The doctor will see you now

Nevada and Washington put consumer health data under a microscope – is your organization ready for its checkup?

New state data privacy laws focus on consumer health data

In the wake of the U.S. Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization,* Nevada and Washington[1] State have enacted legislation that extends privacy safeguards to an emerging category of personal data known as "Consumer Health Data." Requirements go beyond the purview of Protected Health Information ("PHI") already governed by the U.S. Health Insurance Portability and Accountability Act[2] ("HIPAA"). These new laws come in the wake of increasing enforcement actions brought by the Federal Trade Commission under HIPAA, perhaps signal a renewed broad regulatory focus on healthcare personal data.

Organizations interacting with consumers in these states need to evaluate their personal data management capabilities to validate they can comply with the expanded requirements and increased oversight. Failure to act now can expose the organization to lawsuits from private individuals, fines, and reputational damage.

From the headlines…

In 2023, a telehealth provider of mental health services made headlines after being fined by the FTC for sharing sensitive health data with tech companies for advertising purposes, after promising users that the information would remain private. This practice put user information at risk and violated the company's own privacy policies.

Source: Federal Trade Commission, press release (March 2, 2023).

Comparing the requirements across the states

There is substantial overlap between the two state laws: both Nevada and Washington broaden the definition of personal data beyond HIPAA's PHI, impose new restrictions on consumer health data collection and use, and require specific protection and management controls. The below table provides a high-level comparison of the operative requirements, their similarity and major differences.

	Key differences			Substantial similarities			
	Data Classification	**HIPAA Exemption**	**Enforcement Mechanism**	**Notice & Consent**	**Data Subject Rights**	**Information Security**	**Data Usage**
Washington "House Bill 1155 My Health My Data Act"	"Consumer Health Data" (broader definition)	Data-level exemption for data regulated as PHI (narrower exemption)	State attorney general + private right of action	• Implied consent for primary purpose(s) • Affirmative consent for any secondary purpose(s) • Special consent required for sale of data	• Access • Identities of 3rd party recipients • Withdraw consent • Deletion	"Establish, implement, and maintain administrative, technical, and physical data security practices"	Specific restrictions of data use, including prohibitions on geofencing around certain locations (2,000-feet distance)
Nevada "Senate Bill No. 370"	"Consumer Health Data" (narrower definition)	Entity-level exemption for organizations regulated by HIPAA (broader exemption)	State attorney general only	• Implied consent for primary purpose(s) • Affirmative consent for any secondary purpose(s) • Special consent required for sale of data	• Access • Identities of 3rd party recipients • Withdraw consent • Deletion	"Establish, implement, and maintain administrative, technical, and physical data security practices"	Specific restrictions of data use, including prohibitions on geofencing around certain locations (1,750-feet distance)

Capabilities for addressing compliance requirements

Organizations subject to these new state privacy requirements should utilize a flexible capability model to address these new requirements. The following capabilities provide a good foundation for consumer health data compliance as well as data privacy compliance more generally.

Capabilities

Data Governance

Enables the organization to understand data at a conceptual and physical level and manage it across the extended enterprise IT environment through classifications, data dictionaries, inventories, and data mapping of flows

Third Party Privacy Risk Mgmt.

Enables the organization to establish and enforce privacy-related agreements with third (and fourth) parties, validate the types of data shared with third parties, and monitors the use, management and protection of data in the third party's custody

Information Security

Enables the organization to maintain reasonable layers of security to protect the confidentiality of consumer health data with particular focus upon restricting data access to only necessary employees and contractors

Notice & Consent Mgmt.

Enables the organization to provide accurate notice of data privacy use and management practices to consumers, collect and track consent when its required, and tie usage of data to valid notice-and-consent

Consumer Rights Fulfillment

Enables the organization to receive, track, action, and respond to consumers exercising their rights under the law, such as right to receive access to health data and to receive a list of third parities who received the data

