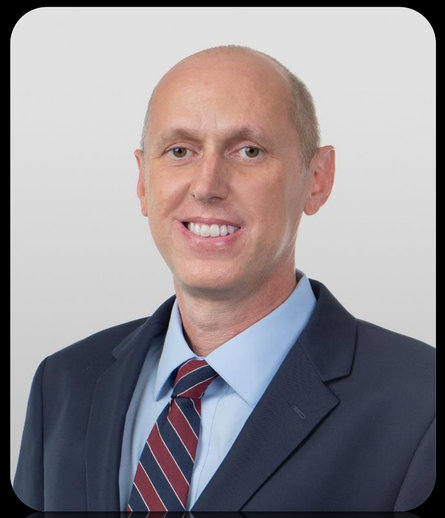
Clark Hill

The New Health Data Laws Every Retailer Must Know



Paul Schmeltzer
Member at Clark Hill
(323) 497-4493
pschmeltzer@clarkhill.com

John Howard
Senior Attorney at Clark Hill
(480) 684-1133
jfhoward@clarkhill.com

November 12, 2025

Agenda:

- Growing patchwork of state consumer health privacy laws
- Implications for retailers and wellness organizations
- Spotlight on Washington's My Health, My Data Act, Nevada SB 370, CPRA, and Connecticut Data Privacy Act
- Examples of enforcement trends, and
- Strategies for compliance and risk mitigation

What Is “Consumer Health Data”?

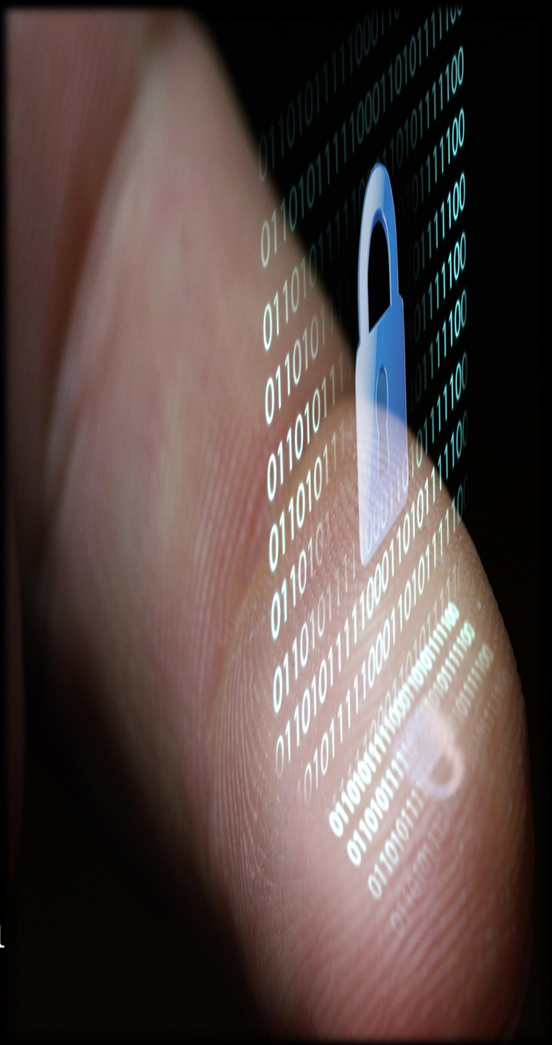
“CHD” = personal information reasonably linkable to a consumer’s physical or mental health status, seeking of healthcare, or inference thereof.

Broader than HIPAA – covers any data that can reveal or infer health-related information, even if collected outside a clinical context.

Examples:

- Purchase history (e.g., prenatal vitamins, fitness products)
- Location near clinics or pharmacies
- Web searches for symptoms or treatments
- App usage tied to sleep, fertility, or stress tracking

Implication: Retailers and e-commerce companies now qualify as “health data controllers” even without medical services.



