Comparison of Washington & Nevada Consumer Health Privacy Frameworks

Washington's 'My Health, My Data' Act (MHMD), enacted in late April 2023, has created a new framework for the protection of consumer health data in the states and inspired the introduction of similar bills in other states. ***Nevada's 'My Health, My Data'-style bill (SB 370), which was recently signed into law by Governor Lombardo, is closely modeled after MHMD but is narrower in several significant ways.*** The act will take effect March 31, 2024.

Washington 'My Health, My Data' (MHMD)	Nevada SB 370	Observations
SCOPE: *Covered Data*		
"**Consumer health data**" is "personally identifiable information that is linked or reasonably capable of being linked to a consumer" and "identifies the consumer's past, present, or future physical or mental health status." *§3(8)(a)* • Excludes personal information used public-interest research that is "approved, monitored, and governed by an institutional review board;" *§3(8)(c);* information used for "public health purposes and activities" only; HIPAA-covered data; GLBA, FCRA, and FERPA-covered personal information; and information originating from a HIPAA-covered entity or business associate. *§12* The act provides an inclusive list of **examples of types of data that constitute "physical or mental health status**," including: • "[H]ealth conditions, treatment, diseases, or diagnosis; • Social, psychological, behavioral, and medical interventions; • Health-related surgeries or procedures; • Use or purchase of prescribed medication; • Bodily functions, vital signs, symptoms, or measurements of information...; • Diagnoses or diagnostic testing, treatment, or medication; • Gender-affirming care information; • Reproductive or sexual health information; • Biometric data and Genetic data; • Precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies; • Data that identifies a consumer seeking health care services; or"	"**Consumer health data**" is "personally identifiable information that is linked or reasonably capable of being linked to a consumer and that a regulated entity *uses to identify* the past, present or future health status of the consumer." (emphasis added) *§8* • Excludes information used for certain research purposes; information used for public health purposes; FCRA and FERPA-covered personally-identifiable data; health data collected and shared as authorized by other state or federal law *§20;* information used to "provide access to or enable [video] gameplay;" and information used to "[i]dentify the shopping habits or interests of a consumer," if not used to infer health information. *§8(2)* The act provides an inclusive list of **examples of "consumer health data,"** including "information relating to:" • "[H]ealth condition or status, disease or diagnosis; • Social, psychological, behavioral or medical interventions; • Surgeries or other health-related procedures; • The use or acquisition of medication; • Bodily functions, vital signs or symptoms; • Reproductive or sexual health and Gender-affirming care;" • Health-related Biometric data or genetic data; • Precise geolocation information "that a regulated entity uses to indicate an attempt by a consumer to receive health care services or products; and" • Health information that is derived or inferred from	Information is "consumer health data" under SB 370 only when regulated entities actually *use* that data to identify a consumer's health status. SB 370 defines "consumer health data" to include "information related" to precise geolocation, which appears broader than just geolocation information itself. Unlike MHMD, biometric and genetic data is consumer health data under SB 370 only when such data is "related to" consumer health information. SB 370 would create unique exceptions for information used to facilitate video gameplay as well as for data about a consumer's shopping habits and interests, so long as that data is not used to identify something about a consumer's health.

• Health information that is derived or inferred from non-health data. *§3(8)(a)*	non-health data. *§8(1)*	
SCOPE: *Covered Entities*		
Regulated Entities that "conduct[] business" in Washington State <u>or</u> "produce[] or provide[]" products or services targeted to Washington consumers <u>and</u> solely or with others "determine[] the purpose and means of collecting, processing, sharing, or selling consumer health data." *§3(23)* • Excludes government agencies, government agency contracted service providers, and tribal nations. *§3(23)* **Small Businesses** are regulated entities and that "collect[], process[],sell[], or share" the health data of less than 100,000 consumers annually <u>or</u> make less than 50% of "gross revenue" from the "collection, processing, selling, or sharing" of consumer health data <u>and</u> "control[], process[], sell[], or share[]" consumer health data of >25,000 people. *§3(28)(a)-(b)* **Processors** that "process consumer health data on behalf of a regulated entity or small business." *§3(23)*	**Regulated Entities** that "conduct business" in Nevada <u>or</u> "produce[] or provide[]" products or services targeted to Nevada consumers <u>and</u> solely or with others "determine the purpose and means of processing, sharing, or selling consumer health data." *§15* • Excludes HIPAA & GLBA-covered entities; law enforcement agencies and activities; and the contractors of law enforcement agencies. *§20(1)(a)-(b) & (m)* **Processors** that "process consumer health data on behalf of a regulated entity." *§14*	SB 370 does not create a carve-out or delayed effectiveness dates for small businesses. Unlike MHMD, which excludes HIPAA-covered data, SB 370 excludes HIPAA-covered entities.
INDIVIDUAL CHOICE: *Consent Requirements*		