Privacy by Design

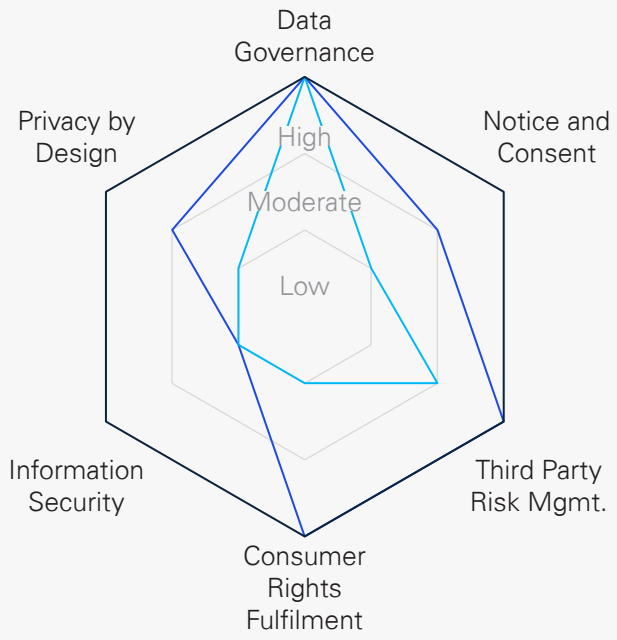
Enables the organization to evaluate new data collect/use cases to understand whether its permissible, whether the minimal amount of personal data is being used, and whether privacy-friendly design and controls are employed

Updating existing capabilities to bring your organization into compliance

Organizations should leverage their existing capabilities for HIPAA or other comprehensive state privacy law (e.g., California Consumer Privacy Act ["CCPA"]), and tailor those capabilities to comply with the new health data regulations. Assuming that the organization is compliant with those existing regulatory frameworks, their current capabilities would provide a solid foundation from which to expand. To get an idea of where to start, the diagram at right provides a high-level analysis of the change impact of the new state healthcare regulations upon the privacy management capabilities for organizations that are currently compliant with HIPAA, CCPA, or neither.

> It's an old adage because it's true: you can't manage what you don't measure. No matter the level of maturity, most organization should begin by getting back to data governance fundamentals – define what consumer health data means to your organization and inventory it.
>
> Jaime Pego
> Principal, Healthcare Advisory

Change Impact on Organizations



Source: "The Doctor Will See You Now," KPMG LLP (September 2023)

Your organization's prescription to get into privacy management shape

Organizations that are subject to these new laws should consider the following next steps to uplevel their privacy management capabilities:

Current-State Assessment and Roadmap: conduct an assessment to gauge your organization's readiness and compliance posture and chart a roadmap for enhancing existing capabilities to meet the new requirements, wherever possible.

Data Discovery and Classification: update policies to define consumer health date for the organization, and execute a data discovery campaign to classify consumer health data and inventory its storage/processing systems, business uses and third-party sharing

Notice and Consent Management: review and update external privacy notices, and design processes to collect affirmative consent for secondary processing activities

Third party management: review and update third party contracts for data sharing of consumer health data so that proper security and usage requirements are in place

Security Assessment and Control Design: utilize the updated inventory of consumer health data to assess systems that stores, transmit and process the data, paying particular attention to validating access management processes given that both laws specifically mention this area

> Organizations are fooling themselves if privacy capabilities are not being considered holistically. As new categories of data fall into modern state laws like My Health My Data, the imperative to protect consumer health data is urgent and has the potential to destroy brands if not taken seriously."
>
> Orson Lucas
> Principal, US Privacy Lead

How KPMG can help

Our privacy and healthcare compliance practices offer a deep bench of technologists, security professionals, former regulators and attorneys. We have successfully helped hundreds of organizations break down the complex data privacy and healthcare regulatory environment to develop risk-based, flexible and proven capabilities for achieving compliance.

In the face of evolving data privacy regulations, it is imperative for organizations to adapt swiftly. By harnessing existing capabilities, developing new processes, and collaborating with KPMG, organizations can maintain consumer trust in an era of heightened health data privacy scrutiny.

Footnotes

[1] Source: "Washington becomes first state to adopt health data protections post-Roe," Cat Zakrzewski, The Washington Post (April 27, 2023).

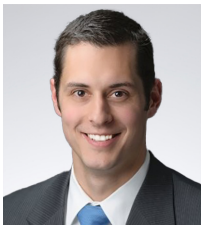
[2] Source: "Washington state on track to pass board-based health data privacy law," Jennifer Bryant, International Association of Privacy Professionals (April 12, 2023)

Contact us

Orson Lucas
Principal, Privacy Advisory and US Privacy Lead, KPMG LLP
T: 813-301-2025
E: olucas@kpmg.com

Jaime Pego
Principal, Healthcare Advisory, KPMG LLP
T: 908-416-1662
E: jpego@kpmg.com

Michael Henzey
Director, Privacy Advisory, KPMG LLP
T: 571-635-4336
E: mhenzey@kpmg.com



Matthew Colford
Director, Healthcare Advisory, KPMG LLP
T: 973-912-6112
E: mcolford@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia