- *N.Y. Gen. Bus. Law 394-h*

If someone from another state, or federal law enforcement, asks for information about abortion or gender-affirming care (California Confidentiality of Medical Information Act (CMIA), including the Genetic Information Privacy Act)

- Contact a lawyer before answering.
- Don't release medical information about someone seeking or obtaining an abortion, or gender-affirming health or mental health care, in response to a subpoena or request based on another state's law that interferes with these rights, or on a foreign penal civil action.
- Don't release it to law enforcement enforcing such laws, and don't cooperate with an inquiry from another state, or from federal law enforcement as far as federal law allows, that would identify the person, unless California law allows the request.
- A subpoena from another state needs a California court order before you act on it.
- You may still cooperate with investigations of activity that is a crime under California law.
- *Cal. Civ. Code 56.10(b)(1)(B); Cal. Civ. Code 56.108; Cal. Civ. Code 56.109*

If medical information is released without authorization (California Confidentiality of Medical Information Act (CMIA), including the Genetic Information Privacy Act)

- Contact a lawyer at once.
- Each person whose information was negligently released can sue for $1,000 without proving harm, plus actual damages; regulators can fine up to $2,500 per negligent violation, $25,000 per knowing violation and $250,000 where it was for financial gain.
- A HIPAA covered entity or business associate may have a defence if, among other things, it notified everyone entitled to notice, the release went only to another covered entity or business associate, it had security policies, a security official and encryption, and it acted promptly to recover the data and prevent a repeat.
- Check the state breach-notification laws, which this report doesn't assess.
- Keep every relevant record, and don't delete or change anything.
- *Cal. Civ. Code 56.35; Cal. Civ. Code 56.36*

7. What was NOT assessed

This report says nothing about any of the following. Each may impose obligations on this app.

- **Laws still being added to RuleAlign, not included in this report:** California companion chatbot laws (SB 243 and Adam's Law). It may apply to this app.
- Other US state comprehensive privacy laws (for example Colorado, Virginia, Texas, Oregon, Maryland and others). Several treat health data as sensitive and require opt-in consent.
- Parts of California's Confidentiality of Medical Information Act (CMIA) that cover other kinds of organization: employers handling their own staff's medical information, health care service plans, insurers, pharmaceutical companies, companies administering payment for health care, cannabis businesses, and hospitals answering inquiries about patients; and patients' right to see and copy records held by licensed providers (California's Patient Access to Health Records Act, Health and Safety Code 123100 and following).
- California laws taking effect on 1 January 2027: the rewritten Age-Appropriate Design Code for online services likely to be used by children (Cal. Civ. Code 1798.99.28 and following), limits on addictive features for users under 16 (Cal. Bus. & Prof. Code 22682 and following), and the ban on apps undoing users' privacy settings (Cal. Bus. & Prof. Code 22710 and following).
- Privacy duties for your employees', job applicants' and business contacts' data, which California's CCPA also covers.
- State data breach notification laws (all 50 states, DC and territories).
- State laws on AI in mental health care: Illinois (Wellness and Oversight for Psychological Resources Act), Nevada (AB 406), Utah (HB 452), and New York's AI companion law.

- State app store accountability acts (Texas SB 2420, currently enforceable while a court challenge continues; Utah; Louisiana; California AB 1043), including any age-signal duties on developers.
- Section 5 of the FTC Act (unfair or deceptive practices), including whether your privacy policy and marketing claims match what the app actually does.
- HIPAA obligations beyond the principal ones listed (the Security Rule alone has about 50 implementation specifications), the substance-use records rule (42 CFR Part 2), and state medical-records laws that reach health care providers.
- Federal information-blocking rules (45 CFR Part 171), which apply to health care providers, developers of certified health IT, and health information networks.
- FDA regulation of software as a medical device (for example apps that diagnose, treat or recommend treatment).
- Telehealth, professional licensing, and rules on who may provide therapy or medical advice.
- Any non-US law, including EU and UK GDPR.
- Accessibility (ADA, WCAG).
- App store platform policies (Apple and Google rules on health data, AI and children).
- Security beyond the listed controls. No penetration test or vulnerability scan was performed.
- Your contracts: vendor terms (including your AI provider's data-use, retention and training terms), data processing agreements, and business associate agreements.
- The wording of your privacy policy, consent screens and notices.
- Whether any control is actually deployed in your production environment. Repository reading shows what is in code; it does not test a running system.

Appendix A. What was assessed

Scope: Direct-to-consumer apps that collect health or wellness information (mood, journaling, sleep, fitness, diet, cycle tracking, meditation, symptoms), and apps built for hospitals, clinics and health plans (patient portals, telehealth, remote monitoring), used by people in the United States, including any AI features they offer.

Laws and rules considered: HIPAA (covered entities and business associates) (`us-hipaa`); FTC Health Breach Notification Rule (`us-ftc-hbnr`); Washington My Health My Data Act (`us-wa-mhmda`); Nevada consumer health data law (SB 370) (`us-nv-chd`); Connecticut Data Privacy Act (including its health-data and minors' rules) (`us-ct-ctdpa`); New York health-data protections (geofencing ban, abortion-referral reports, shield laws, police access) (`us-ny-geofencing`); California Consumer Privacy Act (as amended by the CPRA) (`us-ca-ccpa`); California Confidentiality of Medical Information Act (CMIA), including the Genetic Information Privacy Act (`us-ca-cmia`); Children's Online Privacy Protection Act (COPPA) and COPPA Rule (`us-coppa`).

A.1 Facts used

Fact	Answer	Source	Evidence in code
Stores health or wellness data	yes	declared	-
Handles reproductive, sexual health or gender-affirming care information	no	declared	-
Helps manage health, or offers health services	unknown	answered unknown	-

Fact	Answer	Source	Evidence in code
Can pull data from more than one source	yes	declared	-
Sends health data into, or is offered through, another health app	no	declared	-
Collects precise location	yes	declared	-
US states with users	CA, IL, NY, OH, TX, WA (list may be incomplete)	declared	-
People use it for themselves	yes	declared	-
Is mainly a place for users to socialise	no	declared	-
Offers genetic testing or analyses users' DNA data	no	declared	-
Some users are under 13	unknown	answered unknown	-
Knows specific users are under 18	unknown	answered unknown	-
Knows specific users are under 16	unknown	answered unknown	-
Sends data to advertising platforms	no	declared	-
Sends data to analytics or session-recording tools	unknown	answered unknown	-
Sends user content to an outside AI provider	yes	declared	-
Shares health data with other organisations	no	declared	-
Sells user data	no	declared	-
Has an AI chat feature	yes	declared	-
AI acts as a companion	yes	declared	-
Lets users under 18 use the AI chat	unknown	answered unknown	-
Makes automated decisions about health care or other significant matters	no	declared	-

Fact	Answer	Source	Evidence in code
States where the company is located, headquartered or incorporated	OH (complete list)	declared	-
For-profit operator	yes	declared	-
Annual gross revenue (USD)	0	declared	-
California residents whose data you handle per year	1,200. Note: About 250 registered California users plus roughly 950 California visitors a year to the marketing site	declared	-
% of revenue from selling or sharing data	0	declared	-
Is a HIPAA covered entity	no	declared	-
Holds a California-licensed provider's patient data	no	declared	-
Handles data for a HIPAA covered entity (directly or as a subcontractor)	no	declared	-
Handles health data for other businesses, as their vendor	no	declared	-
Uses patient data beyond the service	not asked	not asked: not relevant to this app	-
Gets requests for patient data from authorities or researchers	not asked	not asked: not relevant to this app	-
Family or caregivers can see patient information	not asked	not asked: not relevant to this app	-

A.2 Where your answers and your code disagree

No repository was provided, so no answer was checked against code.

Appendix B. Laws and rules in full

B.1 May apply

FTC Health Breach Notification Rule (`us-ftc-hbnr`)

Citation: 16 CFR Part 318 (as amended, effective 29 July 2024; 89 FR 47028); 42 U.S.C. 17937 · **Jurisdiction:** US-federal · **Size threshold:** none · **Private right of action:** no · **Confidence:** medium · **Legal status:** in force, effective 2009-09-24 (checked 2026-10-19)

Requires vendors of personal health records that are not covered by HIPAA, which now explicitly includes health and wellness apps, and companies whose apps connect with them (PHR related entities), to notify users, the FTC and sometimes the media after a breach of security. Service providers that handle the data must tell the business they serve. Under the 2024 amendments, a 'breach' includes an unauthorized disclosure, such as sending health information to an advertising platform, and not only a hack.

Why it may apply

- **No**: The operator is a HIPAA covered entity, so its health data is protected health information under HIPAA *(declared)*
- **Yes**: The app holds identifiable information about users' physical or mental health (the rule treats apps that track mood, sleep, symptoms, fitness, diet, fertility and similar as health care services) *(declared)*
- **Yes**: People use the app for themselves, so the health record is managed primarily for the individual *(declared)*
- **Yes**: The app has the technical capacity to draw information from more than one source (for example user entries plus a wearable, a health platform, the phone's calendar or another API) *(declared)*
- **Yes**: The app collects location from the device, which the FTC treats as a second source of information (2024 rule, 89 FR 47036, Example 3) *(declared)*

Findings that need attention

- **[MEDIUM] Analytics or session-recording tools may receive health data** (not ruled out). Third-party analytics and session-recording tools receive event names, page URLs and sometimes recordings of what users type. If any of that reveals health information, the same unauthorized-disclosure analysis applies. Check what each tool actually receives.
- **[MEDIUM] User content is sent to an outside AI provider** (identified). Whether this counts as an unauthorized disclosure depends on the provider's role and terms. A provider that processes data only to deliver your feature, under contract, may be analysed differently from one that retains it or uses it for its own purposes such as model training. Review the provider's data-use, retention and training terms, and tell users about the flow.

Its principal obligations, and how they are addressed

- `hbnr-authorized-disclosure` (technical) Share identifiable health information with other companies (advertising, analytics, data partners) only with the user's authorization. The rule does not forbid sharing, but sharing without authorization is itself a 'breach of security' that triggers every notice below. The FTC reads authorization as sharing consistent with what you told users and what they would reasonably expect, with a meaningful choice for anything beyond that; disclosures buried in a privacy policy don't count. *16 CFR 318.2 (definition of 'breach of security'); 89 FR 47029, 47041 (2024 rule, citing 74 FR 42967)* → Versioned consent capture (`consent-capture-versioned`), Third-party disclosure inventory and gate (`third-party-disclosure-gate`)
- `hbnr-breach-discovery` (technical) Be able to detect and scope breaches. A breach counts as discovered on the first day anyone in the organization (other than the person committing it) knows of it, or reasonably should have known, so the notification clock can start before you notice. Unauthorized access is presumed to be acquisition unless you have reliable evidence that the data was not, or could not reasonably have been, acquired: access logs are that evidence. *16 CFR 318.3(c); 318.2 (definition of 'breach of security')* → Access and change audit log (`audit-logging`)
- `hbnr-notify-individuals` (process) After discovering a breach of security, notify each affected individual who is a US citizen or resident without unreasonable delay and within 60 calendar days. A law-enforcement official can require a delay. You don't have to wait until you know everything: the rule lets you send the notice in more than one mailing as information becomes available. *16 CFR 318.3(a)(1), 318.4(a), 318.4(d), 318.5(a)(1)*
- `hbnr-notify-ftc` (process) Notify the FTC, using the instructions on its website. If 500 or more people are affected, do it at the same time as notifying individuals. If fewer are affected, you may instead keep a log of such breaches and send the year's log to the FTC within 60 calendar days after the end of the calendar year. *16 CFR 318.3(a)(2), 318.4(b), 318.5(c)*

- `hbnr-notify-media` (process) If the information of 500 or more residents of one state or jurisdiction is, or is reasonably believed to have been, acquired, notify prominent media outlets serving it, without unreasonable delay and within 60 calendar days after discovery. *16 CFR 318.3(a)(3), 318.4(a), 318.5(b)*
- `hbnr-notice-content` (document) Prepare breach notice content in plain language that covers what the rule lists: what happened, with the date of the breach and of its discovery; who acquired the information, if known (for example the advertising platform); the types of information involved, which can include the fact that someone used a health app; steps individuals should take; what you are doing to investigate, limit harm and protect them; and at least two ways to contact you (toll-free number, email, website, in-app or postal address). Drafting it for the first time during an incident makes omissions likely. *16 CFR 318.6*
- `hbnr-contact-preference` (technical) Let users choose email as their primary way to hear from you, and record that choice (as good practice, with its date, so you can show who chose email). Breach notices may go by email only to users who chose it; everyone else must get first-class mail at their last known address, which many apps never collect. *16 CFR 318.5(a)(1)* → Contact-preference record for breach notices (`contact-preference-record`)
- `hbnr-notice-method` (process) Plan how a breach notice would reach every affected user. Notice by email must be clear and conspicuous and go with a text message, in-app message or banner. If contact details are missing or out of date for 10 or more people, post a substitute notice on your home page for 90 days or in major print or broadcast media, with a toll-free number that stays active for 90 days. If a user has died, notice goes to the next of kin they named and authorized you to contact. In urgent cases you may also phone people. *16 CFR 318.5(a); 318.2 (definitions of 'electronic mail' and 'clear and conspicuous')*
- `hbnr-notification-records` (document) Keep records showing that every notice you send under this rule (to individuals, the FTC and the media, or, as a service provider, to the business you serve) went out on time and by the required method, and the evidence for any delay, such as a law-enforcement request. The burden of proof is on you. *16 CFR 318.4(c), 318.4(d)*
- `hbnr-service-provider-terms` (vendor/contract) Tell each service provider that handles the health data for you (hosting, analytics, advertising, AI, support tools) that your app may be a vendor of personal health records or a PHR related entity under this rule, As good practice, also name in your contract the person who should receive their breach notices; otherwise they go to a senior official. The rule requires vendors to tell service providers their status, and requires service providers to report a breach to the vendor within 60 calendar days, identify the affected customers and get the vendor's acknowledgment. *16 CFR 318.3(b), 318.4(a)*
- `hbnr-service-provider-notice` (process) If a business whose health data you handle is covered by this rule (as a vendor of personal health records or a PHR related entity), then after discovering a breach of that data, notify the official your contract names, or otherwise a senior official, at that business without unreasonable delay and within 60 calendar days. Identify each affected customer, and get the official's acknowledgment that the notice was received. Covered businesses must tell their service providers that they are covered, so ask each business you serve and keep its answer. *16 CFR 318.3(b), 318.4(a)* **Not triggered: No**: The company handles health or wellness data for another business's app or service, as its vendor *(declared)*

Recommended, not duties under this law

- `hbnr-encryption-safe-harbor` **Encrypt stored health data to HHS's standard.** This rule's duties cover only "unsecured" health information. Data encrypted as HHS's guidance specifies, with the keys kept on a device or at a location separate from the data and not themselves breached, is not unsecured, so losing it is not a breach you must report under this rule. It does not help when readable data is sent to someone else, such as through an ad tag, or when an attacker gets in through the app itself, because the app decrypts the data for them. *16 CFR 318.2 (definition of 'unsecured'); HHS guidance, 74 FR 42740 (24 Aug 2009)*

Parts of this law handled outside the obligations above

- 16 CFR 318.4(d) (Law enforcement exception): see "If this happens".

