

Washington's My Health My Data Act and Other U.S. Health Data Regulation: Health and Health-ish Data Practices Under the Microscope

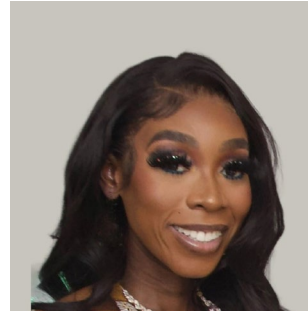
September 28, 2023
12:00 PM – 1:00 PM EST



Today's Speakers



Kyle R. Fath
Partner
Los Angeles | New York
Kyle.Fath@squirepb.com



Owobolade Shonowo
Senior Associate
Washington, D.C.
Owobolade.Shonowo@squirepb.com



Gicel Tomimbang
Associate
Los Angeles
Gicel.Tomimbang@squirepb.com

Why are we here?



AG Ferguson, Rep. Slatter bill creating health data privacy protections passes Legislature

FOR IMMEDIATE RELEASE:
Apr 17 2023



New state laws force families with trans kids to seek gender-affirming care elsewhere

Nation Jul 10, 2023 2:27 PM EDT



Governor Inslee Signs Washington My Health My Data Act Into Law: First-of-Its-Kind Consumer Health Data Law, Explained

The New York Times

In 6-to-3 Ruling, Supreme Court Ends Nearly 50 Years of Abortion Rights

The decision will lead to all but total bans on the procedure in about half of the states.



HEALTH

Families with transgender kids are increasingly forced to travel out of state for the care they need

(Slip Opinion)

OCTOBER TERM, 2021

1

Syllabus

NOTE: Where it is feasible, a syllabus (headnote) will be released, as is being done in connection with this case, at the time the opinion is issued. The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States v. Detroit Timber & Lumber Co.*, 200 U. S. 321, 337.

SUPREME COURT OF THE UNITED STATES

Syllabus

DOBBS, STATE HEALTH OFFICER OF THE MISSISSIPPI DEPARTMENT OF HEALTH, ET AL. *v.* JACKSON WOMEN'S HEALTH ORGANIZATION ET AL.

CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FIFTH CIRCUIT

No. 19–1392. Argued December 1, 2021—Decided June 24, 2022

The Washington Post

Arkansas federal judge blocks first ban on gender-affirming care

U.S. district judge in Arkansas issued a permanent injunction against a state law that banned trans youth and their families from seeking gender-affirming medical care

Forbes

BREAKING

Idaho Becomes First State To Restrict Interstate Travel For Abortion

- Health and Health-ish Data Landscape
 - HIPAA in comparison to MHMD
 - Additional health law schemes
 - Litigation and enforcement trends
- Washington's My Health My Data Act ("MHMD")
 - Legislative background
 - MHMD overview
 - Who must comply with MHMD?
 - Who is a "consumer"?
 - What is "consumer health data"?
 - Some broadly defined aspects of CHD
 - A few examples
 - Your organization's obligations
 - CHD privacy policy
 - MHMD consumer rights
 - Consent and authorization requirements
 - Where to start
- Key Takeaways
- Appendices

Commentary on the My Health My Data Act in this webinar should not be viewed as a lack of support for the rights of individuals to seek health care services and privacy rights in relation to the same, most notably in respect of reproductive and sexual health, and gender-affirming care, which are both implicated under the Act. We recognize and applaud the Washington state legislature's intent to ensure access to these types of health care services and to protect the privacy of those who seek such care.

The commentary we provide in this webinar, to the extent it is critical of the law, is focused on the various compliance challenges that organizations will face due to its breadth, which reaches far beyond the legislature's laudable intent.