How CHD Differs from HIPAA PHI

Feature	HIPAA PHI	Consumer Health Data (MHMDA/SB 370/etc.)
Applies to	Covered Entities & BAs	*Anyone* collecting from consumers
Consent	Generally implied for treatment, payment, ops	Must be affirmative opt-in
Sale	Broadly prohibited except narrow disclosures	Allowed *only* with explicit, written consent
Enforcement	OCR & State AGs	State AGs + Private Right (WA)
Examples	EHR, lab results	Browsing, location, purchases, app data

State Law Trends

Emerging Themes Across States:

- Expansion of “consumer health data” beyond HIPAA’s scope
- Opt-in rights for data sharing and sales
- Transparency and deletion obligations
- Enforcement by AGs and private rights of action

Key Differences Between the State Regimes

Topic	WA (MHMDA)	NV (SB 370)	CA (CPRA/ADMT)	CT (CDPA)
Private right of action	Yes (via Washington Consumer Protection Act).	No (AG enforcement).	Limited: private suits only for security breaches; otherwise CPPA/AG.	No (AG enforcement).
Consent required for collection	Affirmative opt-in for collection & sharing of CHD.	Affirmative opt-in for collection & sharing of CHD.	Generally no opt-in to collect; opt-out for sale/sharing; opt-in for minors; SPI "limit use" right.	Clear, affirmative consent for any processing of CHD (amendments).
Sale/transfer restrictions	Sale requires written authorization; strict limits on sharing.	Sale requires written authorization; limits on sharing.	Opt-out of sale/sharing under CPRA; additional limits for Sensitive Personal Information (SPI).	Consent required for sale/processing of CHD under amendments.
Geofencing prohibition	Yes — ban around sensitive health locations. (Geofencing provision operative earlier than main obligations.)	Yes — ban within 1,750 ft of medical facilities when tied to CHD.	No explicit CPRA geofencing ban (separate CA laws/regs may still affect location-based uses).	Yes — ban around mental or sexual-health facilities.
Enforcement body	WA AG + private plaintiffs.	Nevada AG.	CPPA + AG; private suits only for breaches.	Connecticut AG.

Washington My Health My Data Act

- Covers “consumer health data” broadly—including mental health, fertility, biometric, and lifestyle data
- Applies to all entities collecting data from Washington residents—not just Washington-based businesses

Practical impact for retailers:
- tracking pixel = CHD risk
- apps using location near clinics = geofence

- <u>Requires</u>:
  - Opt-in consent for collection and sharing
  - A standalone “Consumer Health Data Privacy Policy”
  - Ability to revoke consent at any time
  - Ban on geofencing near sensitive health locations (e.g., clinics)

Washington My Health My Data Act in Practice: Loyalty App + Ad Pixels

Scenario (Retailer)Regional beauty & wellness chain with a loyalty app and e-commerce site

- Uses pixels/SDKs for attribution and retargeting; sends page URLs and event metadata
- Runs a “new parent” campaign; push offers near pharmacies/clinics

What created CHD risk

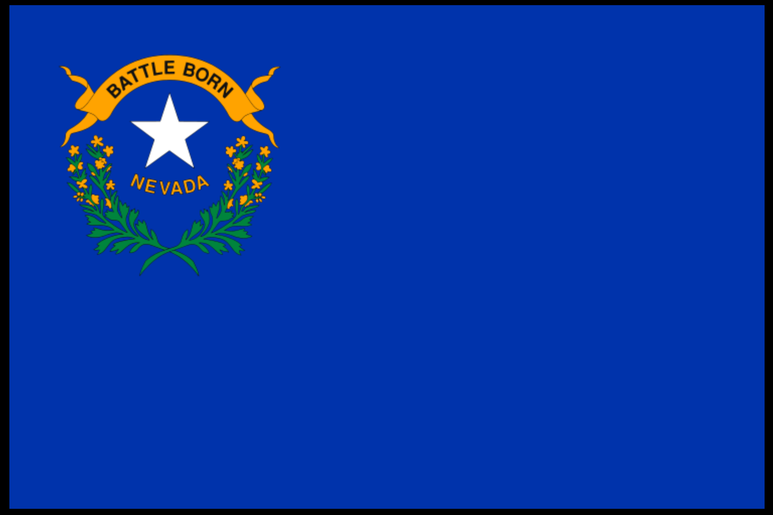
- URLs/metadata reveal intent (e.g., /pregnancy-tests, cart adds, store-locator near clinics)
- Loyalty ID + browsing + location can infer a health status/condition
- No standalone CHD policy; opt-in not captured before collection/sharing
- Push notifications triggered within geofenced areas around “sensitive locations”