What to know: The 2024 amendments made clear that this rule covers health and wellness apps outside HIPAA. Any online service that provides mechanisms to track diseases, conditions, symptoms, bodily functions, fitness, fertility, sexual health, sleep, mental health or diet furnishes 'health care services or supplies', so the identifiable data it collects is PHR identifiable

health information. The 'multiple sources' test is about technical capacity, not use: an app that can sync with a fitness tracker qualifies even if a given user never connects one, and the second source need not supply health information. The FTC's examples include an app that reads the phone's calendar, and one that collects geolocation through an API (89 FR 47036-37). The biggest trap is that a breach does not require a hacker. Sharing identifiable health information without the user's authorization, for example with an advertising platform, is a breach of security, and the FTC has said disclosures buried in a privacy policy do not amount to authorization. Advertising, analytics and cloud firms that handle the data under contract for your benefit are 'third party service providers'; one that also uses the data for its own purposes is a 'PHR related entity' for that use (89 FR 47045). Either way, the question for you is whether users authorized the sharing. The fact that someone uses a health app can itself be the health information involved (318.6(b)). Information encrypted to HHS's specifications, with the keys kept separately, is not 'unsecured', so its loss is not a notifiable breach; this safe harbor does not help when the data is sent in readable form to a third party. The rule preempts only contrary state law; state breach-notification laws can still apply and are not assessed here. The rule has no size threshold and no private right of action. The FTC enforces it with civil penalties per violation, adjusted for inflation: $53,088 per violation under 16 CFR 1.98(d), unchanged in the eCFR current to 1 Oct 2026. It does not apply to HIPAA covered entities, or to activity performed as a HIPAA business associate. A company that is a business associate for clinics but also offers its app directly to consumers can be covered for that consumer side, which is why this rule looks at whether people use the app for themselves. Three kinds of company are covered. The app itself can be a vendor of a personal health record. An app that sends health data into someone else's personal health record, or is offered through one or through a provider's patient app, is a PHR related entity with the same duties: an app that only writes entries into another health platform can be covered this way even though it draws from a single source. A company that handles the data for a covered app, such as a developer hosting it for a client or an analytics or AI vendor, is a third party service provider: its one notice duty is to the business it serves, within 60 days of discovering a breach. A service provider that only accesses the data to provide its service does not become a PHR related entity by doing so (318.3(b)).

Sources: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318 · https://www.federalregister.gov/documents/2024/05/30/2024-10855/health-breach-notification-rule · https://www.law.cornell.edu/uscode/text/42/17937 · https://www.ftc.gov/business-guidance/resources/complying-ftcs-health-breach-notification-rule-0 · https://www.ftc.gov/news-events/news/press-releases/2026/09/ftc-withdraws-obsolete-policy-statement · https://www.ecfr.gov/current/title-16/chapter-I/subchapter-A/part-1/subpart-L/section-1.98 · https://www.federalregister.gov/documents/2009/08/24/E9-20169/breach-notification-for-unsecured-protected-health-information

Washington My Health My Data Act (`us-wa-mhmda`)

Citation: RCW 19.373 · **Jurisdiction:** US-WA · **Size threshold:** none · **Private right of action:** yes · **Confidence:** high · **Legal status:** in force, effective 2024-03-31 (checked 2026-10-23)

Regulates the collection, sharing and sale of 'consumer health data', defined far more broadly than medical records. It requires separate consents for collecting and for sharing, gives users rights to access and delete their data, bans geofencing around health facilities, and is enforceable by individuals through Washington's Consumer Protection Act. A company that handles consumer health data for another business (a processor) must follow that business's contract and help it meet its duties.

Why it may apply

- **Yes**: The app collects data that identifies a person's past, present or future physical or mental health status (defined broadly, including wellness data and health status inferred from other data) *(declared)*
- **No**: HIPAA applies, so the app's health data is protected health information, which this Act exempts *(assessed: unlikely to apply)*
- **Yes**: People use the app for themselves, rather than a clinic, employer or insurer running it for them *(declared)*
- **No**: The operator is a HIPAA covered entity, so all its health data is protected health information *(declared)*
- **Yes**: The app has users in Washington, or markets to Washington consumers *(declared: CA, IL, NY, OH, TX, WA (list may be incomplete))*

Its principal obligations, and how they are addressed

- `mhmda-privacy-policy` (document) Publish a consumer health data privacy policy, prominently linked from your homepage, stating the categories of health data collected and why, the sources, the categories shared, who receives them, and how users exercise their rights. *RCW 19.373.020*
- `mhmda-new-purposes-need-consent` (technical) Before collecting new categories of health data, or using it for purposes your privacy policy doesn't list, update the policy and get the user's affirmative consent first. Adding an AI feature that reads users' existing entries is a new purpose. *RCW 19.373.020(1)(c)-(d)* → Versioned consent capture (`consent-capture-versioned`)
- `mhmda-consent-to-collect` (technical) Get the user's consent for a specified purpose before collecting consumer health data, unless the collection is necessary to provide the product or service they asked for. The request must clearly state four things: the categories of health data, the purpose including the specific ways it will be used, the categories of recipients, and how to withdraw consent. Consent can't be buried in general terms of service or obtained through deceptive design. *RCW 19.373.030(1)(a), (1)(c); RCW 19.373.010(6)* → Versioned consent capture (`consent-capture-versioned`)
- `mhmda-consent-to-share` (technical) Get a separate consent, distinct from the consent to collect, before sharing consumer health data with any third party, unless sharing is necessary to provide the requested product or service. The request must clearly state four things: the categories of health data, the purpose including the specific ways it will be used, the categories of recipients, and how to withdraw consent. Disclosure to a processor acting under a binding contract, for purposes you disclosed, is not 'sharing'. *RCW 19.373.030(1)(b)-(c); RCW 19.373.010(27)* → Versioned consent capture (`consent-capture-versioned`), Third-party disclosure inventory and gate (`third-party-disclosure-gate`)
- `mhmda-sale-authorization` (technical) Do not sell consumer health data without a valid authorization signed by the user, containing the elements the Act lists. Authorizations expire after one year, and both seller and buyer must keep a copy for six years. Whether passing data to ad platforms is a 'sale' is unsettled. Treat it as a review question, not an assumption. *RCW 19.373.070* **Not triggered: No**: The operator sells user data or exchanges it for something of value *(declared)*
- `mhmda-right-to-access` (technical) Let users confirm whether you collect, share or sell their health data, access it, and get a list of every third party and affiliate it was shared with or sold to, with contact details. *RCW 19.373.040(1)(a)* → Data subject request intake and tracking (`data-subject-request-intake`)
- `mhmda-withdraw-consent` (technical) Let users withdraw consent to collection and to sharing, and stop the corresponding processing. *RCW 19.373.040(1)(b)* → Versioned consent capture (`consent-capture-versioned`), Data subject request intake and tracking (`data-subject-request-intake`)
- `mhmda-right-to-delete` (technical) Delete a user's consumer health data on request from all parts of your systems, including archives and backups (backup deletion may be delayed up to six months), and notify every processor, affiliate and third party you shared it with, so they delete it too. *RCW 19.373.040(1)(c)* → Account deletion cascade (`deletion-cascade`), Data subject request intake and tracking (`data-subject-request-intake`)
- `mhmda-appeals` (process) Run an appeal process for refused requests. Respond in writing with reasons, and if the appeal is denied, give the user a way to contact the Washington Attorney General. *RCW 19.373.040(1)(h)*
- `mhmda-request-handling` (technical) Accept rights requests through a secure, reliable method described in your privacy policy, without forcing people to create an account. Verify identity with commercially reasonable efforts, and respond free of charge up to twice a year per person. *RCW 19.373.040(1)* → Data subject request intake and tracking (`data-subject-request-intake`)
- `mhmda-no-discrimination` (process) Don't treat people worse because they used any right under the Act, for example by cutting features or refusing service after they ask to see, delete or withdraw their data. *RCW 19.373.030(1)(d)*
- `mhmda-restrict-access` (technical) Restrict access to consumer health data to the employees, processors and contractors for whom access is necessary. *RCW 19.373.050(1)(a)* → Row-level access control (`row-level-access-control`), Sensitive data segregation (`sensitive-data-segregation`)
- `mhmda-data-security` (technical) Maintain administrative, technical and physical data security practices that meet the reasonable standard of care in your industry for the confidentiality, integrity and accessibility of consumer health data. *RCW 19.373.050(1)(b)* → Row-level access control (`row-level-access-control`), Sensitive data segregation

(`sensitive-data-segregation`), Access and change audit log (`audit-logging`)

- `mhmda-processor-contracts` (vendor/contract) Let processors (hosting, AI, analytics vendors acting for you) handle consumer health data only under a binding contract that sets processing instructions and limits what they may do, and only in ways consistent with your privacy policy. *RCW 19.373.060; RCW 19.373.020(1)(e)*
- `mhmda-processor-follow-contract` (vendor/contract) Handle another business's consumer health data only under a binding contract with that business that sets out its processing instructions and limits what you may do with the data, and only as those instructions allow. If you go beyond them, the Act treats you as a regulated entity for that data, with all of its duties. *RCW 19.373.060(1)(a), (1)(c)* **Not triggered: No**: The company handles health or wellness data for another business's app or service, as its vendor *(declared)*
- `mhmda-processor-assist` (process) Help each business whose consumer health data you handle to meet its duties under this Act, with appropriate technical and organizational measures as far as possible: for example, finding, exporting or deleting a person's data when the business receives a request, and keeping the data secure. *RCW 19.373.060(1)(b)* **Not triggered: No**: The company handles health or wellness data for another business's app or service, as its vendor *(declared)*
- `mhmda-no-geofencing` (technical) Do not set up a geofence within 2,000 feet of an in-person health care facility to identify or track people seeking care, collect health data, or send them health-related notifications or ads. *RCW 19.373.080; RCW 19.373.010(14)* → **no control in this library** (see D.1)

What to know: There is no revenue or size threshold, so a pre-revenue hobby app with Washington users is in scope. The Act's 'small business' definition (under 100,000 consumers a year, or under 50% of revenue from health data and under 25,000 consumers) only delayed the original compliance date to 30 June 2024. It exempts nobody today. 'Consumer health data' is much broader than medical records. Mood, wellness and fitness data count, as do precise location that could show someone seeking care and health status an algorithm infers from non-health data. The Act applies to nonprofits too. A 'consumer' includes anyone whose health data is collected in Washington, not only residents. HIPAA protected health information is exempt, but only that data: a HIPAA business associate's separate direct-to-consumer data is still covered. The Act declares every violation an unfair or deceptive practice affecting the public interest under the Washington Consumer Protection Act (RCW 19.373.090), which lets individuals sue. A person suing still has to show an injury to business or property caused by the violation, but even so this makes the Act materially riskier than most state privacy laws for small apps. The geofencing ban and the rule on selling health data apply to 'any person', not only regulated entities. Besides HIPAA protected health information, the Act exempts, among other things: de-identified data; human-subjects research data; substance-use treatment records under 42 CFR Part 2; and information governed by the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act or FERPA (RCW 19.373.100). This assessment treats any Washington users as enough for the Act to possibly apply. Strictly, it covers businesses that conduct business in Washington or target Washington consumers, so an app with only incidental Washington users may fall outside it. A processor that handles the data outside its contract, or for its own purposes, is treated as a regulated entity for that data, with every duty in the Act (RCW 19.373.060(1)(c)). Developers and agencies that host or run a wellness app for a client are usually processors for it.

Sources: https://app.leg.wa.gov/RCW/default.aspx?cite=19.373&full=true

New York health-data protections (geofencing ban, abortion-referral reports, shield laws, police access) (`us-ny-geofencing`)

Citation: N.Y. Gen. Bus. Law 394-e to 394-i · **Jurisdiction:** US-NY · **Size threshold:** none · **Private right of action:** yes · **Confidence:** medium · **Legal status:** in force, effective 2023-07-02 (checked 2026-10-23)

New York bars anyone from geofencing health care facilities to send ads, build profiles or infer health status; bars businesses from disclosing reports of abortion referrals or inquiries except to set recipients; bars police from obtaining health data without a warrant; and requires companies based in New York to resist other states' demands for information about reproductive or gender-affirming care that is legal in New York.

Why it may apply

- **Yes**: The app collects precise location *(declared)*

- **Yes**: The app has users in New York, or does business there *(declared: CA, IL, NY, OH, TX, WA (list may be incomplete))*

Its principal obligations, and how they are addressed

- `ny-no-geofencing` (technical) Don't set up a geofence or similar virtual boundary (a radius of 1,850 feet or less, drawn with GPS, cell, Wi-Fi, IP address or any other location data) around any health care facility other than your own, to send digital ads, build consumer profiles, or infer anyone's health status, condition or treatment; and don't deliver digital ads to people at or inside such a facility through a geofence. 'Health care facility' covers any provider of medical care or related services, including licensed mental health and addiction programs. *N.Y. Gen. Bus. Law 394-g(1)-(2)* → **no control in this library** (see D.1)
- `ny-abortion-referral-reports` (technical) Don't give anyone a report of a person being referred for abortion services, or of their inquiry or request for them, except: law enforcement (whose request must include a sworn statement that it is solely for law enforcement purposes, and is further limited by the warrant and shield rules), the New York State or New York City health department, someone the person authorized in writing, or under a court order. Every request must be in writing and give the requester's name and address. *N.Y. Gen. Bus. Law 394-e(1)* **Not triggered: No**: The app handles reproductive, sexual health or gender-affirming care information *(declared)*

Parts of this law handled outside the obligations above

- N.Y. Gen. Bus. Law 394-f (Out-of-state warrants for data on care protected in New York): see "If this happens".
- N.Y. Gen. Bus. Law 394-h (Police access to electronic health information): see "If this happens".
- N.Y. Gen. Bus. Law 394-i (Demands for information on care protected in New York): see "If this happens".