HIPAA in Comparison to MHMD

		HIPAA	MHMD
1	Who is Covered?	Covered Entities Business Associates	Regulated Entities, Small Businesses Processors, Persons, Third Parties
2	Data Type	Protected Health Information (PHI)	Consumer Health Data (CHD) **Note that there are PHI exemptions in the law
3	Safeguards	HIPAA Privacy and Security Rules	Prescriptive privacy obligations Data security and access restriction
4	Notice	Notice of Privacy Practices	Consumer Health Data Privacy Policy
5	Consent, Authorization	Authorization for uses and disclosures NOT for <u>T</u> reatment, <u>P</u> ayment, or Health Care <u>O</u> perations (TPO).	Requires consent for collection, sharing + Authorization for SALE of CHD
6	Enforcement	Individual may file complaint with OCR OCR investigation and enforcement	Private Right of Action AG Enforcement
7	Consumer Rights	Rights to request restriction of uses and disclosures, access, amend, accounting of disclosures, non-retaliation.. NO deletion right	Rights to know, access, withdraw consent, revoke valid authorization, delete, non-discrimination, appeal

- **FTC**

- Health Breach Notification Rule (HBNR)
- Section 5 of FTC Act utilized recently in consumer health data enforcement

- **Omnibus state privacy laws (CCPA, CPA, etc.)**

- **State Health Data Privacy Laws**

- Nevada: New law mirroring MHMD (minus private right of action)
- Connecticut: Amendments to CTPA adds *consumer health data* as a type of *sensitive data*.
- NY: Legal restrictions on geofencing (within 1,750 ft. radius) around healthcare facilities for digital advertising purposes.

How much health systems are paying to settle Pixel lawsuits

Naomi Diaz - Wednesday, August 23rd, 2023

18 hospitals, health systems facing lawsuits for healthcare data-sharing

Naomi Diaz - Updated Wednesday, April 26th, 2023

A health data privacy showdown

By BEN LEONARD and ERIN SCHUMAKER | 05/23/2023 02:00 PM EDT

Bloomberg Law

Meta Pixel's Video Tracking Spurs Wave of Data Privacy Suits (1)

July 24, 2023, 2:05 AM

The FTC's settlement with GoodRx puts the digital health ecosystem on notice

The fine and ban on sharing health data could give all health websites reason to pause.

FTC steps up scrutiny of digital health apps with proposed changes to data privacy rule

By Heather Landi - May 18, 2023 04:00pm

Agencies warn hospitals, others about tracking technology compliance risks

Jul 21, 2023 - 02:28 PM

ClassAction.org

in Newswire

Published on February 13, 2023

Major California Medical Center Secretly Shares Patient Data with Facebook, Class Action Says

Pixel Hunt

The FTC Is Taking on Telehealth's Data Sharing Problem—Starting with GoodRx

Abortion-Rights States Begin Shielding Digital Data Near Clinics

MEDCITY INFLUENCERS

DEEP DIVE

Geofencing: The latest data privacy issue facing healthcare

There are a lot of questions to consider when it comes to geofencing and healthcare. Geofencing involves using GPS and other means target people for a marketing campaign.

Fertility app Premom settles with FTC over risky data sharing

The app allegedly shared sensitive user information with China-based companies known for privacy problems

Governance & Risk Management, HIPAA/HITECH, Privacy

Lawsuit: Fertility App Maker Sent Data to Google, Facebook

Proposed Class Action Claims Flo Health Shared Users' Sensitive Data Without Consent

Meta Platforms must face medical privacy class action

By Jonathan Stempel

September 11, 2023 8:13 AM PDT - Updated 3 days ago

Washington's My Health My Data Act



Broad Extraterritorial Scope

Defines “consumer” as (1) a natural person who is a Washington resident; *or* (2) a natural person whose consumer health data is collected in Washington.

Applies, primarily, to “regulated entities” and “small businesses.”

Broad Scope of CHD

Includes, “consumer seeking health care services.” “Health care services” is broadly defined as “any service provided to a person to assess, measure, improve, or learn about a person’s mental or physical health.”

Geofencing Prohibition

No location detection *within 2,000 feet or less* around any entity providing in-person health care services for purposes of identifying or tracking consumers seeking health care services; collecting CHD from consumers; sending notifications, messages or ads to consumers related to their CHD or health care services.

Familiar Consumer Privacy Law Concepts with Draconian Consent & Authorization Requirement

Effective Dates

Regulated Entities: March 31, 2024.

Small Businesses: June 30, 2024.

Geofencing Prohibition: Already effective as of July 23, 2023.

Private Right of Action + AG Enforcement

MHMD allows consumers to recover actual damages, limited to \$25,000, reasonable attorney’s fees, and costs. Courts have discretion to award treble damages. WAAG championed passage of this law and will vigorously enforce requirements.

(See Washington Consumer Protection Act, RCW § 19.86 et seq.)

Who Must Comply with MHMD?

REGULATED ENTITY

(a) Conducts business in Washington, or produces or provides products or services that are targeted to consumers in Washington;

and

(b) alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling of consumer health data.

Excludes: government agencies, tribal nations, or contracted service providers when processing consumer health data on behalf of the government agency.

SMALL BUSINESS

A regulated entity that:

(a) Collects, processes, sells, or shares consumer health data of *fewer than 100,000 consumers during a calendar year;*

or

(b) Derives less than 50 percent of gross revenue from the collection, processing, selling, or sharing of consumer health data, and controls, processes, sells, or shares consumer health data of fewer than 25,000 consumers.

PROCESSOR

A person that processes CHD on behalf of a regulated entity or small business.

PERSON

Natural persons, corporations, trusts, unincorporated associations, and partnerships, *excluding* government agencies, tribal nations, or contracted services processing CHD on behalf of government agency.

THIRD PARTY

An entity other than a consumer, regulated entity, processor, small business, or affiliate of the regulated entity or the small business.

Who is a “Consumer”?

- A natural person who
 - is: (i) a Washington resident; *OR* (ii) whose CHD is *collected in Washington*.
 - acts only in an individual or household context, however identified, including by any unique identifier.
- Individual/Household context: excludes B2B data
- “Does *not* include an individual acting in an employment context” - i.e., excludes employee data
- What does “collected in Washington” mean?
 - While the consumer is physically there?
 - While CHD is collected on servers located there?

What is “Consumer Health Data”?

Personal information that is linked or reasonably linkable to a consumer and that identifies past, present, or future physical or mental health status.

Physical or mental health status includes, but is not limited to:

- Health conditions, treatment, diagnoses
 - Social, psychological, behavioral, and medical interventions
 - Health-related surgeries or procedures
 - Bodily functions, vital signs, symptoms, measurements of physical/mental health status data
 - Diagnoses or diagnostic testing, treatment, or medication
 - *Gender-affirming care information*
 - *Reproductive or sexual health information*
 - *Biometric data*
 - *Genetic data*
 - *Precise geolocation info* reasonably indicating attempt to acquire/receive *health care services* or supplies
 - Data identifying a consumer seeking *health care services*
 - Any CHD derived or extrapolated from non-health information, such as proxy, derivative, inferred, or emergent data
- Red/italicized terms are defined in MHMD.*

Some Broadly Defined Aspects of CHD

- “Data identifying a consumer seeking health care services”
 - “Health care services” = any service provided to a person to assess, measure, improve, or learn about a person's mental or physical health
- Inferences
 - “Any CHD derived or extrapolated *from non-health information*, such as proxy, derivative, inferred, or emergent data”
 - Inferences based on, or derived or extrapolated from, CHD would also be in scope

A Few Examples

- Information collected by pixels/cookies
- Impression data regarding health-related ads, and non-health ads on health-related websites and services
- Inferences that someone may be interested in a particular medication or health service or topic
- Purchase history and analytics
- Allergies and dietary limitations
- Information regarding disabilities and physical limitations
- Hair color, eye color, other genetic characteristics
- Health-related search engine queries or GAI prompts, and their respective outputs
- Biometric data = e.g., imagery of the face from which an identifier template can be extracted

Your Organization's MHMD Obligations

Consumer Health Data Privacy Policy

Entities subject to the law must maintain a CHD privacy policy.

Consumer Rights Response Procedures

Consumers have rights of access and deletion, to withdraw/ revoke consents and authorizations, to appeal, and of non-discrimination.

Consents for “Collecting” and “Sharing”

Prescriptive opt-in requirements for CHD “collection” and “sharing.”

Valid Authorizations for “Selling”

Separate and distinct “valid authorization” (per recipient) required prior to “sale” of CHD.

Processor (Vendor) Agreements

Must execute data processing agreement with each processor setting forth processing instructions and limiting what processor to processing only on behalf of regulated entity/small business.

Data Security and Access Restriction

Must implement and maintain reasonable administrative, technical and physical data security practices, and restrict access to CHD only to parties as necessary to further very limited purposes permitted by the law.