Resulting exposure under MHMDA

- Collection/sharing without affirmative opt-in
- Missing Consumer Health Data Privacy Policy and revocation mechanism
- Geofencing ban risk (targeting around clinics)
- Private right of action → litigation leverage even before AG

Nevada Senate Bill 370 (SB 370)

- Largely mirrors MHMDA
- Applies to businesses doing business in NV or that produce or provide products or services that are targeted to NV consumers, and
- Alone or with others, determines the purpose of processing, sharing or selling consumer health data
- No private right of action (AG enforcement)



California Privacy Rights Act (“CPRA”)

- Applies to health-related personal info not covered by HIPAA
- Strengthens consumer rights: access, correction, deletion, opt-out
- Requires data minimization and purpose limitation
- CPPA enforcement + private rights of action (for data breaches)

CPRA’s Impact on Healthcare Providers & Wellness Companies

- Applies to personal health data outside HIPAA’s scope (e.g., wellness apps, digital therapeutics)
- Key rights: access, correction, deletion, opt-out of sale/sharing
- Business obligations: data minimization, purpose limitation, risk assessments (when processing sensitive info)
- Applies even if the entity is not located in California but targets California consumers

AI, ADMT, and Consumer Health Data: California ADMT/AI Rules: New Risks for Retail Algorithms

California's ADMT regulations treat certain **AI and automated decision-making tools** as "profiling" requiring **pre-use notices** and **opt-outs.**

- Applies when tools analyze or infer health-related attributes (e.g., product recommendations for supplements, wellness score generation).

- **Intersection:** Using health-adjacent datasets for personalization or fraud detection can qualify as "processing consumer health data."

- **Action item:** Inventory all algorithmic tools tied to personalization, recommendations, or health-related advertising.

Businesses that use ADMT for significant decisions must comply with the ADMT requirements by January 1, 2027.

Connecticut Data Privacy Act

- First comprehensive consumer privacy law to be amended to include “consumer health data”
- Does not have an exemption for Non-Profits
- Requires clear and affirmative (opt-in) consent for *<u>any</u>* collection, use, disclosure, sale or other processing of consumer health data
- Geofencing restrictions around mental or sexual health facilities

Common Themes:

Generalizing the Patchwork

- Targets health data not otherwise protected under Health Information Portability and Accountability Act (HIPAA)
- Consumer Health Data: Personal information that is linked or reasonably linkable to a consumer and that is used to identify, or can infer, the past, present, or future health status of a consumer.
- MHMDA & NYHIPA (pending the governor's signature) are more broadly interpreted to potentially apply to technical data such as internet browsing activity, search and purchase history, and other "analytical data"
- Sensitive Personal Information: Current consumer privacy laws include "health information" as SPI
- Scope Expansion: No applicable thresholds; only need to do business within a jurisdiction

Business Obligations

- Understand the data being collected from:
  - Retail sale, consumer profiles, purchase history, etc…
  - Consumer facing tools, such as AI chatbots
  - Advertising/Marketing data collections, cookies, ad-campaigns, etc..
- Confirm opt-in / opt-out mechanisms are configured appropriately and functioning correctly
- Publish dedicated consumer health data privacy policies (if applicable)
- Confirm consent mechanisms for any data sales
- Conduct data protection assessment (i.e., data privacy impact assessments)