What to know: These New York rules apply to anyone, with no size threshold. The geofencing ban targets drawing a virtual fence around clinics to send ads, build profiles or infer health status; ordinary location features aren't caught, and a provider may geofence its own facility. 'Health care facility' is broad: any provider of medical care or related services, including licensed mental health and addiction programs. The radius (1,850 feet) sits between Washington's 2,000 and Nevada's and Connecticut's 1,750. Disclosing reports of abortion referrals or inquiries outside the permitted recipients lets individuals sue for up to $10,000 per wilful violation. Police need a warrant to obtain health data. A company located, headquartered or incorporated in New York that receives another state's demand for information about reproductive or gender-affirming care legal in New York must not comply without a sworn statement, must notify the Attorney General within 5 business days, and must give the people concerned 30 days' notice: where the company is based matters, not where its users are.

Sources: https://www.nysenate.gov/legislation/laws/GBS/394-E · https://www.nysenate.gov/legislation/laws/GBS/394-F · https://www.nysenate.gov/legislation/laws/GBS/394-G · https://www.nysenate.gov/legislation/laws/GBS/394-H · https://www.nysenate.gov/legislation/laws/GBS/394-I · https://ag.ny.gov/shield-law-notice

B.2 Need more information

Nevada consumer health data law (SB 370) (`us-nv-chd`)

Citation: NRS 603A.400 to 603A.550 (added by SB 370, 2023) · **Jurisdiction:** US-NV · **Size threshold:** none · **Private right of action:** no · **Confidence:** medium · **Legal status:** in force, effective 2024-03-31 (checked 2026-10-21)

Regulates collecting, sharing and selling consumer health data about people in Nevada, much like Washington's law: separate consents for collecting and for sharing, a health-data privacy policy, rights to see who received the data and to have it deleted within 30 days, appeals, a signed authorization to sell, and a geofencing ban within 1,750 feet of health care facilities. Companies that handle the data for another business must follow its contract and help it. The Attorney General enforces it; individuals cannot sue under it.

Established so far

- **Yes**: The app collects data it uses to identify a person's past, present or future health status *(declared)*
- **Yes**: People use the app for themselves, rather than a clinic, employer or insurer running it for them *(declared)*

Unresolved: answer these to decide

- **Unknown**: The app has users in Nevada, or markets to Nevada consumers *(declared: CA, IL, NY, OH, TX, WA (list may be incomplete))*

If it does apply, its principal obligations would include

- `nv-privacy-policy` (document) Publish a consumer health data privacy policy, and link to it conspicuously from your main website (or otherwise provide it clearly and conspicuously). It must state: the categories of health data you collect and how you use them; their sources; the categories you share; the categories of third parties and affiliates you share with; your purposes; how the data is processed; how to make a request under these rights; any process for reviewing and asking to change one's data; how you tell people about material changes to the policy; whether third parties may collect health data across sites and services when people use yours; and the policy's effective date. *NRS 603A.495(1)-(2)*
- `nv-new-purposes-need-consent` (technical) Don't collect, use or share categories of health data, share with third parties or affiliates, or use the data for purposes, beyond those named in your privacy policy, unless you first tell each person affected and get their affirmative, voluntary consent. *NRS 603A.495(3)(a)-(c)*
- `nv-consent-to-collect` (technical) Get the consumer's affirmative, voluntary consent before collecting consumer health data, unless the collection is necessary to provide the product or service they asked for. The consent request must clearly and conspicuously state the categories of data, the purpose and how the data will be used, and how to withdraw consent and ask you to stop. *NRS 603A.500(1), (3)*
- `nv-consent-to-share` (technical) Get a separate consent, distinct from the consent to collect, before sharing consumer health data, unless sharing is necessary to provide the requested product or service or is required or authorized by law. The request must state the categories of data, the purpose and use, the categories of people and organizations it will go to, and how to withdraw consent. Unlike Washington's, Nevada's definition of sharing has no exception for your own vendors: giving the data to an analytics or AI provider, for example, needs this consent unless it's necessary to provide what the person asked for. *NRS 603A.500(2)-(3), 603A.480*
- `nv-consumer-rights` (technical) On request, confirm whether you collect, share or sell the person's health data, give them a list of all third parties you shared it with or sold it to, and stop collecting, sharing or selling it. Deletion requests have their own, shorter deadline (nv-right-to-delete). *NRS 603A.505(1)*
- `nv-request-handling` (technical) Offer a secure and reliable way to make these requests that lets you authenticate who is asking. Answer within 45 days of authenticating a request; you may extend once by up to 45 more days if needed, telling the person why within the first 45. If you can't authenticate a request after commercially reasonable efforts, you may ask for more information instead of acting on it. Answer at least two requests a year free of charge; you may charge a reasonable fee only for requests that are manifestly unfounded, excessive or repetitive, and you must be able to prove that. *NRS 603A.505(2), 603A.510*
- `nv-right-to-delete` (technical) Within 30 days of authenticating a deletion request, delete the health data from your records and network, and notify every affiliate, processor, contractor or other third party you shared it with, so they delete it too. Copies on backup or archive systems may wait up to two years, as needed to restore those systems. *NRS 603A.505(1)(d), 603A.515(1), (3)*
- `nv-appeals` (process) Set up a way for people to appeal a refusal to act on their request, conspicuously available on your website and similar to the request process. Within 45 days of receiving an appeal, tell the person in writing what you did or decided and why, and, if you refused, how to contact the Nevada Attorney General. *NRS 603A.520*
- `nv-restrict-access` (technical) Let employees and processors access consumer health data only where reasonably necessary for the purpose the consumer consented to, or to provide what they asked for. *NRS 603A.525(1)*
- `nv-data-security` (technical) Establish, implement and maintain administrative, technical and physical security policies and practices for consumer health data that meet your industry's standard of care, are reasonable for the volume and nature of the data, and meet Nevada's general data-security law (NRS 603A.010 to 603A.290) where it applies. *NRS 603A.525(2)*

- `nv-processor-contracts` (vendor/contract) Let processors handle consumer health data for you only under a contract that sets the processing instructions and the specific actions they may take, and that is consistent with your privacy policy. *NRS 603A.495(3)(d), 603A.530(1)*
- `nv-sale-authorization` (technical) Don't sell or offer to sell consumer health data without the consumer's signed written authorization, and only within its scope. It must be in plain language and give: the seller's and buyer's names and contact details; the specific data to be sold; the purpose, how the data will be gathered and how the buyer will use it; that your goods or services can't be made conditional on it; that it can be revoked at any time, and how; that the buyer may pass the data on, after which this law no longer protects it; and its expiry date, at most one year after signing. Give a copy to the consumer and to the buyer; seller and buyer must each keep a copy for six years after it expires. *NRS 603A.535*
- `nv-no-geofencing` (technical) Do not set up a geofence within 1,750 feet of a medical facility or other provider of in-person health care to identify or track people seeking care, collect health data, or send them notifications or ads. *NRS 603A.540(1)*
- `nv-no-discrimination` (process) Don't discriminate against anyone for exercising these rights or for acting to enforce this law. *NRS 603A.545*
- `nv-processor-follow-contract` (vendor/contract) Handle another business's consumer health data only under a contract with that business that sets the processing instructions and the specific actions you may take. If you go outside it, the law treats you as a regulated entity for that data, with all of its duties. *NRS 603A.530(1), (3)*
- `nv-processor-assist` (process) As far as practicable, help each business whose consumer health data you handle to meet its duties under this law. *NRS 603A.530(2)*
- `nv-processor-delete-on-notice` (technical) When a business you handle consumer health data for tells you about a deletion request, delete that data from your records and network within 30 days. Copies on backup or archive systems may wait up to two years, as needed to restore those systems. *NRS 603A.515(2)-(3)*

Parts of this law handled outside the obligations above

- NRS 603A.490(2) (Buyers of a regulated entity take on its duties): see "If this happens".

What to know: Nevada's law follows Washington's, with differences that matter. Individuals cannot sue: NRS 603A.550 says it creates no private right of action, and a violation is treated as a deceptive trade practice. Deletion requests must be carried out within 30 days of authenticating them, faster than the 45 days for other requests; anyone you shared the data with must be told, and must delete it within 30 days of hearing. Request deadlines run from authenticating the request, not from receiving it. The geofencing ban is 1,750 feet rather than 2,000, and it and the sale rule apply to any person, not only regulated entities. A 'consumer' must have requested a product or service, so people who only visit a website are generally outside it. 'Consumer health data' is data the business uses to identify health status, including inferences, which is narrower than Washington's definition; data used only for gameplay, or for shopping interests that aren't used to identify health status, is excluded. There is no size threshold. The law does not apply to 'any person or entity that is subject to' HIPAA, wording broader than Washington's data-only exemption: it may exempt a clinic vendor's whole company, including its own consumer app. To be safe, this report still treats that consumer-side data as covered and refers the question to a lawyer. It also exempts GLBA financial institutions, 42 CFR Part 2 records, human-subjects research and public-health uses, FCRA and FERPA data, government and law enforcement, nonrestricted gaming licensees, and data de-identified to HIPAA's standard, among others (NRS 603A.490). A processor that acts outside its contract is treated as a regulated entity for that data (NRS 603A.530(3)). A sale authorization lasts at most one year, and both seller and buyer must keep it for six years after it expires. Anyone you shared the data with, not only your processors, must delete it within 30 days of being told about a deletion request (NRS 603A.515(2)); this report asks only whether you handle data as another business's vendor, so a business that received health data in some other way should apply this itself.

Sources: https://www.leg.state.nv.us/nrs/nrs-603a.html · https://www.fisherphillips.com/en/news-insights/beyond-hipaa-states-join-trend-to-protect-consumer-health-data.html · https://www.bassberry.com/news/nevada-consumer-health-data-law-takes-effect-on-march-31-2024/

Connecticut Data Privacy Act (including its health-data and minors' rules) (`us-ct-ctdpa`)

Citation: Conn. Gen. Stat. 42-515 to 42-526 and 42-529 to 42-529e, as amended by P.A. 23-56 and P.A. 25-113 · **Jurisdiction:** US-CT · **Size threshold:** none · **Private right of action:** no · **Confidence:** medium · **Legal status:** in force, effective 2023-07-01 (checked 2026-10-23)

Connecticut's privacy law covers any business that processes Connecticut residents' sensitive data, such as health data or precise location, whatever its size. It requires consent before processing that data, limits collection to what is necessary, gives residents rights to access, correct, delete and opt out, with appeals, and requires data protection assessments. Its health-data rules (confidential access, vendor contracts, consent before selling, and a geofencing ban near mental and reproductive health facilities) also reach nonprofits. Apps used by known minors have extra duties, including no targeted ads or sale of minors' data. Only the Attorney General enforces it.

Established so far

- **Yes**: The app processes health data, which the Act treats as sensitive data *(declared)*
- **Yes**: The app collects precise location, which the Act treats as sensitive data *(declared)*
- **Yes**: The operator is a for-profit business (nonprofits are exempt from most of the Act, but not from its health-data rules) *(declared)*
- **Yes**: People use the app for themselves, rather than a clinic, employer or insurer running it for them *(declared)*
- **Yes**: The app processes data used to identify a person's physical or mental health condition, diagnosis or status *(declared)*
- **Yes**: The operator is a for-profit business (nonprofits are exempt from the minors' rules) *(declared)*

Unresolved: answer these to decide

- **Unknown**: The app has users in Connecticut, or targets Connecticut residents *(declared: CA, IL, NY, OH, TX, WA (list may be incomplete))*
- **Unknown**: The operator knows that specific users are under 18 *(answered unknown)*

If it does apply, its principal obligations would include

- `ct-privacy-notice` (document) Publish a clear privacy notice stating: the categories of personal data you process and why; how people exercise their rights and appeal your decisions; the categories of data you sell and to which categories of third parties; any targeted advertising or sale for targeted advertising; an email address or other online contact; whether you collect, use or sell personal data to train large language models; and the month and year it was last updated. Link to it with a link containing the word "privacy" on your website's home page, on your app-store or download page, and in the app's settings menu. Provide it in every language you offer the product in, accessible to people with disabilities. If you make a retroactive material change, tell the people affected and give them a fair chance to withdraw consent. *Conn. Gen. Stat. 42-520(b)*
- `ct-data-minimization` (process) Collect only the personal data that is reasonably necessary and proportionate to the purposes you disclosed. *Conn. Gen. Stat. 42-520(a)(1)(A)*
- `ct-new-purposes-need-consent` (technical) Don't use personal data for any new purpose that is neither reasonably necessary to nor compatible with the purposes you disclosed, unless the person consents first. *Conn. Gen. Stat. 42-520(a)(1)(B), as amended by P.A. 26-64, s. 14*
- `ct-consent-sensitive-data` (technical) Process sensitive data, including health data and precise location, only where reasonably necessary for the purposes you disclosed and with the person's consent: a clear, affirmative, specific and informed agreement, not acceptance of general terms and not obtained through dark patterns. For children under 13, follow COPPA's parental consent. *Conn. Gen. Stat. 42-520(a)(1)(D); 42-515(7)*
- `ct-revoke-consent` (technical) Let people withdraw consent at least as easily as they gave it, and stop the processing as soon as practicable, and no later than 15 days after receiving the withdrawal. *Conn. Gen. Stat. 42-520(a)(1)(G)*
- `ct-consent-to-sell` (technical) Don't sell, or offer to sell, health data without first getting the person's consent; selling other sensitive data needs consent too. This applies to anyone handling Connecticut consumers' health data, nonprofits included. *Conn. Gen. Stat. 42-526(a)(1)(D); 42-520(a)(1)(H)*