- Prescriptive content requirements
- Another footer link...“shall prominently publish a link to its [CHD] privacy policy on its *homepage*”
- Does not state explicitly whether the CHD PP must be separate from your main privacy policy. However, the CHD PP must “clearly and conspicuously disclose[]” required content.

- Sec. 5: Right to non-discrimination
- Sec. 6
 - Right to confirm processing*
 - Right to access* (incl. list of sale/share recipients and their contact info)
 - Right to withdraw consent* (from collection and sharing)
 - Right to delete*
 - Right to appeal
- Sec. 9: Right to revoke valid authorization

** Subject to authentication/ID verification and other CCPA-like requirements (timing, etc.)*

1. Foundational definitions – “collect,” “share,” “sale,” “consent”
2. Consent for collection and sharing. How many consents, covering what purposes, etc.
3. Authorizations for sales. How many, covering what purposes and recipients, etc. How to treat cookies/pixels/digital advertising?
4. Form of consents – need to consider prescriptive yet ambiguous requirements
5. Form of authorizations – prescriptive (but relatively clear) requirements

- **Collect** means to buy, rent, access, retain, receive, acquire, infer, derive, **or otherwise process** consumer health data in any manner.

TLDR; collection = any processing (minus “sharing” or “selling”)

- **Share** means to release, disclose, disseminate, divulge, make available, provide access to, license, or otherwise communicate orally, in writing, or by electronic or other means, consumer health data by a regulated entity or a small business to a third party or affiliate.

- **Sale** means the exchange of consumer health data for monetary or other valuable consideration.

Disclosures to processors ≠ share or sale

Share = e.g., disclosure to a state government; disclosure to an affiliate. No consideration involved.

Sale = Applying *Sephora* interpretation - since consideration aspect of definition (“or other valuable consideration”) is identical to CCPA – certain cookies/pixels/digital advertising use cases may implicate sale. Certainly, whether consideration is implicated in such use cases will be up for debate under MHMD (the argument of no consideration was likely moot long ago under CCPA, but is more clearly moot after *Sephora*).

All sales are shares, but not all shares are sales.

Consents and Authorizations – Summary of Requirements

- Separate consent needed for each “specified purpose” of collection
 - *Drafting inconsistencies → wiggle room for “specified purpose” to mean more than one purpose? (as long as they are related and compatible)*
- Separate consents for collection and sharing
- No consent needed for purposes that are “necessary to provide a product or service”
 - *Unlike other privacy laws, there are not numerous exemptions/exceptions that could excuse consent*
- What disclosures to consider shares (consent) vs. sales (authorizations)
- Sale authorizations separate from consents
- No “compound authorizations” (but it’s unclear what that means)

“a **clear affirmative act** that signifies a consumer’s **freely given, specific, informed, opt-in, voluntary, and unambiguous** agreement, including by electronic agreement”

Clear Affirmative Act**
Opt-in*
Unambiguous**

Freely Given**
Voluntary**

Specific**

Informed**

* Not defined in MHMD, but informed by other definitions or requirements in MHMD

+ Clearly/further defined in other legal schemes (such as GDPR, CPA)

Takeaway: Plaintiffs’ lawyers and regulators will look to other legal schemes for consent standards (and arguments for violations). You should too!

MHMD's Consent Standard

Clear Affirmative Act
Opt-in
Unambiguous

- No pre-checked boxes
- No dark patterns
- Cannot be obtained by agreement to general terms

Freely Given
Voluntary

Cannot require consent to receive a product/service
(consumer refuses to consent + prevents access to a product/service = unlawful discrimination)

Specific

- Consent only applicable to specific purposes and/or parties
- Separate consents for collection and sharing
- Separate consents for each “specified purpose”

Informed

- Consent request must include specific, prescribed information
- Can some of the information be included in a linked disclosure?
Arguably yes, subject to “unambiguous” analysis

Valid Authorization – Enumerated Requirements

1. The specific CHD concerning the customer that the regulated entity/small business intends to sell.
2. Name and contact information of the person collecting and selling the CHD.
3. Name and contact information of the person purchasing the CHD.
4. Description of purpose for the sale, including how the CHD will be gathered and used by the purchaser
5. Statement that the provision of goods or services may not be conditioned on the consumer signing the valid authorization
6. Statement that the consumer has a right to revoke the valid authorization at any time and a description on how to submit a revocation
7. Statement that the CHD sold pursuant to the valid authorization may be subject to redisclosure by the purchaser and may no longer be protected by MHMD
8. Expiration Date (must be one year from date of consumer signature).
9. Signature of the consumer and date. [Electronic signature likely sufficient]

Where to Start: What CHD Does Your Company “Collect”?