Unless **necessary** to provide a consumer-requested product or service regulated entities must obtain **consent** for the: ● "**Collection**" of consumer health data; *§5(1)(a)(i)* ● "**Sharing**" of consumer health data; §*5(1)(b)(i)* ● Collection, use, or sharing of **additional categories** of consumer health data; *§4(1)(c)* or ● Collection, use, or sharing of **secondary categories** of consumer health data, *§4(1)(c)* or of consumer health data for **secondary purposes**. *§4(1)(d)* "**Consent**" is "a clear affirmative act that signifies a consumer's freely given, specific, informed, opt-in, voluntary, and unambiguous agreement." Consent cannot be obtained through a consumer's: ● "acceptance of a general or broad terms of use;" ● "hovering over, muting, pausing, or closing a given piece of content;" or ● "agreement obtained through the use of deceptive designs." *§3(6)(a)* Regulated entities must obtain separate "**valid authorization**" in the form of a document that meets requirements specified in *§9(2)(a)-(h)* and is signed by the consumer *§9(2)(i)*, for the "**sale**" of consumer health data. *§9(1)*	Unless **necessary** to provide a consumer-requested product or service regulated entities must obtain consumer's "**affirmative, voluntary consent"** for the: ● "**Collection**" of consumer health data; *§22(1)(a)* ● "**Sharing**" of consumer health data *§22(2)(a)* ● Collection, use, or sharing of **secondary categories** of consumer health data; *§21(3)(a)* or of consumer health data for **secondary purposes** *§21(3)(c);* ● Sharing of consumer health data with **additional third parties or affiliates**; *§21(3)(b).* Persons must obtain separate "**written authorization**" in the form of a "plain language" document that meets the requirements specified in *§30(3)(a)-(h)* and is signed by the consumer in order to "**sell**" consumer health data. *§30(1)(a)*	SB 370 does not define "consent," which might allow regulated entities to disclose information about their health data practices within a general terms of use agreement. While both SB 370 and MHMD allow for the collection and sharing of consumer health data when "necessary" to fulfill a consumer request, neither bill clarifies the precise boundaries of such "necessity." MHMD and SB 370 both require heightened, written consent for the sale of health data, and define "sell" broadly to include the "exchange of consumer health data for money or other valuable consideration." *§17*
INDIVIDUAL CHOICE: *Individual Rights*		
MHMD grants individuals: ● The **right to confirm** whether a regulated entity is collecting, sharing, or selling their health data; *§6(1)(a)* ● The **right to access** health data held by a regulated entity, along with "a list of [and contact information for] all third parties and affiliates with whom the regulated entity…has shared or sold" that data; *§6(1)(a)* ● The **right to withdraw consent** for a regulated entity's collection or sharing of their health data; *§6(1)(b)* ● The **right to delete** their health data. *§6(1)(c)* Regulated entities that receive deletion requests from individuals must: ● **Delete** that consumer's health data from all of its records, including archived or backup systems; *§6(1)(c)(i)(A)* and ■ If the data is stored on an archived or backup system that requires restoration, the consumer request may be delayed six months from the date of authenticating the request (*§6(1)(c)(iii)*)	SB 370 would grant individuals: ● The **right to confirm** whether a regulated entity is collecting, sharing, or selling their health data; *§24(1)(a)* ● The **right to access** "a list of all third parties with whom the regulated entity has shared [or sold] consumer health data relating to the consumer;"*§24(1)(b)* ● The **right to request that a regulated entity cease** collection, sharing, or selling their consumer health data *§24(1)(c)* as well as to **withdraw consent** for such collection, sharing, or selling; *§22(3)(d)* ● The **right to delete** their health data. *§24(1)(d)* Regulated entities that receive deletion requests from individuals must, within 30 days: ● **Delete** the requests consumer health data from its "records and network;" *§26(1)(a)* ■ If the data is stored on archived or backup systems,	SB 370's right to access would not grant individuals the right to access a copy of their health data held by the regulated entity SB 370 would require regulated entities to comply with requests within 45 days of "authenticating" a request, rather than within 45 of days of receipt of that request as required by MHMD (both allow for the possibility of one 45-day extension). SB 370 would allow regulated