- `ct-no-location-sale` (technical) Never sell anyone's precise location data, even with their consent. Anyone who receives it from you may not sell it either. *Conn. Gen. Stat. 42-520(a)(3) and 42-521(a)(2), as amended by P.A. 26-64, ss. 14-15*
- `ct-no-discrimination` (process) Don't discriminate against people for exercising their rights under the Act, for example by refusing service, charging more or giving a worse service. Genuine loyalty, rewards or premium-feature programs that people join voluntarily are allowed. *Conn. Gen. Stat. 42-520(a)(1), (a)(2)*
- `ct-anti-bias` (process) Don't process personal data in a way that breaks state or federal laws against unlawful discrimination. *Conn. Gen. Stat. 42-520(a)(1)(E)-(F)*
- `ct-opt-out` (technical) Let people opt out of targeted advertising, sale of their data and certain profiling: a clear link on your website to an opt-out page, honouring opt-out preference signals such as Global Privacy Control, and accepting opt-outs from people's authorized agents. Opt-out requests don't need identity checks; you may refuse one only with a documented, good-faith belief that it is fraudulent, and must say so to the requester. Every business the Act covers must offer these as part of its request methods, even if it doesn't do targeted advertising or sell data. *Conn. Gen. Stat. 42-518(a)(5), 42-518(c)(4), 42-519, 42-520(c)*
- `ct-consumer-rights` (technical) Let people confirm whether you process their data and access it, including inferences drawn from it and whether it is used for profiling behind significant decisions; correct it; delete it, including any profile built from public information and inferences drawn from it; get a portable copy; and get a list of the third parties you sold it to. Where profiling made a significant decision about someone, let them question it, learn the reason and review the data used. When answering access requests, don't reveal Social Security, ID, financial account, health insurance or medical ID numbers, passwords, security answers or biometric data: say that you hold them instead. *Conn. Gen. Stat. 42-518(a), (e), as amended by P.A. 26-64, s. 13*
- `ct-request-handling` (technical) Offer secure and reliable ways to make requests, described in your privacy notice, without requiring a new account. Answer within 45 days of receiving a request; you may extend once by 45 days, telling the person why within the first 45. If you decline, say why and how to appeal within 45 days. Answer free once per person in any 12 months; you may charge or decline only for manifestly unfounded, excessive or repetitive requests, and must be able to prove that. If you can't authenticate a request with commercially reasonable effort, tell the person what more you need. If you got someone's data from a source other than them, you may meet their deletion request by keeping a minimal record of the request, used only to keep the data deleted, or by opting them out of all processing the Act doesn't exempt. *Conn. Gen. Stat. 42-518(b)-(c), 42-520(c)(1)*
- `ct-appeals` (process) Run a process for people to appeal a refusal, conspicuously available and similar to the request process. Answer each appeal in writing within 60 days of receiving it, with reasons; if you deny it, give an online way, if available, or another way to complain to the Attorney General. *Conn. Gen. Stat. 42-518(d)*
- `ct-data-security` (technical) Maintain reasonable administrative, technical and physical data security practices, appropriate to the volume and nature of the personal data. *Conn. Gen. Stat. 42-520(a)(1)(C)*
- `ct-data-protection-assessment` (process) Before processing that carries a heightened risk of harm, including processing sensitive data such as health data, targeted advertising, sale, and risky profiling, conduct and document a data protection assessment weighing the benefits against the risks to people, as reduced by your safeguards. The Attorney General can require you to disclose it. One assessment may cover similar processing, and one done for another law counts if it is similar in scope. *Conn. Gen. Stat. 42-522(a)-(b), (d)-(g)*
- `ct-impact-assessment` (process) If you use profiling to make decisions with legal or similarly significant effects on people, including about access to a health care service, conduct an impact assessment: its purpose and uses, foreseeable risks and how you reduce them, the data used and produced, performance measures and limits, transparency, and monitoring after launch. *Conn. Gen. Stat. 42-522(c), (g)(2); 42-515(15)*
- `ct-deidentified-data` (process) If you keep de-identified data: take reasonable measures so it can't be linked to anyone, publicly commit not to re-identify it, and bind everyone you give it to by contract to the same. If you share pseudonymous or de-identified data, monitor the recipients' compliance and act on breaches of those commitments. *Conn. Gen. Stat. 42-523(a), (e); 42-515(16)*
- `ct-confidential-access` (process) Give employees and contractors access to health data only if they are bound by a contractual or statutory duty of confidentiality. This applies to anyone handling Connecticut consumers' health data, nonprofits included. *Conn. Gen. Stat. 42-526(a)(1)(A)*

- `ct-processor-contracts` (vendor/contract) Give processors access to personal data, and especially health data, only under a binding contract that sets out the processing instructions, the nature and purpose of processing, the type of data, the duration, and both sides' rights and duties, and requires the processor to: keep everyone handling the data under a duty of confidentiality; delete or return the data at the end of the service; give you the information needed to show compliance; use subcontractors only under a written contract, after giving you a chance to object; and allow reasonable assessments. *Conn. Gen. Stat. 42-521(b); 42-526(a)(1)(B)*
- `ct-no-geofencing` (technical) Do not use a geofence within 1,750 feet of a mental health facility or reproductive or sexual health facility to identify, track, collect data from, or send notifications to consumers about their health data. *Conn. Gen. Stat. 42-526(a)(1)(C); 42-515(19), (23), (37)*
- `ct-processor-follow-instructions` (vendor/contract) Process another business's personal data only on its instructions and under a contract with the terms the Act requires. If you aren't limited by its instructions, or don't follow them, the Act treats you as a controller for that processing, with all of a controller's duties. *Conn. Gen. Stat. 42-521(a)-(b), (d)*
- `ct-processor-assist` (process) Help each business you process data for to meet its duties: answering people's requests, keeping the data secure, handling notice of a breach of your systems, and giving it the information it needs for its data protection and impact assessments, including under the minors' rules. *Conn. Gen. Stat. 42-521(a); 42-529c(a)*
- `ct-minors` (technical) Don't use the personal data of anyone you know, or wilfully disregard, is under 18 for targeted advertising, and don't sell it, even with consent. *Conn. Gen. Stat. 42-529a(b)(1)(A); 42-520(a)(1)(I)*
- `ct-minors-data-limits` (technical) Process minors' personal data only where reasonably necessary to provide the service, only for the purpose you disclosed when collecting it (or a compatible one), and for no longer than necessary. Use it for profiling behind significant decisions, including about health care services, only where reasonably necessary and with the minor's consent, or a parent's for children under 13. *Conn. Gen. Stat. 42-529a(b)(1)(B)-(D), (b)(3)*
- `ct-minors-location` (technical) Collect a minor's precise location only if strictly necessary to provide the service, only for as long as necessary, and with a signal visible to the minor for the whole time it is being collected. *Conn. Gen. Stat. 42-529a(b)(2)*
- `ct-minors-design` (technical) For minors: don't use consent screens designed to steer or pressure them, or design features meant to significantly increase or extend their use of the app. If the app has direct messaging, block unsolicited messages from adults to minors they aren't already connected with, by default, with easy safeguards minors and parents can use. *Conn. Gen. Stat. 42-529a(c)*
- `ct-minors-assessment` (process) Use reasonable care to avoid a heightened risk of harm to minors. Conduct a data protection assessment of the service covering its purpose, the minors' data it processes and why, and the foreseeable risks of harm to minors, and an impact assessment if it uses profiling. Review them when the processing changes, keep them for three years after the service ends, and put a plan in place to reduce any heightened risk you find. Doing the assessments gives you a presumption of reasonable care. *Conn. Gen. Stat. 42-529a(a); 42-529b*
- `ct-social-unpublish-minor` (technical) When a user under 18, or the parent or guardian of a user under 16, asks you to unpublish the minor's account, remove it from public view within 15 business days. Offer secure, reliable ways to ask, described in your privacy notice, and don't make a parent create an account to ask. If you can't authenticate a request, say what more you need. *Conn. Gen. Stat. 42-528(b)(1), (3)-(4), (c)*
- `ct-social-delete-minor` (technical) When a user under 18, or the parent or guardian of a user under 16, asks you to delete the minor's account, delete it and stop processing the minor's personal data within 45 business days, unless the law requires or permits you to keep it. You may extend once by 45 business days, telling them why within the first 45. *Conn. Gen. Stat. 42-528(b)(2)*
- `ct-social-safety-center` (document) Build an online safety center into the platform, giving users: resources to prevent cyberbullying and to find mental health services (including a website or phone number for anxiety treatment or suicide prevention); behavioral health education; how to report harmful or unwanted behavior; and information on social media's effects on mental health. Also adopt a cyberbullying policy saying how you handle reports. *Conn. Gen. Stat. 42-530(b)-(c)*
- `ct-genetic-notice` (document) Before accepting any sample, genetic data or payment, tell people your policies on collecting, using and disclosing genetic data. Keep a prominent privacy notice on your website covering how you collect, use, give access to, disclose, transfer, secure, keep and delete their data, and their consent to it. *P.A. 26-64, s. 19(a)(2)-(3)*

- `ct-genetic-consent` (technical) Get express consent before collecting, using or disclosing anyone's genetic data, after telling them how you use it, everyone who may see their results (vendors included) and how you may disclose it. Get separate express consent before sharing it with anyone other than your vendors, using it for anything beyond the testing they asked for, or keeping their biological sample after the test. Sharing it for research needs informed consent under the federal human-subjects rules (45 CFR 46). People own their samples and results and keep exclusive control over them. *P.A. 26-64, s. 18; P.A. 26-64, s. 19(a)(1), (4)-(6)*
- `ct-genetic-no-disclosure` (technical) Don't disclose anyone's genetic test results to anyone but them, without their express consent or a court order, warrant or subpoena. Never disclose genetic data to their employer, to health, life or long-term-care insurers or anyone supplying insurers with data for underwriting, or to anyone you know, or should know, intends to use it for marketing, including targeted advertising. *P.A. 26-64, s. 19(a)(7)-(8)*
- `ct-genetic-security` (technical) Keep biological samples and genetic data secure against unauthorized access, destruction, use, change or disclosure. *P.A. 26-64, s. 19(a)(9)*
- `ct-genetic-rights` (technical) Give people a way to get their genetic data, have it deleted, have their sample destroyed (with confirmation that it was), and withdraw consent to research use of their genetic data, by you or by anyone you gave it to. *P.A. 26-64, s. 19(a)(10)*

Parts of this law handled outside the obligations above

- Conn. Gen. Stat. 42-531 (Connected devices with cameras or microphones): not covered by this report. Covers internet-connected home appliances, televisions and toys with a camera or microphone, and those with access to them under contract with the manufacturer; not apps.
- Conn. Gen. Stat. 42-531a (Connected vehicle services): not covered by this report. Covers motor-vehicle manufacturers' connected services; not health apps.
- Conn. Gen. Stat. 42-522(d), 42-525(b)-(c), 42-529b(f), 42-529e(b)-(c) (Attorney General requests and cure): see "If this happens".
- P.A. 26-64, ss. 1-10 (Data broker registration and deletion mechanism): not covered by this report. Applies to businesses that sell or license identifying data, but exempts data about people the business has a contractual or similar relationship with, such as its own users, and exempts covered entities and business associates (s. 7). An app selling data about people who aren't its users would need to register from 1 January 2027.
- P.A. 26-64, s. 11 (Prices set from personal data; surveillance pricing): not covered by this report. Requires a disclosure on online prices raised by a price-setting device using personal data, and bans surveillance pricing by retailers and delivery services. RuleAlign doesn't ask about pricing; an app that personalises prices from users' data should check it.
- P.A. 26-64, s. 20 (Cable television advertising): not covered by this report. Applies to cable operators; not health apps.

What to know: Connecticut is one of the strictest states for small health apps. Since 1 July 2026 the whole Act applies to any business processing Connecticut residents' sensitive data, which includes health data, precise location and data from known children, whatever its size; its health-data rules (42-526) reach nonprofits too, though the rest of the Act doesn't. Consent means a clear affirmative act: accepting general terms, or agreement obtained through dark patterns, doesn't count, and a withdrawal must be acted on within 15 days. Requests are free only once a year (Washington and Nevada: twice), and appeals get 60 days. The privacy notice must be linked from the app-store page and the app's settings as well as the website, and must say whether data is used to train large language models. Minors' data (under 18) can't be used for targeted ads or sold, even with consent, and since 1 October 2026 nobody's precise location may be sold, even with consent. The geofencing ban (1,750 feet) covers only mental health and reproductive or sexual health facilities. Covered entities and business associates are exempt as whole organizations (42-517(a)(7)), and the 2025 amendments kept this. Read literally, that may put a clinic vendor's own consumer app outside the Act; to be safe, this report still treats that consumer-side data as covered and refers the question to a lawyer. Individuals cannot sue: the Attorney General enforces it, and the mandatory cure period ended on 31 December 2024. The 35,000-consumer test matters only for businesses without sensitive data. Apps that are mainly social platforms (public profiles, connections and posts) have extra duties: remove a minor's account from view within 15 business days and delete it within 45 when asked, and offer an online safety center with mental health resources. Since 1 October 2026, an app that offers genetic testing, or analyses DNA data users upload, has its own duties: express consent, separate consent to share, reuse or keep samples, and never disclosing genetic data to employers, insurers or marketers.

Sources: https://www.cga.ct.gov/2026/sup/chap_743jj.htm · https://www.cga.ct.gov/current/pub/chap_743jj.htm · https://www.cga.ct.gov/2026/ACT/PA/PDF/2026PA-00064-R00SB-00004-PA.PDF · https://www.hunton.com/privacy-and-cybersecurity-law-blog/connecticut-amends-the-connecticut-data-privacy-act · https://www.truevault.com/learn/extensive-changes-to-connecticuts-privacy-law · https://www.manatt.com/insights/newsletters/privacy-and-data-security/connecticuts-new-law-on-consumer-health-data-is-n

California Confidentiality of Medical Information Act (CMIA), including the Genetic Information Privacy Act (`us-ca-cmia`)

Citation: Cal. Civ. Code 56-56.37 · **Jurisdiction:** US-CA · **Size threshold:** none · **Private right of action:** yes · **Confidence:** medium · **Legal status:** in force, effective 1982-01-01 (checked 2026-11-01)

California's medical privacy law. Health care providers, and businesses it treats as providers (health-tracking apps, mental health and reproductive health digital services, record keepers for providers and, from 1 January 2027, health care chatbots), may not disclose medical information without the patient's signed authorization, except where the law requires or allows it, and must keep it confidential. Its Genetic Information Privacy Act sets consent and security rules for genetic testing companies. It has no size threshold and reaches nonprofits.

Established so far

- **Yes**: The app has users in California, or the company markets to or does business there *(declared: CA, IL, NY, OH, TX, WA (list may be incomplete))*
- **Yes**: The app stores health or wellness data *(declared)*

Unresolved: answer these to decide

- **Unknown**: The app is designed to help people manage their health information or a health condition, or markets itself as offering health services *(answered unknown)*

Findings that need attention

- **[HIGH] Tracking tags may be disclosing medical information** (not ruled out). Under the CMIA, sending medical information to an advertising or analytics company that isn't only processing it for you is a disclosure that needs the user's signed authorization. Each affected person can claim $1,000 without proving harm, and class actions over tracking tags on health websites and apps have relied on the CMIA.