- Directly from consumers
- Automatically collected (e.g., cookies/pixels)
- Processors collecting on your behalf
- Internally created inferences
- From third parties
- From affiliates
- Previously collected CHD – i.e., existing on systems and servers (incl. those of processors) as of effective date
- Other sources?

***Don't forget:
collection = processing***

What CHD does your organization “sell” or “share”?

Where to Start: Socializing Requirements with Stakeholders

1. Communicating the Litigation and Enforcement Risk
 - **Private right of action**
 - This law is the Washington AG's pet project
2. Deciding on a compliance approach – how broadly to apply MHMD standards
 - “Consumer” definition makes limited application/approach challenging
 - Aligning your MHMD compliance with other schemes (and vice versa)
3. Scoping the collection, sharing, and sales of CHD
 - Data mapping is key
 - Incl. designation of sales vs. shares in use cases like digital advertising

Where to Start: Socializing Requirements with Stakeholders

4. Assessing the ability to operationalize requirements

- Ability to obtain consents and authorizations?
 - In the position to obtain consent (e.g., direct relationship with consumer)?
 - UX disruption, revenue impact, and other business considerations
 - technical limitations
- Operationalizing consumer requests (online (cookie/pixel) data, non-“online” CHD, third-party pass throughs, etc.)

THANK YOU!

KYLE R. FATH
Partner, Los Angeles | New York
Kyle.Fath@squirepb.com

OWOBOLADE SHONOWO
Senior Associate, Washington, D.C.
Owobolade.Shonowo@squirepb.com

GICEL TOMIMBANG
Associate, Los Angeles
Gicel.Tomimbang@squirepb.com



Appendices



Governor Inslee Signs Washington My Health My Data Act Into Law: First-of-Its-Kind Consumer Health Data Law, Explained

<https://www.privacyworld.blog/2023/04/governor-inslee-signs-washington-my-health-my-data-act-into-law-first-of-its-kind-consumer-health-data-law-explained/>

Health (and Health-ish) Data and Advertising Under Scrutiny

<https://www.squirepattonboggs.com/-/media/files/insights/publications/2023/06/health-and-healthish-data-and-advertising-under-scrutiny/health-and-healthish-data-and-advertising-under-scrutiny-alert.pdf?rev=8f482c303ada4999b53497f019994957>

MHMD vs. HIPAA

	MHMD	HIPAA
Who is Covered?	Regulated Entities, Small Businesses, Processors, Person, Third Parties	Covered Entities Business Associates
Covered Data	Consumer Health Data	Protected Health Information
Notice	Consumer Health Data Privacy Policy	Notice of Privacy Practices
Consent, Authorization	Requires consent for collection, sharing; and authorization for sale.	Authorization for uses and disclosures not for treatment, payment, or health care operations.
Contract with Third-Party Processors/Vendors	✓	✓
Data Minimization	✓	✓
Regulatory Enforcement Body	Washington State, Office of the Attorney General	U.S. Department of Health and Human Services, Office for Civil Rights
Private Right of Action	✓	X
Consumer Rights	Rights to know, access, withdraw consent, revoke valid authorization, delete, non-discrimination, appeal	Rights to request restriction of uses and disclosures, access, amend, accounting of disclosures, not be retaliated against for exercise of HIPAA rights

- Data that is PHI
- Data that is intermingled with PHI and maintained by a covered entity or business associate
- Personal information governed by and collected pursuant to GLBA, FCRA, FERPA, privacy rules adopted by the Washington Insurance Commissioner
- The only broad exemption that excuses compliance with the law is as follows:

“The obligations imposed on regulated entities, small businesses, and processors under this chapter does not restrict a regulated entity's, small business's, or processor's ability for collection, use, or disclosure of consumer health data to prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any activity that is illegal under Washington state law or federal law; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action that is illegal under Washington state law or federal law.”