• **Notify** "all affiliates, processors, contractors, and other third parties with whom the regulated entity…has shared consumer health data of the deletion request." *§6(1)(c)(i)(B)* Regulated entities shall comply with consumer requests within 45 days of receipt, which may be extended once by 45 additional days "when reasonably necessary." *§6(1)(g)*	entities may delay with deletion of the data for not more than two years "as necessary to restore" such systems. *§26(3)* • **Notify** "each affiliate, processor, contractor or other third party with which the regulated entity has shared consumer health data of the deletion request;" *§26(1)(b)* Regulated entities shall comply with consumer requests within 45 days of "authenticating the request," which may be extended once by 45 additional days when "reasonably necessary." *§25(1)*	entities up to two years to comply with deletion requests for consumer health data contained within archive or backup systems, while MHMD requires regulated entities to do so within six months.
GEOFENCING		
MHMD establishes that it is unlawful for any "person" to **geofence** an "entity that provides in-person healthcare services" for the purpose of: • Identifying or tracking consumers getting healthcare • Collecting health data from consumers; or • Sending health data or healthcare-related "notifications, messages, or advertisements" to consumers. *§10(1)-(3)* A "**geofence**" is "a virtual boundary that is 2,000 feet or less from the perimeter of the physical location." *§31(14)*	SB 370 would forbid any person from "implementing a **geofence** within 1,750 ft of any medical facility, facility for the dependent or any other person or entity that provides in-person health care services or products for the purpose of:" • Identifying or tracking consumers getting healthcare; • Collecting health data from consumers; or • Sending health data or healthcare-related "notifications, messages, or advertisements" to consumers. *§31(1)(a)-(c)* A "**geofence**" is "a virtual boundary with a radius of 1,750 feet or less around a specific physical location." *§31(2)(b)*	SB 370's restriction on the geofencing of health facilities is narrower than MHMD's only applying to geofences within 1,750 ft of such facilities (MHMD's applies to geofences within 2,000 ft).
BUSINESS RESPONSIBILITIES*: Regulated Entity Duties*		
MHMD establishes the following duties for regulated entities: • To maintain and adhere to a "**consumer health data privacy policy**" that makes a specific set of disclosures and to "**prominently publish**" a link to this policy on its homepage *§4(1)* • To **restrict access** to consumer health data to necessary employees, processors, and contractors *§7(1)(a)* • To "establish, implement, and maintain" **reasonable data security practices** *§7(1)(b)* • To establish a **consumer appeals process** *§6(1)(h)* • Non-retaliation. *§5(d)*	SB 370 would establish the following duties for regulated entities: • To develop and maintain a **consumer health data privacy policy** that "clearly and conspicuously" makes a specific set of disclosures *§21(1)(a)-(k)* • To **restrict access** to consumer health data to necessary employees and processors *§28(1)* • To "establish, implement, and maintain" **reasonable data security practices** *§28(2)* • To establish a **consumer appeals process** *§27* • **Non-discrimination.** *§33(1)-(2)*	SB 370 adds a duty for non-discrimination that is not present in MHMD, but does not define "discriminate," which may create uncertainty about whether the discrimination that would be forbidden by the bill encompasses price and service discrimination.
BUSINESS RESPONSIBILITIES*: Processor Duties*		

MHMD establishes the following duties for processors: ● To only process consumer health data "pursuant to" and "consistent with" a **binding contract** between the processor and the regulated entity; *§8(1)(a)(i)-(ii)* ● To "**assist**" regulated entities in fulfilling their obligations under the Act. *§8(1)(b)* Processors that do not follow a regulated entity's instructions or process consumer health data outside the scope of their contract with a regulated entity are "**considered a regulated entity**... with regard to such data." *§8(1)(c)*	SB 370 would establish the following duties for processors: ● To only process consumer health data "pursuant to" a **contract** between the processor and the regulated entity; *§29(1)* ● To "**assist**" regulated entities in fulfilling their obligations under the Act. *§29(2).* Processors that process consumer health data outside the scope of or inconsistently with their contract with a regulated entity are "**deemed a regulated entity**" under the Act. *§29(3)*	Unlike MHMD, SB 370 does not explicitly require that processors only process consumer health data "consistent with" a contract with a regulated entity.
ENFORCEMENT		
Violations of the Act are unfair or deceptive trade practices under the Washington Consumer Protection Act (WCPA) *§11* The WCPA provides for **enforcement by the Washington Attorney General** (WA AG) (*Ch. 19.86.80 RCW*) as well as through a **Private Right of Action** (*Ch. 19.86.090 RCW*). ● The WA AG's office may seek injunctive relief as well as monetary damages for restitution and legal costs, including reasonable attorney's fees (*Ch. 19.86.80 RCW*). ● Individuals may seek injunctions and actual damages (including legal fees). The court has discretion to award treble damages up to $25,000 (*Ch. 19.86.090 RCW*). MHMD does not provide a right-to-cure.	Violations of the Act are unfair or deceptive trade practices under the Nevada Consumer Protection Act (NCPA) *§34(1)* SB 370 would **not be enforceable through a Private Right of Action** *§34(2)(a)* The NCPA provides for **enforcement by the Nevada Attorney General** (NV AG) (*NRS 598.0963*). ● The NV AG's office may seek injunctive relief as well as monetary damages for restitution and legal costs and administrative fines of the greater of $1,000 or treble the restitution amount ordered. (*NRS 598.0971).* SB 370 would not provide a right-to-cure.	While MHMD contains a provision for enforcement through a private right of action, SB 370 does not.