If it does apply, its principal obligations would include

- `cmia-authorization-before-disclosure` (technical) Don't disclose users' medical information (their medical history, mental or physical condition or treatment, including what they log in a mental health or reproductive health app) to anyone without the user's signed authorization, unless the law requires it, for example a court order or a valid search warrant, or allows it: to other providers for diagnosis or treatment; for payment; to a company providing billing, claims management, medical data processing or other administrative services for you, which may not disclose it further; to anonymize it; for approved research; and the other purposes the law lists. A company that only processes the information for you, under a contract forbidding it to use or disclose it for anything else, comes within the allowance for data-processing and administrative services and may not pass it on. Any company that uses it for its own purposes needs the user's authorization first: advertising platforms always do, and analytics tools and AI providers do when they keep it for their own use or train on it. *Cal. Civ. Code 56.10(a)-(c), 56.13*
- `cmia-authorization-form` (document) Make every authorization valid: handwritten or in type no smaller than 14 point; clearly separate from any other text, with a signature (electronic is fine) used for nothing else; signed and dated by the user or their legal representative (a minor signs only for care they could consent to themselves); stating the specific uses and limits of the information to be disclosed, who may disclose it, who may receive it and how they may use it; with an expiry date or event no more than a year away, unless the user asks for longer or it is for a clinical trial or research study; and telling the user they may have a copy. Give them a copy and say how to get more copies or a digital version.

Accepting your terms of use is not an authorization. Tell each recipient the limits on its use. A user may cancel or change an authorization in writing, effective once you receive it. *Cal. Civ. Code 56.11, 56.12, 56.14, 56.15*

- `cmia-no-sale-or-marketing` (process) Unless the user expressly authorizes it, don't share or sell medical information, use it for marketing, or use it for anything not necessary to provide health care services to the user, and never disclose it for immigration enforcement. Training AI models on users' medical information, or analysing it for anything other than providing the service to that user, needs their express authorization. If you receive it from a provider, don't pass it on to anyone not providing direct health care to the user. *Cal. Civ. Code 56.10(d)-(f)*
- `cmia-no-conditioning` (process) Don't make users sign an authorization, release, consent or waiver allowing disclosures the law would otherwise forbid, as a condition of using your services. Any other waiver of the CMIA's protections is void. *Cal. Civ. Code 56.37*
- `cmia-confidential-storage` (technical) Create, keep, store and destroy medical information in a way that preserves its confidentiality. If information is released because of negligence, each affected person can recover $1,000 without proving harm, plus any actual damages, and regulators can fine up to $2,500 per negligent disclosure. *Cal. Civ. Code 56.06, 56.101(a), 56.36(b)*
- `cmia-record-integrity` (technical) If your system is an electronic health or medical record system (a record of health information created, gathered, managed and consulted by clinicians and staff), it must protect the integrity of the records and automatically record every change or deletion: who made it, when the information was accessed, and what changed. *Cal. Civ. Code 56.101(b), (d)*
- `cmia-sensitive-services-safeguards` (technical) If you store medical information about sensitive services electronically for a provider, health plan, contractor or employer, have the ability to: limit access to information about gender-affirming care, abortion and contraception to the people authorized to see it; stop that information being disclosed, accessed, transferred or processed outside California, as the CMIA requires; keep it separate from the rest of the patient's record; and automatically switch off access to it from other states. These capabilities were due by 1 July 2024; from 1 January 2027 they must also be switched on. *Cal. Civ. Code 56.101(c), as amended by Stats. 2026, ch. 607*
- `cmia-abortion-records-out-of-state` (technical) Don't knowingly disclose, transfer or give access to identifying medical information about an abortion that is lawful in California (seeking, obtaining, providing or helping with one), held in an electronic health record system, which this report takes to include a health app's own database, or shared through a health information exchange, to anyone in another state. The exceptions: an authorization that expressly covers abortion information; payment; accreditation or quality review; bona fide research; the patient; a California or federal court order that keeps the patient's identity sealed; and what federal law expressly requires. *Cal. Civ. Code 56.110*
- `cmia-clinic-data-limits` (process) Use and disclose patients' medical information you receive from a clinic or other provider only to provide your services to it, such as billing, medical data processing or other administrative services, and don't disclose it further except as the CMIA allows or under a new valid authorization. *Cal. Civ. Code 56.10(c)(3), 56.13*
- `cmia-free-copy` (process) When a user asks in writing, give them, free of charge, a copy of any medical profile, summary or information you keep about them. *Cal. Civ. Code 56.07*
- `cmia-mental-health-partner-notice` (document) If you partner with a health care provider to offer a mental health digital service, tell the provider how to find data breaches reported on the California Attorney General's website. *Cal. Civ. Code 56.251*
- `gipa-privacy-notice` (document) Make available a plain-language summary of how you collect, use, keep and disclose genetic data; a prominent, easy-to-find privacy notice covering collection, consent, use, access, disclosure, maintenance, transfer, security, retention and deletion, and how to complain about a violation; and a notice that deidentified genetic or phenotypic information may be shared for research under the Common Rule. *Cal. Civ. Code 56.181(a)(1)*
- `gipa-express-consent` (technical) Get separate express consent (a deliberate action after a clear, prominent notice; never inferred from silence, and never obtained through dark patterns) for each of: using the genetic data from the test, including who can access it, how it may be shared and why; keeping the biological sample after the test; each use beyond the test's main purpose; each transfer to a third party other than a service provider, naming that third party; and marketing based on the user's genetic data, or a third party's marketing based on their use of the test. Offer easy ways to withdraw consent, at least one through your main way of communicating with users; act on a withdrawal within 30 days, and destroy a stored sample within 30 days of a withdrawal of consent to keep it. *Cal. Civ. Code 56.18(b)(1), (6), 56.181(a)(2), (b), (c)*

- `gipa-ad-labels` (document) If you show users ads for another company's products or services, whether based on their genetic data (with their consent) or on their having used your test, label each ad prominently as advertising and name every third party that helped place it, and, where it applies, say that you haven't vetted or endorsed the product or its claims. You don't need consent to advertise your own products on your own website or app based only on what the user ordered or used, if the ad uses nothing else specific to them and isn't placed to reach people differently by race, sex, religion, disability or another characteristic protected by California's civil rights law. *Cal. Civ. Code 56.181(a)(2)(E)(ii), (iii)*
- `gipa-security-and-rights` (technical) Protect genetic data with reasonable security, and let users easily see their genetic data, delete their account and genetic data (except what the law requires you to keep), and have their biological sample destroyed. *Cal. Civ. Code 56.181(d)*
- `gipa-no-insurer-employer-disclosure` (process) Never disclose genetic data to anyone who administers or decides on health, life, long-term care or disability insurance or employment, or who advises them, unless that company isn't mainly in those businesses, doesn't receive it in that role, and keeps its insurance and employment staff from accessing it. *Cal. Civ. Code 56.181(f)*
- `gipa-no-discrimination` (process) Don't deny service, charge more, give a worse service, suggest either, or treat someone as suspect of wrongdoing because they used their genetic-privacy rights. *Cal. Civ. Code 56.181(e)*
- `gipa-service-provider-contracts` (vendor/contract) Contracts with labs and others that collect, transport or analyse samples or deliver results for you must forbid them to keep, use or disclose the sample, the genetic data or the user's identity (including whether they sought or had a test) for anything but the contracted services, or to combine any of it with other data. *Cal. Civ. Code 56.18(b)(10)*

Parts of this law handled outside the obligations above

- Cal. Civ. Code 56.102 (Pharmaceutical companies): not covered by this report. Covers pharmaceutical companies, which this report doesn't ask about.
- Cal. Civ. Code 56.104 (Requests for outpatient psychotherapy information): see "If this happens".
- Cal. Civ. Code 56.106 (Mental health records of minors removed from parental custody): see "If this happens".
- Cal. Civ. Code 56.107 (Health care service plans: sensitive services and confidential communications): not covered by this report. Covers health care service plans licensed in California. This report doesn't ask whether your company is one.
- Cal. Civ. Code 56.108 (Abortion information: subpoenas and out-of-state requests): see "If this happens".
- Cal. Civ. Code 56.109 (Gender-affirming care information: subpoenas and out-of-state requests): see "If this happens".
- Cal. Civ. Code 56.16 (Hospitals' release of general patient information): not covered by this report. Covers general acute care hospitals answering inquiries about a patient.
- Cal. Civ. Code 56.17 (Health plans' disclosure of genetic test results): not covered by this report. Covers health care service plans disclosing genetic test results in members' records.
- Cal. Civ. Code 56.20 (Employers: confidentiality of employees' medical information): not covered by this report. Covers employers' handling of their own employees' medical information. This report assesses the app's users, not your staff.
- Cal. Civ. Code 56.21 (Employers: authorizations): not covered by this report. Covers employers' handling of their own employees' medical information. This report assesses the app's users, not your staff.
- Cal. Civ. Code 56.22 (Employers: copies of authorizations): not covered by this report. Covers employers' handling of their own employees' medical information. This report assesses the app's users, not your staff.
- Cal. Civ. Code 56.23 (Employers: telling recipients the limits): not covered by this report. Covers employers' handling of their own employees' medical information. This report assesses the app's users, not your staff.
- Cal. Civ. Code 56.24 (Employers: cancelling authorizations): not covered by this report. Covers employers' handling of their own employees' medical information. This report assesses the app's users, not your staff.
- Cal. Civ. Code 56.245 (Employers: recipients may not disclose further): not covered by this report. Covers employers' handling of their own employees' medical information. This report assesses the app's users, not your staff.
- Cal. Civ. Code 56.26 (Administrators of health payment programs): not covered by this report. Covers companies administering programs that pay for health care, which this report doesn't ask about.
- Cal. Civ. Code 56.265 (Insurers: no health information for credit decisions): not covered by this report. Covers insurers and annuity sellers, which this report doesn't ask about.

- Cal. Civ. Code 56.35 (Patients' right to sue): see "If this happens".
- Cal. Civ. Code 56.36 (Misdemeanor; nominal damages; fines and penalties; affirmative defense): see "If this happens".

What to know: The CMIA has no size threshold and covers nonprofits: a small mood, symptom, cycle or therapy app with California users, or run by a company based in California, can owe its duties from its first user. It treats apps designed to keep health information so people can manage it, or to help diagnose, treat or manage a condition, and mental health and reproductive or sexual health digital services, as health care providers; from 1 January 2027 health care chatbots join them. For the CMIA only: under the CCPA they aren't providers, so this report treats their health data as covered by both laws. The core rule is permission first: no disclosure of medical information without the user's signed authorization unless the law requires or allows it. An authorization has a strict form (14-point type, separate from other text, its own signature, specific uses, an expiry of at most a year), so accepting your terms of use doesn't count, and you can't make signing one a condition of using the app. Ad tags, and analytics tags whose vendors use the data for their own purposes, are disclosures that need authorization; so is sending health information to an AI provider that keeps it or trains on it. Training your own AI models on users' health information also needs their authorization, because it isn't needed to care for that user. Where information is negligently released, each affected person can claim $1,000 without proving harm, and class actions over tracking tags on health websites and apps have relied on the CMIA. HIPAA doesn't displace the CMIA: a clinic's vendor keeping patient records owes both, including, for abortion, contraception and gender-affirming care information, safeguards against access from other states. Information about abortion is protected from disclosure to anyone in another state, with narrow exceptions. The CMIA's duties for employers, health plans, insurers, pharmaceutical companies and payment administrators aren't assessed here, nor is patients' right to see licensed providers' records under California's Patient Access to Health Records Act.

Sources:
https://leginfo.legislature.ca.gov/faces/codes_displayexpandedbranch.xhtml?tocCode=CIV&division=1.&title=&part=2.6.&chapter=&artic · https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260AB1979 · https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260AB2448

Children's Online Privacy Protection Act (COPPA) and COPPA Rule (`us-coppa`)

Citation: 15 U.S.C. 6501-6506; 16 CFR Part 312 (as amended 2025) · **Jurisdiction:** US-federal · **Size threshold:** none · **Private right of action:** no · **Confidence:** high · **Legal status:** in force, effective 2000-04-21 (checked 2026-10-23)

Requires operators of online services directed to children under 13, or operators with actual knowledge that they collect personal information from a child under 13, to give notice to parents and obtain verifiable parental consent before collecting, using or disclosing children's personal information.

Unresolved: answer these to decide

- **Unknown**: Some of the app's users are under 13 *(answered unknown)*

If it does apply, its principal obligations would include

- `coppa-notice` (document) Before collecting, give parents direct notice of what you collect from their child, how you use it and whom you disclose it to, that their consent is required and nothing will be collected without it, and how to consent; give fresh notice of any material change. Post a prominent, clearly labelled link to an online notice of your children's information practices on your home or landing screen and at every place you collect children's information, stating every operator's name, address, phone number and email, what you collect and how you use and disclose it (naming third parties or their categories and why), your written data retention policy, any persistent identifiers you use only for internal operations, how you use any recordings of children's voices and that you delete them immediately, and how parents can review, delete and stop further collection. *16 CFR 312.4*
- `coppa-verifiable-parental-consent` (technical) Get verifiable parental consent before collecting, using or disclosing a child's personal information, and again for any material change you make. Use a method reasonably calculated to make sure the person consenting is the parent, such as a signed form, a card payment with transaction notice, a call or video call with trained staff, checking ID against a database (then deleting it), knowledge-based questions a child couldn't

answer, or a photo-ID match; email or text plus a follow-up step only if you don't disclose the child's information. The rule allows a few narrow exceptions, such as collecting a parent's contact details only to ask for consent, and deleting them if consent doesn't follow. For voice features: you may record a child's voice, with no other personal information, without parental consent only to respond to that child's specific request, and only if you don't use or disclose the recording for anything else and delete it immediately after responding. *16 CFR 312.5(a)(1), (b), (c), including (c)(9)*

- `coppa-separate-consent-third-party` (technical) Let parents consent to collection and use without consenting to disclosure to third parties, unless disclosure is integral to the service, and get separate verifiable consent before any such disclosure. *16 CFR 312.5(a)(2)*
- `coppa-parental-review-delete` (technical) On a parent's request, after making sure they are the child's parent: describe the kinds of personal information you collect from children, let them review what you collected from their child, and let them at any time refuse further use or collection and have it deleted. You may then end the child's service, within the limit on conditioning participation. *16 CFR 312.6*
- `coppa-no-conditioning` (process) Don't make a child's participation in a game, prize or other activity depend on their giving more personal information than is reasonably necessary for it. *16 CFR 312.7*
- `coppa-security-program` (process) Keep a written information security program for children's personal information, suited to its sensitivity and to your size and activities: name someone to coordinate it, assess internal and external risks at least once a year, put safeguards in place for those risks, regularly test and monitor them, and review and update the program at least once a year. *16 CFR 312.8(b)*
- `coppa-reasonable-security` (technical) Keep reasonable procedures to protect the confidentiality, security and integrity of children's personal information. *16 CFR 312.8(a)*
- `coppa-vendor-assurances` (vendor/contract) Before letting other operators, service providers or third parties collect or keep children's personal information for you, or before giving it to them, take reasonable steps to check they can protect it, and get their written assurance that they will. *16 CFR 312.8(c)*
- `coppa-retention-policy` (document) Keep children's personal information only as long as reasonably necessary for the purpose you collected it for, never indefinitely, and then delete it securely. Keep a written retention policy stating why you collect it, why you keep it and when you delete it, and include it in your online notice. *16 CFR 312.10*