Vendor Contracts

- Establish agreements, such as Data Processing Agreements, with vendors (Processors), that include:
  - Strict limitations on the processing/use of consumer health data,
  - Establishes processing instructions,
  - Establish the nature, purpose, and duration of process
  - Assist regulated entity comply with legal obligations, including responding to consumer rights requests
  - Obligation to act as a regulated entity even if not technically covered under the law (i.e., step in the shoes of the regulated entity), and
  - Establish and maintain appropriate technical and organizational information security controls

Transparency

- Businesses must establish stand alone consumer health data privacy notices (MHMDA and NV) or update current privacy notices to describe how and when consumer health data is collected, used, or disclosed.
- Consent mechanisms must be put in place to provide clear and affirmative notice to consumers of consumer health data privacy practices and obtain opt-in consent for any regulated uses
- Methods for responding to consumer rights requests (access, deletion, how disclosed) must be in place and effective

Data Monetization

- Sale: exchange of CHD for monetary or other valuable consideration
- Consent / Authorization must be obtained for any sale of consumer health data, that contains:
  - Name and contact info of the seller and purchaser;
  - Description of the CHD to be sold, purpose of the sale, and intended use of CHD
  - Statement indicating authorization not required for the provision of goods/services
  - Right to revoke;
  - Statement that CHD may lose protection once sold; and
  - Expiration date and consumer signature

Consumer Health Data – Retail Examples

- Consumer profiles that contain purchase history of health-related products:
  - Awards account, memberships, etc…
  - Toiletries and common products tend to be excluded
  - Purchases of medicines, sexual health products, etc. covered
- Consumer facing CSR type technologies (AI chatbots)
  - Data use for AI training restricted unless consent/authorization obtained
- Advertising / Marketing
  - Collection of browsing / search history, click throughs, IP addresses, etc. if activity is related to a health activity or can infer an individual health or condition

High-Risk Retail Scenarios

- Loyalty programs offering wellness incentives → CHD collection
- Location-based ads near fertility or weight-loss clinics → geofencing violation
- AI chatbots collecting symptom data → CHD processing
- Fitness app sharing data with social media platforms → sale/sharing risk

Enforcement Trends: What Regulators Are Watching

- California AG and CPPA targeting improper “sale” or “sharing” of health data
- Pixel tracking lawsuits expanding in retail as it pertains to health data
- Class actions under MHMD
- California Delete Act may empower CPPA to target shadow health data markets by requiring data brokers to register & by creating DROP platform

Enforcement Example

Healthline Media LLC (Health and Wellness information website):

Enforcement action brought by CA AG for CCPA violation

Allegation: Healthline used online tracking technology on health information website and used such information to target consumers with advertising without providing an opt-out, included data *suggesting that a person may have a serious health condition*.

- *Violation of purpose limitation, privacy practices deception, insufficient contracts, no opt-out*

Settlement:

- *$1.55 M*
- *Strong injunction including prohibition of sharing article titles that may reveal a consumer may have a medical condition*

Practical Tips for Risk Mitigation

- Use consent management platforms (CMPs) that support GPC signals
- Establish standard operating procedures for responding to consumer rights
- Establish and maintain accurate data maps
- Monitor vendor and third-party data-sharing practices
- Document compliance efforts for legal defensibility
- Engage privacy counsel for high-risk states

Top 5 Retailer Takeaways

1. Treat any health-adjacent data as regulated.
2. Publish standalone CHD privacy notice where applicable.
3. Re-evaluate ad tech, pixels, and loyalty tracking for consent gaps.
4. Embed data minimization and purpose limitation into vendor terms.
5. Monitor state AG actions and plaintiff filings (esp. WA private suits).

Questions?

Thank You

Legal Disclaimer
The views and opinions expressed in this material represent the view of the authors and not necessarily the official view of Clark Hill PLC. Nothing in this presentation constitutes professional legal advice nor is it intended to be a substitute for professional legal advice.

Clark Hill