Scope of Health-Related Data Covered: MHMD vs. Comprehensive State Laws

MHMD	CCPA	CPA	CTPA	UCPA	VCDPA
<p>"Consumer health data" means personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status.</p>	<p>"Sensitive Personal Information" includes "personal information collected and analyzed concerning a consumer's health."</p>	<p>"Sensitive Data" includes "personal data revealing an individual's mental or physical condition or diagnosis, sex life or sexual orientation."</p>	<p>"Sensitive Data" includes "personal data revealing a mental or physical condition or diagnosis, sex life or sexual orientation."</p> <p><i>S.B. 3 amendment to CTPA:</i> Adds "consumer health data" to definition of "sensitive data." Defines "consumer health data" as any personal data that a controller uses to identify a consumer's physical or mental health condition or diagnosis, and includes, but is not limited to, gender-affirming health data and reproductive or sexual health data.</p>	<p>"Sensitive Data" includes "personal data revealing an individual's sexual orientation; or medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional."</p>	<p>"Sensitive data" includes "personal data revealing mental or physical health diagnosis, or sexual orientation."</p>

Applicability Thresholds: MHMD vs. Comprehensive State Privacy Laws

MHMD	CCPA	CPA	CTPA	UCA	VCDPA
<p>“Regulated Entities” (no revenue or number of consumer threshold)</p> <p>“Small Businesses” (fewer than 100,000 consumers/year or Derives less than 50 percent of gross revenue from the collection, processing, selling, or sharing of consumer health data, and controls, processes, sells, or shares consumer health data of fewer than 25,000 consumers.)</p>	<p>For-profit “businesses” that meet thresholds:</p> <ol style="list-style-type: none"> Gross global annual revenue of > \$25M in preceding calendar year; Annually buy, “sell,” or “share” for cross-context behavioral advertising purposes the personal information of 100,000 or more California residents, households, or devices; OR Derive 50% or more of annual revenues from selling or sharing consumers’ personal information 	<p>Any legal entity that:</p> <ol style="list-style-type: none"> Conducts business in Colorado or that produces or delivers commercial products or services that intentionally target Colorado residents; AND that satisfies one or both of the following: <ol style="list-style-type: none"> During a calendar year, controls or processes personal data of 100,000 or more Colorado residents OR Both derives revenue or receives discounts from selling personal data and processes or controls the personal data of 25,000 or more Colorado residents 	<p>Individuals and entities that do business in Connecticut, or that produce products or services that are targeted to Connecticut residents, that in the preceding year either:</p> <ol style="list-style-type: none"> Controlled or processed the personal data of at least 100,000 Connecticut residents (excluding for purpose of completing a payment transaction) OR Controlled or processed the personal data of at least 25,000 Connecticut residents, if the individual or entity derived more than 25% of its annual gross revenue from selling personal data 	<p>Applies to “controllers” or “processors” who:</p> <ol style="list-style-type: none"> Conduct business in Utah or produce a product or service targeted to Utah residents With annual revenue of US\$25M or more AND Either (a) Controls or processes data of 100,000 or more Utah residents in a calendar year OR (b) derives over 50% of the entity’s gross revenue from the sale of personal data and controls or processes the personal data of 25,000 or more Utah residents 	<p>Business entities, including for-profit and B-to-B entities, conducting business in Virginia or that produce products or services that target Virginia residents and, during a calendar year, either:</p> <ol style="list-style-type: none"> Control or process personal data of at least 100,000 Virginia residents OR Derive 50% of gross revenue from the sale of personal data AND control or process personal data of at least 25,000 Virginia residents

Consumer Rights: MHMD vs. State Privacy Laws

	MHMD	CCPA	CPA	CTPA	UCPA	VCDPA
Right to access	✓	✓	✓	✓	✓	✓
Right to confirm data is being processed	✓	Implied	✓	✓	✓	✓
Right to data portability	X	✓	✓	✓	✓	✓
Right to delete	✓	✓	✓	✓	✓	✓
Right to correct	X	✓	✓	✓	X	✓
Right to opt-out of “sale”	✓	✓	✓	✓	✓	✓
Right to opt-out of targeted advertising (CO, VA, UT, CT) / cross-context behavioral advertising (CA)	X	✓	✓	✓	✓	✓
Right to object to automated decision-making	X	✓	X	X	X	X
Right to opt-out of profiling	X	✓	✓	✓	X	✓
Choice required for processing of “sensitive” data?	Opt-In	Opt-Out	Opt-In	Opt-In	Notice + Opp. to Opt-Out	Opt-In
Right to non-discrimination	✓	✓	✓	✓	✓	✓
Right to appeal	✓	X	✓	✓	✓	✓

Organizational Obligations: MHMD vs. Comprehensive State Privacy Laws

	MHMD	CCPA	CPA	CTPA	UCPA	VCDPA
Specific privacy policy content requirements	✓	✓	✓	✓	X	✓
Purpose/use/retention limitations	✓	✓	✓	✓	X	✓
Third-Party (e.g., vendor, processor) Agreements (i.e., Data Processing Agreement)	✓	✓	✓	✓	✓	✓
Privacy and security impact assessments sometimes required	X	✓	✓	✓	X	✓
Obligation to maintain reasonable security standards	✓	✓	✓	✓	✓	✓

MHMD & Other Health-Specific State Laws

	MHMD	CT (SB 3)	NV	NY
Effective Date	<u>Regulated Entities</u> March 31, 2024. <u>Small Businesses</u> June 30, 2024. <u>Geofencing Prohibition</u> Already effective as of July 23, 2023.	July 1, 2023	March 31, 2024	July 2, 2023
Defines “consumer health data”	✓	✓	✓ (narrower definition than MHMD)	X
Defines type of regulated entity	Regulated Entity, Small Business	Consumer Health Data Controller	Regulated Entity	X
Notice at Collection	✓	✓	✓	X
Geofencing	✓ Within 2,000ft. or less around an entity that provides in-person health care services	✓ Within 1,750ft. of mental health facility or reproductive or sexual health facility	✓ Within 1,750ft. of any person or entity providing in-person health care services or products	✓ Within 1,850ft. of health care facility, other than company’s own health care facility
Private Right of Action	✓	X	X	X

MHMD and Other Health-Specific State Law Restrictions

Connecticut	Nevada	New York
<p><i>S.B. 3 amendment to CTPA:</i> Adds “consumer health data” to definition of “sensitive data.” Defines CHD as any personal data that a controller uses to identify a consumer’s physical or mental health condition or diagnosis, and includes, but is not limited to, gender-affirming health data and reproductive or sexual health data.</p> <p><i>Requirements</i></p> <ul style="list-style-type: none"> • May not provide CHD to employee or contractor unless they are subject to a contractual or statutory duty of confidentiality. • Opt-in consent before selling or offering to sell CHD • Prohibits geofence to establish boundary that is within 1,750 ft. of any mental health facility or reproductive or sexual health facility for the purpose of identifying, tracking, collecting data from or sending any notification to a consumer re: consumer’s CHD. 	<p>“Regulated entity” means a person who: (1) conducts business in NV or produces or provides products or services targeted to NV consumers; AND (2) determines the purpose and means of processing, sharing or selling CHD.</p> <p>“Consumer health data” means personally identifiable information that is linked or reasonably capable of being linked to a consumer <i>and is used by a regulated entity</i> to identify the past, present or future health status of a consumer (e.g., data re: bodily functions; reproductive or sexual health care; gender-affirming care; precise geolocation indicating consumer’s attempt to receive health care services or products)</p> <p><i>Requirements:</i></p> <ul style="list-style-type: none"> • Maintain detailed CHD privacy policy. • Separate and distinct opt-in “consent” for CHD “collection” and “sharing.” • Valid authorization prior to “selling” CHD. • <u>Consumer Rights:</u> access, opt-out and deletion rights • Prohibits geofence within 1,750 ft of any medical facility, any other facility providing in-person health care services or products for the purpose of: (1) identifying or tracking consumers seeking in-person health care services/products; (2) collecting CHD; or (3) sending notifications, messages, or ads to consumers related to their CHD or health care services/products. <p>No private right of action. Enforceable by the NV Attorney General. Effective: March 31, 2024.</p>	<p>NY General Business Law amended with new section 394-g re: geofencing of “health care facilities” (e.g., hospitals, nursing homes, mental health care facilities, and services provided to individuals with developmental disabilities)</p> <p>It shall be unlawful to establish a geofence or similar virtual boundary around any health care facility, <i>other than their own health care facility</i>, for the purpose of delivering digital advertisement to a user, for the purpose of building consumer profiles, or to infer health status, medical condition, or medical treatment of any person at or within such health care facility.</p> <p>It shall be unlawful to deliver any digital advertisement to a user at or within any such health care facility, <i>other than their own health care facility</i>, through the use of geofencing or similar virtual boundary.</p>

Local Connections, Global Influence

Abu Dhabi

Atlanta

Beijing

Berlin

Birmingham

Böblingen

Bratislava

Brussels

Cincinnati

Cleveland

Columbus

Dallas

Denver

Dubai

Dublin

Frankfurt

Hong Kong

Houston

Leeds

London

Los Angeles

Madrid

Manchester

Miami

Milan

New Jersey

New York

Palo Alto

Paris

Perth

Phoenix

Prague

San Francisco

Santo Domingo

Shanghai

Singapore

Sydney

Tampa

Tokyo

Warsaw

Washington DC

Africa

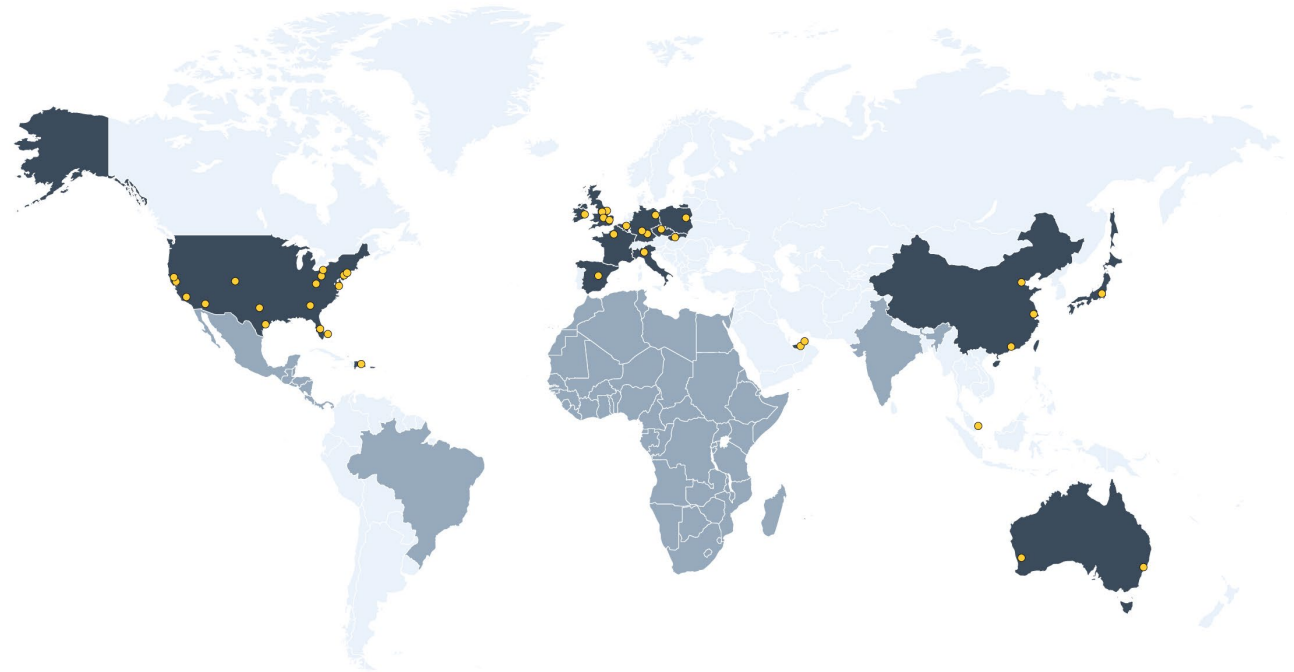
Brazil

Caribbean/Central America

India

Israel

Mexico



■ Office locations

■ Regional desks and strategic alliances