Recommended, not duties under this law

- `coppa-age-check-intake` **Be ready to receive age-check results from app stores and age-verification services.** App stores, phone operating systems and age-verification services can now tell an app a user's age group. An app that receives that result knows when a user is under 13, which brings COPPA in for that user. Texas already requires apps offered there through an app store to use the store's age information and to delete it once the check is done (Tex. Bus. & Com. Code 121.054-121.055), and from 1 January 2027 California requires apps to request an age signal from the device's operating system or app store (Cal. Civ. Code 1798.501). The COPPA Rule requires a service aimed partly at children to ask ages neutrally, without defaulting to an age or encouraging false answers (16 CFR 312.2, mixed audience). *16 CFR 312.2, 312.3; Tex. Bus. & Com. Code 121.054-121.055; Cal. Civ. Code 1798.501 (from 1 Jan 2027)*

What to know: In law, COPPA has two triggers: the service is directed to children under 13, or the operator has actual knowledge that it collects personal information from a specific child under 13. To be safe, this report asks one broader question and treats any users under 13, known or expected, as bringing COPPA in. Having no age gate does not by itself trigger COPPA, and general-audience apps are not required to add one. But once an age field, a support message, an app-store review or an app-store age signal tells you a particular user is under 13, you have actual knowledge for that user. Some states, including Texas (currently enforceable while a court challenge continues), now require app stores to pass age signals to developers. 'Directed to children' is judged on factors including subject matter, visual content, animated characters, child-oriented activities, music, advertising, audience composition and marketing, and since 2025 also marketing plans, representations to third parties, reviews, and the ages of users of similar services. A service aimed partly but not mainly at children (mixed audience) may screen ages neutrally and treat users not identified as under 13 as adults. Persistent identifiers such as cookies, device IDs and IP addresses are personal information, so ad or analytics tags in a child-directed app collect it; that needs parental consent unless the identifier is used only to support the app's internal operations, such as contextual ads, measuring how the app works or security, never behavioural advertising or profiling. Biometric identifiers, including genetic data, are personal information since 2025. Letting a child post anything identifiable publicly counts as

collecting and disclosing under COPPA. An app avoids this only if it removes the identifying details before the post goes public. COPPA's definition of operator excludes nonprofits that are outside the FTC's authority, which covers most charities, though not nonprofits that work for their members' profit or that operate for profit in practice. To be safe, this report still lists COPPA's duties for nonprofit operators. The FTC and state attorneys general enforce COPPA; individuals cannot sue under it. Answer 'unknown' honestly: if you have never checked your support inbox or reviews for users who say they are children, you don't know yet.

Sources: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312 · https://www.law.cornell.edu/uscode/text/15/chapter-91 · https://www.federalregister.gov/documents/2025/04/22/2025-05904/childrens-online-privacy-protection-rule

B.3 Considered, unlikely to apply

HIPAA (covered entities and business associates) (`us-hipaa`)

Citation: 45 CFR Parts 160 and 164 (Privacy, Security and Breach Notification Rules); definitions at 45 CFR 160.103 · **Jurisdiction:** US-federal · **Size threshold:** none · **Private right of action:** no · **Confidence:** medium · **Legal status:** in force, effective 2003-04-14 (checked 2026-10-05)

HIPAA binds covered entities (health plans, health care clearinghouses, and health care providers that conduct standard electronic transactions such as insurance billing) and their business associates: anyone who creates, receives, keeps or transmits protected health information on a covered entity's behalf. Building or running a patient portal, telehealth or remote-monitoring app for a clinic usually makes you a business associate. Most direct-to-consumer wellness apps are neither.

Why it is unlikely to apply

- **No**: The organization offering the app is a HIPAA covered entity (a health plan, a health care clearinghouse, or a health care provider that conducts standard electronic transactions such as insurance billing) *(declared)*
- **No**: The app creates, receives, keeps or transmits health information on behalf of a HIPAA covered entity, directly or as a subcontractor of one of its vendors (a business associate role) *(declared)*

Findings that need attention

- **[HIGH] Tracking tags may be disclosing patient data** (not ruled out). Advertising and analytics tags on screens where patients are logged in, or inside the app, can send PHI to the tag's vendor. HHS guidance treats that as an impermissible disclosure unless the vendor has signed a BAA or patients have authorized it. A 2024 court decision (AHA v. Becerra) limited the guidance only for public pages patients aren't logged into.
- **[HIGH] Patient data sent to an AI provider needs a BAA** (identified). An AI provider that receives PHI for you is your subcontractor. You need a signed BAA covering the exact API product you use, and terms that bar training on the data. Not every AI provider or plan offers one.

What to know: HIPAA follows the relationship, not the data. A consumer who downloads your app and types in their own diagnosis, or uploads a record from their own doctor, does not make you a covered entity or a business associate. You become a business associate when you work on behalf of a covered entity: building and running a clinic's patient portal, telehealth or remote-monitoring app usually does it, and so does hosting or processing its patient data. Since 2013, business associates are directly liable for Security Rule failures and impermissible disclosures; the agreement with the clinic is not the only source of duty. Every vendor that touches the PHI for you is in turn your subcontractor and needs a BAA: hosting and database (on Supabase, only through its HIPAA add-on, which is not available on every plan; check current terms), file storage, email, error logging, analytics and AI providers. Most advertising and analytics tools won't sign one, so they can't be used where patients are logged in. Providers paid only by patients, who never send insurance claims or eligibility checks electronically (themselves or through a billing company), are usually not covered entities. Many online therapy and telehealth startups fall here: HIPAA probably doesn't apply to them, but the FTC Health Breach Notification Rule and state health-data

laws can. In the other direction, a hosting provider that stores PHI is a business associate even when the data is encrypted and it holds no key (HHS cloud computing guidance, 2016), so your database host needs a BAA regardless. Mixed cases are common: the same company can be a business associate for its clinic product and outside HIPAA for a direct-to-consumer app, and then this rule and the consumer-health rules can both apply, to different data. Using PHI to build analytics or train AI models is itself a use of PHI: a business associate needs its BAA to allow it, and data stops being PHI only when de-identified by HIPAA's safe-harbor or expert-determination method (45 CFR 164.514(a)-(b)). HIPAA sets a floor: stricter state medical-privacy laws still apply alongside it (45 CFR 160.203). Many Security Rule safeguards (encryption, automatic logoff) are 'addressable': you must implement them or document why an equivalent measure is reasonable.

Sources: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-160/subpart-A/section-160.103 · https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164 · https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html · https://www.hhs.gov/hipaa/for-professionals/special-topics/health-apps/index.html · https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html · https://hklaw.com/en/insights/publications/2024/06/american-hospital-assn-v-becerra-are-tracking-tools-ok-again · https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-pro · https://www.hhs.gov/guidance/document/are-you-covered-entity · https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html

California Consumer Privacy Act (as amended by the CPRA) (`us-ca-ccpa`)

Citation: Cal. Civ. Code 1798.100-1798.199.100; Cal. Code Regs. tit. 11, 7000-7304 · **Jurisdiction:** US-CA · **Size threshold:** yes · **Private right of action:** yes · **Confidence:** medium · **Legal status:** in force, effective 2020-01-01 (checked 2026-11-01)

Gives California residents rights over their personal information: to know, delete and correct it, to opt out of its sale or sharing, and to limit the use of sensitive information such as health data. It covers for-profit businesses that meet one of three size tests (revenue, the number of people whose data is bought, sold or shared, or the share of revenue from selling or sharing data), the vendors that handle data for them, and, for one narrow rule, anyone holding deidentified patient information. Its regulations add risk assessments, cybersecurity audits and rules on automated decisions.

Why it is unlikely to apply

- **No**: Annual gross revenue last year was more than $26,625,000 (the threshold as adjusted from 1 January 2025) *(declared: 0)*
- **No**: The operator sells personal information *(declared)*
- **No**: The app or its site uses advertising tags, which the CCPA treats as sharing for cross-context behavioural advertising *(declared)*
- **No**: The personal information of 100,000 or more California consumers or households is handled each year *(declared: 1,200)*
- **No**: 50% or more of annual revenue comes from selling or sharing personal information *(declared: 0)*
- **No**: The company handles health or wellness data for another business's app or service, as its vendor *(declared)*
- **No**: The app handles patients' data for a HIPAA covered entity *(declared)*
- **No**: The operator is a HIPAA covered entity *(declared)*

What to know: Most small apps fall outside the CCPA, and saying so plainly is half the value here. The revenue test uses the company's total gross revenue for the previous calendar year, wherever it was earned: more than $26,625,000 since 1 January 2025, adjusted every two years. The 100,000 figure counts California consumers or households whose personal information you buy, sell or share, not everyone you collect from. This report treats advertising tags such as the Meta Pixel as sharing, so visitors to a website or app with an ad tag count too, and the number can exceed your registered users. An app with no revenue doesn't meet the 50%-of-revenue test. Nonprofits are generally outside the definition of a business, though anyone holding HIPAA-deidentified patient information must not reidentify it (1798.148). Health data, precise location (within 1,850 feet), genetic and neural data, and, under the regulations, data of consumers you know are under 16 are

sensitive personal information. Since 1 January 2026, processing it needs a documented risk assessment, so nearly every covered health app needs one; for processing already under way, by 31 December 2027. For an app, the CCPA's 'homepage' includes the app-store download page and the app's settings, so required links belong there. A cookie banner isn't an opt-out, and a business that sells or shares must honour Global Privacy Control. HIPAA protected health information is exempt, but only that data: a clinic vendor's consumer-side data is covered. Patient information held by or for a health care provider or clinic licensed in California is medical information under California's Confidentiality of Medical Information Act (CMIA), which the CCPA exempts. Apps that the CMIA only treats as providers for its own purposes (health-tracking apps, mental health and reproductive health digital services, and from 1 January 2027 health care chatbots) aren't providers under the CCPA, so this report treats their health data as covered by both laws. From 1 January 2027 the right to delete reaches data you got about a person from anywhere, not only from them, and online-only businesses must offer a web form as well as email. The private right of action covers only breaches caused by failing to keep reasonable security (1798.150). Terms that waive CCPA rights are void (1798.192), and steps taken to avoid the definitions of sale or sharing are disregarded (1798.190). The CCPA also covers your employees', job applicants' and business contacts' data; this report assesses only the app's users. A business that buys or receives personal information sold or shared by another business has further duties (1798.115(d)), which this report doesn't assess. Falling outside the CCPA doesn't put you outside California law: the Confidentiality of Medical Information Act and the companion chatbot law (SB 243) have no size thresholds.

Sources:
https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article= · https://cppa.ca.gov/regulations/pdf/ccpa_statute_eff_20260101.pdf · https://cppa.ca.gov/regulations/cpi_adjustment.html · https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260SB923 · https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260AB1979

Appendix C. Technical controls

C.1 Cannot be added later

These cost little on day one and cannot be bought back later at any price. Every day without them adds to a gap that can't be closed afterwards.

- **Versioned consent capture** (`consent-capture-versioned`, IMPLEMENTED): Consent never recorded cannot be reconstructed. You can start capturing it for new users immediately, but existing users stay without a record unless re-prompted, and re-consent campaigns reach only part of a user base.
- **Third-party disclosure inventory and gate** (`third-party-disclosure-gate`, PENDING): Data already sent to a third party cannot be recalled. You can stop future flows, but past disclosures remain, and under some rules they may already count as a breach that has to be notified.
- **Access and change audit log** (`audit-logging`, PENDING): Logs never switched on cannot be backfilled. Nobody can reconstruct who accessed what before logging began, and that affects both detection and how narrowly a breach can be scoped.

C.2 Status

Control	Status	Can be added later?	Recommended for
Access and change audit log (`audit-logging`)	PENDING	**no**	`hbnr-breach-discovery`, `mhmda-data-security`

Control	Status	Can be added later?	Recommended for
Versioned consent capture (`consent-capture-versioned`)	IMPLEMENTED	**no**	`hbnr-authorized-disclosure`, `mhmda-consent-to-collect`, `mhmda-consent-to-share`, `mhmda-new-purposes-need-consent`, `mhmda-withdraw-consent`
Third-party disclosure inventory and gate (`third-party-disclosure-gate`)	PENDING	**no**	`hbnr-authorized-disclosure`, `mhmda-consent-to-share`
Contact-preference record for breach notices (`contact-preference-record`)	PENDING	yes	`hbnr-contact-preference`
Data subject request intake and tracking (`data-subject-request-intake`)	IMPLEMENTED	yes	`mhmda-request-handling`, `mhmda-right-to-access`, `mhmda-right-to-delete`, `mhmda-withdraw-consent`
Account deletion cascade (`deletion-cascade`)	IMPLEMENTED	yes	`mhmda-right-to-delete`
Row-level access control (`row-level-access-control`)	IMPLEMENTED	yes	`mhmda-data-security`, `mhmda-restrict-access`
Sensitive data segregation (`sensitive-data-segregation`)	IMPLEMENTED	yes	`mhmda-data-security`, `mhmda-restrict-access`

PENDING means the control is specified but this library version provides no code. It must not be treated as done.

C.3 Controls that may be needed

Recommended only if the open questions resolve that way.

- **Opt-out of sale and sharing (including Global Privacy Control)** (`sale-share-opt-out`, PENDING): via `ct-opt-out`
- **Minors' precise location: only when strictly necessary, with a visible signal** (`minor-location-limits`, PENDING): via `ct-minors-location`
- **Safe-by-default design for minors: fair consent screens, messaging safeguards, no engagement-maximising features** (`minor-safe-design`, PENDING): via `ct-minors-design`
- **Multi-factor authentication for sensitive data** (`mfa-for-sensitive-access`, IMPLEMENTED): via `cmia-confidential-storage`
- **Verifiable parental consent** (`parental-consent-verification`, PENDING): via `coppa-separate-consent-third-party`, `coppa-verifiable-parental-consent`

C.4 Control detail

Offered as a starting point, not warranted. Test every control in your own environment before relying on it.

Access and change audit log (`audit-logging` v1): PENDING

Keep a tamper-resistant record of who read, changed or exported sensitive data, and of administrative actions, without copying the sensitive values into the log.

Why it matters: Breach notification deadlines can start from when you should reasonably have known. Without access logs you can neither detect a breach promptly nor show who was affected, which pushes toward notifying everyone.

Implementation: none in this library version (PENDING). Do not treat as done.

How to check it: Read a health record as a test user and as an admin, then export it. Confirm each event appears in the log with actor, time, action and record id, but without the health values themselves. Confirm an ordinary user cannot read or delete log rows.

Common mistakes: - Logging writes but not reads or exports - Keeping logs in a table users (or the app's public key) can delete - Copying the sensitive values into the log, creating a second copy to protect - No retention period, or one shorter than the look-back a breach investigation needs - On Supabase: assuming triggers capture reads. They don't; reads need the pgaudit extension or application-level logging.

Why it cannot be added later: Logs never switched on cannot be backfilled. Nobody can reconstruct who accessed what before logging began, and that affects both detection and how narrowly a breach can be scoped.

Versioned consent capture (`consent-capture-versioned` v1): IMPLEMENTED

Record that a specific user agreed (or withdrew) for a specific purpose, under a specific version of the text they were shown, at a specific moment, in a form you can produce as evidence later.

Why it matters: Several rules require consent you can demonstrate, not merely claim, and some require separate consents for separate purposes (collecting health data versus sharing it). A boolean 'accepted_terms' column proves nothing about what was agreed, when, or under which policy text.

Implementation (postgres_supabase): `controls/consent-capture-versioned/supabase.sql`. Append-only table plus a current-consent view and a has_current_consent() helper. A withdrawal is a new row, never an UPDATE. Timestamps are set by the database, not the client. *Executed against PostgreSQL 16.15 (postgres:16-alpine) with a Supabase roles/auth stub, not a live Supabase project; applied twice and behaviour-checked by verification/supabase/run.py on 2026-09-30.*

How to check it: As a test user: insert a 'granted' consent for one purpose, then a 'withdrawn' one. Query current_consent and confirm it shows 'withdrawn'. Then try to UPDATE or DELETE a consent row as that user and confirm both are refused. Finally, insert a row with a recorded_at in the past and confirm the stored time is the actual insert time.

Common mistakes: - A single boolean with no timestamp, purpose or policy version - Updating the consent row when terms change, which destroys the earlier record - One blanket consent where a rule requires separate consent per purpose (collection vs sharing) - Trusting a timestamp sent by the client - Recording consent after the data has already been collected or sent

Why it cannot be added later: Consent never recorded cannot be reconstructed. You can start capturing it for new users immediately, but existing users stay without a record unless re-prompted, and re-consent campaigns reach only part of a user base.

Contact-preference record for breach notices (`contact-preference-record` v1): PENDING

Let each user choose whether email is their primary way to hear from you, store that choice with the date it was made, and, for users who don't choose email, collect a postal address, so a breach notice can reach everyone by a method the rule allows.

Why it matters: Under the FTC rule, a breach notice may go by email only to people who chose email as their primary contact method; everyone else must get a letter at their last known address. Apps that never ask can't send a lawful email notice, and often have no postal address either.

Implementation: none in this library version (PENDING). Do not treat as done.

How to check it: Sign up as a new test user and confirm you're asked for a contact preference. Choose email and confirm the choice and its date are stored; choose not to and confirm you're asked for a postal address. Change the preference and confirm the new choice and date are stored, with the earlier choice kept in its history.

Common mistakes: - Treating the sign-up email address as consent to receive breach notices by email - Pre-ticking the email choice - Storing the choice without its date, so you can't show when it was made - Collecting no postal address at all, leaving no lawful way to notify users who didn't choose email - Losing the record when a user changes their preference

Adding it later: Can be added at any time, but existing users haven't chosen yet: until each one does, a notice to them has to go by post, so ask existing users soon.

Data subject request intake and tracking (`data-subject-request-intake` v1): IMPLEMENTED

A single place where requests to access, delete, correct or withdraw consent are received, dated, assigned a deadline from the rules that apply to you, and tracked to completion.

Why it matters: Rights requests come with legal deadlines, and you have to be able to show you met them. Requests that arrive by email and live in someone's inbox are how deadlines get missed. Deadlines vary by rule, so none is assumed here.

Implementation (postgres_supabase): `controls/data-subject-request-intake/supabase.sql`. Requests table with no default deadline (R10): set due_at from the deadlines listed in your assessment record. Views list open requests with no deadline set and overdue requests. Requests from people without accounts should be inserted by an Edge Function using the service role. *Executed against PostgreSQL 16.15 (postgres:16-alpine) with a Supabase roles/auth stub, not a live Supabase project; applied twice and behaviour-checked by verification/supabase/run.py on 2026-09-30.*

Deadlines: set each request's `due_at` from the deadlines in D.4. No default is assumed.

How to check it: As a test user, submit a deletion request and confirm it appears with status 'received' and no due_at. Confirm the user cannot change its status or deadline. As staff (service role), set due_at from your record's deadline table, then move a test request past its due date and confirm it appears in dsr_overdue.

Common mistakes: - Hardcoding one deadline (such as 45 days) for every request type and every law - Letting the requester edit the status of their own request - Deleting the request record together with the account, which leaves no evidence the request was honoured - No identity verification step before disclosing or deleting data - Handling requests only for logged-in users when people without accounts (such as tracked visitors) can make them too

Adding it later: Can be added at any time, but requests received before the log existed cannot be evidenced afterwards.

Account deletion cascade (`deletion-cascade` v1): IMPLEMENTED

When a user's account is deleted, every row that belongs to them is deleted with it automatically, so nothing is left behind in tables someone forgot about.

Why it matters: Deletion rights are only real if deletion is complete. Apps grow tables over time, and a hand-written 'delete account' routine silently misses the new ones. Foreign keys with ON DELETE CASCADE make completeness structural.

Implementation (postgres_supabase): `controls/deletion-cascade/supabase.sql`. Audits for non-cascading and missing foreign keys to auth.users, plus a private.cascade_user_fk() helper. Trigger account deletion server-side with supabase.auth.admin.deleteUser() from an Edge Function after re-authenticating the user; never expose the service-role key

to the client. Foreign keys do not delete Storage files (uploads, avatars): delete those in the same function. Backups and third parties are covered by separate obligations. *Executed against PostgreSQL 16.15 (postgres:16-alpine) with a Supabase roles/auth stub, not a live Supabase project; applied twice and behaviour-checked by verification/supabase/run.py on 2026-09-30.*

How to check it: Create a test user and give them rows in every user-owned table (and a Storage upload). Delete the user through your real deletion path. Count that user's rows in each table (all must be 0) and confirm the upload is gone. Re-run both audit queries: no rows.

Common mistakes: - Deleting the profile row but not auth.users (or the reverse) - New tables added later without the cascade - Forgetting Storage objects, analytics profiles, email-tool contacts and AI-provider logs - ON DELETE SET NULL on tables that hold the user's content, which leaves the content behind anonymously but not deleted - Treating deletion from the live database as deletion from backups

Adding it later: Cascades can be added later, but adding a foreign key fails if orphaned rows from earlier deletions already exist. Those rows are data you were supposed to have deleted. Find and remove them first.

Row-level access control (`row-level-access-control` v1): IMPLEMENTED

Make the database itself refuse to return one user's rows to anyone else, instead of relying on the app's front end to filter them.

Why it matters: In Supabase and similar backends the browser talks to the database directly. A table without row-level security in an exposed schema can be read in full by anyone holding the public key, which ships inside every copy of your app. Tables named profiles, entries and chat_messages are exposed this way in vibe-coded apps all the time.

Implementation (postgres_supabase): `controls/row-level-access-control/supabase.sql`. Audit queries (tables without RLS, tables with RLS but no policies, allow-everyone policies) plus a private.apply_owner_only_policies() helper that enables RLS and adds owner-only policies in one step. *Executed against PostgreSQL 16.15 (postgres:16-alpine) with a Supabase roles/auth stub, not a live Supabase project; applied twice and behaviour-checked by verification/supabase/run.py on 2026-09-30.*

How to check it: Run the audit queries: the first must return no rows. Then, from the browser console of your running app while signed in as user A, query user B's rows through the Supabase client and confirm none come back. Repeat signed out.

Common mistakes: - RLS enabled but a policy of using (true) that lets everyone read everything - Policies that check user_metadata, which users can edit themselves - Shipping the service_role key in front-end code (it bypasses RLS entirely) - Views over protected tables that run with the owner's rights and bypass RLS (see sensitive-data-segregation) - No index on the owner column, making every policy check a full scan

Adding it later: It can be added to a live app, but enabling row-level security on a table denies all access until policies exist, so existing queries break unless policies go in within the same migration. Test on a branch first. Data already exposed before the fix may have been read, and you can't tell without logs.

Sensitive data segregation (`sensitive-data-segregation` v1): IMPLEMENTED

Keep health data in its own tightly-guarded table, never mixed into widely-read tables like profiles, and make sure no view or function quietly exposes it.

Why it matters: Health data in a general table inherits that table's loosest access rule. Two Supabase patterns leak it even with row-level security on. Views run with their owner's rights unless told otherwise. SECURITY DEFINER functions in the public schema can be called by anyone.

Implementation (postgres_supabase): `controls/sensitive-data-segregation/supabase.sql`. A segregated health_entries table pattern with owner-only access, plus audits for RLS-bypassing views, materialized views, exposed SECURITY DEFINER functions, and health-like columns living outside the segregated table. *Executed against PostgreSQL 16.15 (postgres:16-alpine) with a Supabase roles/auth stub, not a live Supabase project; applied twice and behaviour-checked by verification/supabase/run.py on 2026-09-30.*

How to check it: Run the four audit queries. The view audit and the function audit must return no rows (or only ones you have deliberately reviewed), and the column audit must not list health data outside the segregated table. Then, signed in as user A, confirm you can't read user B's health entries through any table, view or RPC.

Common mistakes: - Storing mood or symptoms as columns on profiles, which is often readable by other users for display names - Creating a view for a dashboard without security_invoker, which exposes every user's rows - Materialized views over health data in the public schema (these cannot enforce RLS at all) - Helper functions declared SECURITY DEFINER in public and callable through the API - Logging full request bodies containing health data to a third-party logging service

Adding it later: Moving live data is a migration with downtime risk, and health data already copied into logs, analytics events or backups stays there after you move it.

Third-party disclosure inventory and gate (`third-party-disclosure-gate` v1): PENDING

Keep a list of every outside service that receives user data (ad pixels, analytics, session recording, AI APIs, email tools), and make sure health-related data reaches one only when the user has agreed to that recipient and purpose.

Why it matters: Several rules treat sending health data to a third party without authorization as a violation in itself; under the FTC Health Breach Notification Rule it is a breach of security. In vibe-coded apps these flows are often added by templates or marketing tags nobody reviewed.

Implementation: none in this library version (PENDING). Do not treat as done.

How to check it: Open the app in a browser with developer tools on the Network tab. Using a test account, enter some health information (for example a symptom, a mood or an appointment) and filter requests for facebook, google, tiktok, segment, mixpanel, posthog, hotjar, clarity and your AI provider. For each request, check whether page URLs, page titles, event names or payloads reveal health information. Withdraw consent and repeat: no request should then carry health information.

Common mistakes: - Ad pixel on logged-in pages whose URLs or titles reveal health information (for example /log/anxiety) - Custom events named after health actions ('logged_depression_entry') sent to ad platforms - Session recording capturing typed journal text - Treating the AI provider as 'just an API' without reading its retention and training terms - Consent banner that records a choice but tags fire before it loads

Why it cannot be added later: Data already sent to a third party cannot be recalled. You can stop future flows, but past disclosures remain, and under some rules they may already count as a breach that has to be notified.

Multi-factor authentication for sensitive data (`mfa-for-sensitive-access` v1): IMPLEMENTED

Require a second sign-in factor before anyone can read or change sensitive data, enforced by the database rather than by the app's screens.

Why it matters: Stolen passwords are the most common way into health data. HIPAA requires verifying the identity of anyone accessing PHI, and multi-factor authentication is a strong way to do it.

Implementation (postgres_supabase): `controls/mfa-for-sensitive-access/supabase.sql`. A private.require_mfa() helper adds a restrictive policy so a table is usable only with a second-factor (aal2) session, on top of its other policies. Turn on MFA in Supabase Auth and enrol accounts before applying it. *Executed against PostgreSQL 16.15 (postgres:16-alpine)*

with a Supabase roles/auth stub, not a live Supabase project; applied twice and behaviour-checked by verification/supabase/run.py on 2026-10-03.

How to check it: Sign in with only a password and try to read the protected table: no rows come back and writes are refused. Complete the second factor and try again: access works. Run the audit query and check every table holding patient data has the MFA policy.

Common mistakes: - Checking MFA only in the front end, where calling the API directly skips it - Applying it to tables patients use before patients can enrol a second factor - Exempting admin or service accounts - Leaving text-message codes as the only second factor where stronger options exist

Adding it later: Can be added at any time. Accounts must enrol a second factor first, or they are locked out of the protected tables.

Minors' precise location: only when strictly necessary, with a visible signal (`minor-location-limits` v1): PENDING

For users you know, or have clear signs, are under 18, collect precise location only while a feature that cannot work without it is in use, stop as soon as that feature is done, and show the minor a visible signal for the whole time location is being collected.

Why it matters: Connecticut forbids collecting a minor's precise location unless strictly necessary to provide the service, only for as long as necessary, and only with a signal visible for the entire collection. Precise location is also sensitive data under the Act, and near a clinic it can reveal that someone is seeking care.

Implementation: none in this library version (PENDING). Do not treat as done.

How to check it: Sign in as a test user marked as under 18. Confirm the app doesn't ask for or collect location until you open a feature that can't work without it; that a visible indicator appears as soon as collection starts and stays for the whole time; and that collection stops when you leave the feature. Check that no analytics, advertising or crash-reporting library collects location for that user on its own.

Common mistakes: - Asking for background location during onboarding, before any feature needs it - Third-party libraries (analytics, ads, crash reporting) collecting location independently of the app's own code - Relying on the phone's one-time permission prompt as the signal: the law asks for a signal for the whole time - Using precise location where an approximate area would do: location coarser than a 1,750-foot radius isn't 'precise' under the Act - Keeping a location history after the feature that needed it has finished

Adding it later: Can be added at any time, but location already collected from minors without a strict need or without a signal can't be made compliant afterwards; consider deleting it.

Safe-by-default design for minors: fair consent screens, messaging safeguards, no engagement-maximising features (`minor-safe-design` v1): PENDING

For users under 18: present consent choices fairly, without pressure or tricks; if the app has direct messaging, stop adults who aren't already connected with a minor from messaging them, by default, with easy controls for the minor and their parent; and don't use design features meant to significantly increase, sustain or extend a minor's use of the app.

Why it matters: Connecticut prohibits manipulative consent mechanisms, unsafe direct messaging and use-extending design for online services that know, or wilfully disregard, that users are under 18. The Attorney General enforces it, and a documented assessment of risks to minors is required anyway.

Implementation: none in this library version (PENDING). Do not treat as done.

How to check it: As a test user marked as under 18: (1) on every consent screen, check that accepting and declining are equally easy and visible, nothing is pre-ticked, and declining isn't followed by repeated nagging; (2) if the app has direct messages, try to message the minor from a test adult account that isn't connected with them and confirm it's blocked, and that the minor and a parent can see and change the setting; (3) list every feature that encourages continued use (feeds, autoplay, streaks, reminders, re-engagement notifications) and confirm each is off for minors, or serves the minor's own stated purpose, such as a medication reminder they set themselves.

Common mistakes: - Messaging safeguards that exist but are off by default - Ignoring clear signs of age, such as a birth date under 18, which counts as wilful disregard - Re-engagement notifications or streak reminders sent to minors to bring them back - A highlighted 'accept' button next to a hidden or greyed-out 'decline' - Treating parental controls as an optional extra instead of the default

Adding it later: Can be added at any time; settings already on for minors should be switched to the safe default, not left as they are.

Verifiable parental consent (`parental-consent-verification` v1): PENDING

Before collecting a child's personal information, confirm that the person consenting is actually the parent, using a method the FTC accepts, and record that consent.

Why it matters: COPPA requires consent that is reasonably designed to verify parenthood. A checkbox saying 'I am the parent' is not enough.

Implementation: none in this library version (PENDING). Do not treat as done.

How to check it: Walk the sign-up flow as a child user: confirm no personal information beyond what the rule permits for seeking consent is stored before verified consent is recorded, and that the parent's consent record (method, time, what they were shown) exists afterwards.

Common mistakes: - A checkbox with no verification - Collecting the child's data first and asking for consent later - One consent covering third-party disclosures that now need separate consent - No way for the parent to review, revoke or delete later

Why it cannot be added later: A child's information collected without verifiable parental consent cannot be consented after the fact. In general it has to be deleted, and the collection itself is the violation.

Opt-out of sale and sharing (including Global Privacy Control) (`sale-share-opt-out` v1): PENDING

Let users stop you selling their data or sharing it for cross-context advertising, through a visible link and by honouring the browser's Global Privacy Control signal, and make the tags actually stop.

Why it matters: Where the CCPA applies, ad-pixel sharing needs an opt-out, and regulators have acted against sites whose opt-out link didn't stop the tags or that ignored Global Privacy Control.

Implementation: none in this library version (PENDING). Do not treat as done.

How to check it: In a browser with Global Privacy Control enabled (for example Firefox with the setting on, or a GPC extension), load the app and confirm in the Network tab that no ad-platform requests fire. Separately, click your opt-out link while GPC is off and confirm the same.

Common mistakes: - An opt-out link that records the preference but leaves the pixels running - Ignoring the Global Privacy Control signal - Requiring an account to opt out - Opt-out that resets when cookies are cleared, with no server-side record for signed-in users

Adding it later: Can be added at any time. Sharing that happened before users could opt out has already happened.

Appendix D. Obligations and how they are covered

Every principal obligation of every law that may apply is listed in exactly one place: 12 addressed by a technical control (see Appendix C for which are pending), 2 technical with no control, 11 outside your code, 5 not triggered by your facts. Total 30.

D.1 Technical obligations not addressed by any control

Nothing in this library addresses these in code yet. They are listed so they are not lost.

- **Washington My Health My Data Act:** `mhmda-no-geofencing` (technical) Do not set up a geofence within 2,000 feet of an in-person health care facility to identify or track people seeking care, collect health data, or send them health-related notifications or ads. *RCW 19.373.080; RCW 19.373.010(14)*
- **New York health-data protections (geofencing ban, abortion-referral reports, shield laws, police access):** `ny-no-geofencing` (technical) Don't set up a geofence or similar virtual boundary (a radius of 1,850 feet or less, drawn with GPS, cell, Wi-Fi, IP address or any other location data) around any health care facility other than your own, to send digital ads, build consumer profiles, or infer anyone's health status, condition or treatment; and don't deliver digital ads to people at or inside such a facility through a geofence. 'Health care facility' covers any provider of medical care or related services, including licensed mental health and addiction programs. *N.Y. Gen. Bus. Law 394-g(1)-(2)*

D.2 Obligations outside your code

A tool that reads code cannot do these for you. They need a person, a document, or a contract.

Process

- **FTC Health Breach Notification Rule:** `hbnr-notify-individuals` (process) After discovering a breach of security, notify each affected individual who is a US citizen or resident without unreasonable delay and within 60 calendar days. A law-enforcement official can require a delay. You don't have to wait until you know everything: the rule lets you send the notice in more than one mailing as information becomes available. *16 CFR 318.3(a)(1), 318.4(a), 318.4(d), 318.5(a)(1)*
- **FTC Health Breach Notification Rule:** `hbnr-notify-ftc` (process) Notify the FTC, using the instructions on its website. If 500 or more people are affected, do it at the same time as notifying individuals. If fewer are affected, you may instead keep a log of such breaches and send the year's log to the FTC within 60 calendar days after the end of the calendar year. *16 CFR 318.3(a)(2), 318.4(b), 318.5(c)*
- **FTC Health Breach Notification Rule:** `hbnr-notify-media` (process) If the information of 500 or more residents of one state or jurisdiction is, or is reasonably believed to have been, acquired, notify prominent media outlets serving it, without unreasonable delay and within 60 calendar days after discovery. *16 CFR 318.3(a)(3), 318.4(a), 318.5(b)*
- **FTC Health Breach Notification Rule:** `hbnr-notice-method` (process) Plan how a breach notice would reach every affected user. Notice by email must be clear and conspicuous and go with a text message, in-app message or banner. If contact details are missing or out of date for 10 or more people, post a substitute notice on your home page for 90 days or in major print or broadcast media, with a toll-free number that stays active for 90 days. If a user has died, notice goes to the next of kin they named and authorized you to contact. In urgent cases you may also phone people. *16 CFR 318.5(a); 318.2 (definitions of 'electronic mail' and 'clear and conspicuous')*
- **Washington My Health My Data Act:** `mhmda-appeals` (process) Run an appeal process for refused requests. Respond in writing with reasons, and if the appeal is denied, give the user a way to contact the Washington Attorney General. *RCW 19.373.040(1)(h)*
- **Washington My Health My Data Act:** `mhmda-no-discrimination` (process) Don't treat people worse because they used any right under the Act, for example by cutting features or refusing service after they ask to see, delete or withdraw their data. *RCW 19.373.030(1)(d)*

Document

- **FTC Health Breach Notification Rule:** `hbnr-notice-content` (document) Prepare breach notice content in plain language that covers what the rule lists: what happened, with the date of the breach and of its discovery; who acquired the information, if known (for example the advertising platform); the types of information involved, which can include the fact that someone used a health app; steps individuals should take; what you are doing to investigate, limit harm and protect them; and at least two ways to contact you (toll-free number, email, website, in-app or postal address). Drafting it for the first time during an incident makes omissions likely. *16 CFR 318.6*
- **FTC Health Breach Notification Rule:** `hbnr-notification-records` (document) Keep records showing that every notice you send under this rule (to individuals, the FTC and the media, or, as a service provider, to the business you serve) went out on time and by the required method, and the evidence for any delay, such as a law-enforcement request. The burden of proof is on you. *16 CFR 318.4(c), 318.4(d)*
- **Washington My Health My Data Act:** `mhmda-privacy-policy` (document) Publish a consumer health data privacy policy, prominently linked from your homepage, stating the categories of health data collected and why, the sources, the categories shared, who receives them, and how users exercise their rights. *RCW 19.373.020*

Vendor/contract

- **FTC Health Breach Notification Rule:** `hbnr-service-provider-terms` (vendor/contract) Tell each service provider that handles the health data for you (hosting, analytics, advertising, AI, support tools) that your app may be a vendor of personal health records or a PHR related entity under this rule, As good practice, also name in your contract the person who should receive their breach notices; otherwise they go to a senior official. The rule requires vendors to tell service providers their status, and requires service providers to report a breach to the vendor within 60 calendar days, identify the affected customers and get the vendor's acknowledgment. *16 CFR 318.3(b), 318.4(a)*
- **Washington My Health My Data Act:** `mhmda-processor-contracts` (vendor/contract) Let processors (hosting, AI, analytics vendors acting for you) handle consumer health data only under a binding contract that sets processing instructions and limits what they may do, and only in ways consistent with your privacy policy. *RCW 19.373.060; RCW 19.373.020(1)(e)*

D.3 Obligations not triggered by your facts

- **FTC Health Breach Notification Rule:** `hbnr-service-provider-notice` (process) If a business whose health data you handle is covered by this rule (as a vendor of personal health records or a PHR related entity), then after discovering a breach of that data, notify the official your contract names, or otherwise a senior official, at that business without unreasonable delay and within 60 calendar days. Identify each affected customer, and get the official's acknowledgment that the notice was received. Covered businesses must tell their service providers that they are covered, so ask each business you serve and keep its answer. *16 CFR 318.3(b), 318.4(a)* **Not triggered: No**: The company handles health or wellness data for another business's app or service, as its vendor *(declared)*
- **Washington My Health My Data Act:** `mhmda-sale-authorization` (technical) Do not sell consumer health data without a valid authorization signed by the user, containing the elements the Act lists. Authorizations expire after one year, and both seller and buyer must keep a copy for six years. Whether passing data to ad platforms is a 'sale' is unsettled. Treat it as a review question, not an assumption. *RCW 19.373.070* **Not triggered: No**: The operator sells user data or exchanges it for something of value *(declared)*
- **Washington My Health My Data Act:** `mhmda-processor-follow-contract` (vendor/contract) Handle another business's consumer health data only under a binding contract with that business that sets out its processing instructions and limits what you may do with the data, and only as those instructions allow. If you go beyond them, the Act treats you as a regulated entity for that data, with all of its duties. *RCW 19.373.060(1)(a), (1)(c)* **Not triggered: No**: The company handles health or wellness data for another business's app or service, as its vendor *(declared)*
- **Washington My Health My Data Act:** `mhmda-processor-assist` (process) Help each business whose consumer health data you handle to meet its duties under this Act, with appropriate technical and organizational measures as far as possible: for example, finding, exporting or deleting a person's data when the business receives a request, and keeping the data secure. *RCW 19.373.060(1)(b)* **Not triggered: No**: The company handles health or wellness data for another business's app or service, as its vendor *(declared)*

- **New York health-data protections (geofencing ban, abortion-referral reports, shield laws, police access):** `ny-abortion-referral-reports` (technical) Don't give anyone a report of a person being referred for abortion services, or of their inquiry or request for them, except: law enforcement (whose request must include a sworn statement that it is solely for law enforcement purposes, and is further limited by the warrant and shield rules), the New York State or New York City health department, someone the person authorized in writing, or under a court order. Every request must be in writing and give the requester's name and address. *N.Y. Gen. Bus. Law 394-e(1)* **Not triggered: No**: The app handles reproductive, sexual health or gender-affirming care information *(declared)*

D.4 Response and notification deadlines from laws that may apply

Taken from the laws themselves. Where several cover the same kind of request, meeting the shortest meets them all.

Obligation	Law	Deadline	Clock starts	Source
`mhmda-right-to-access`	Washington My Health My Data Act	45 days; extendable once by 45 days with notice	receipt of the request	RCW 19.373.040(1)(g)
`mhmda-withdraw-consent`	Washington My Health My Data Act	45 days; extendable once by 45 days with notice	receipt of the request	RCW 19.373.040(1)(g)
`mhmda-right-to-delete`	Washington My Health My Data Act	45 days; extendable once by 45 days with notice	receipt of the request	RCW 19.373.040(1)(g)
`mhmda-appeals`	Washington My Health My Data Act	45 days	receipt of an appeal	RCW 19.373.040(1)(h)
`hbnr-notify-individuals`	FTC Health Breach Notification Rule	60 days	discovery of a breach of security	16 CFR 318.4(a)
`hbnr-notify-ftc`	FTC Health Breach Notification Rule	60 days	the end of the calendar year, for breaches affecting fewer than 500 people that you log instead of reporting at once	16 CFR 318.4(b), 318.5(c)
`hbnr-notify-media`	FTC Health Breach Notification Rule	60 days	discovery of a breach of security	16 CFR 318.4(a)

Appendix E. Limitations and reproducing this report

- Facts marked 'declared' were supplied by the operator and were not independently verified. One wrong answer can change a determination.
- Facts marked 'observed' come from automated reading of the repository provided. It can miss things (tags injected at runtime by a tag manager, code in other repositories, production-only configuration). It can also find things that are present but unused. Observation adds evidence of presence only. It never proves absence. Where the code contradicts an answer, this report follows the code.

- Rules reflect the rule-library version stamped in the header. Laws, regulations and court orders change. Each rule's legal status shows when it was last checked.
- Obligations listed for each rule are its principal obligations, not an exhaustive list.
- This record is not legal advice. It does not create an attorney-client relationship, and unless stated otherwise it has not been reviewed by an attorney.
- Code and configuration referenced as controls are offered as starting points, not warranted. The operator must test them in their own environment before relying on them.

Reproducing this report: check out rule-library commit `d48c083bf67e5957e47f14c94549b23d03017e0e` and run the assessment again with the same answers file, `--as-of 2026-11-03`, and (if one was reviewed) the same repository state. The inputs fingerprint above must match.

Not legal advice

This report is general information, not legal advice, and it should not be relied on or treated as legal advice. It lists laws and rules that may potentially apply to the app, based on the answers given and any code reviewed. It does not state that any law does or does not apply, and it does not determine whether the app complies with any law. Using it does not create a lawyer-client relationship. Laws change, and how they apply depends on facts this report may not capture. Consult a qualified attorney before making legal decisions.