Four More States Join Growing U.S. Privacy Landscape with New Legislation

05.10.2023

ATTORNEYS

Maureen E. Fulton

Mikaela M. Witherspoon

PRACTICE AREAS

Data Privacy and Security

The surge in comprehensive state data privacy laws has continued through the spring of 2023, with state legislatures passing four new bills so far in April and May of 2023. Indiana became the seventh state to pass a comprehensive data privacy law; Tennessee followed suit, while Montana's bill awaits signature by their governor as of May 15, 2023. Meanwhile, the state of Washington has passed a data privacy law related to consumer health data that includes many of the rights and obligations of generally applicable data privacy laws seen in other states and is likely to apply to many businesses in the consumer health space. While some components of these laws bear a strong resemblance to existing state privacy laws, there are several new features to keep track of as the effective dates of these laws approach.

Indiana

Key takeaways: Effective January 1, 2026, Indiana's new state privacy law is more business-friendly than some other state privacy laws, and largely tracks the requirements of the Virginia Consumer Data Protection Act.

On May 1, 2023, Indiana became the seventh state to enact a comprehensive state privacy law. The Indiana Consumer Data Protection Act ("ICDPA"), which goes into effect on January 1, 2026, is similar to other state privacy laws and should not impose a major compliance burden on businesses that will be subject to the law if the business has already attempted to comply with other state privacy laws. The ICDPA applies to

legal entities conducting business in Indiana or producing products or services targeted to Indiana consumers that either (1) control or process the personal data of 100,000 or more Indiana consumers, or (2) control or process the personal data of at least 25,000 Indiana consumers and derive 50 percent of their revenue from the sale of personal data. The law applies only to consumer data.

Consumer rights under the law are consistent with the majority of other state privacy laws and consist of the right to access, right to correct, right to data portability, right to delete, and right to opt out of processing personal data for targeted advertising, profiling and selling of personal data. Like Colorado, Connecticut, and Virginia, the ICDPA requires opt-in consent in order to process sensitive data. Data controllers must conduct data protection impact assessments in some instances, and must enter into data processing agreements with third parties to whom they transfer data. The law includes a 30-day window to cure violations, after which time the Indiana attorney general can enforce violations by issuing an injunction for uncured violations and/or seeking a civil penalty of up to $7,500 per violation.

Washington

Key takeaways: Washington's My Health, My Data Act differs from other comprehensive state privacy laws as it aims to regulate the collection and use solely of consumer health data. However, given the broad definitions of "collection" and "consumer health data", the law will likely apply to the data collection activities of a variety of businesses. Protected Health Information governed by HIPAA is expressly exempted from the law.

On April 27, 2023, Washington's My Health, My Data Act ("MHMDA" or "Washington law") was signed into law. The law, which takes effect on March 31, 2024, applies to legal entities conducting business in Washington or targeting products or services to Washington consumers that determine the purpose and means of collecting, processing, sharing or selling consumer health data. Actions that constitute "collecting" data include buying, renting, accessing, retaining, receiving, acquiring, inferring, deriving, or otherwise processing consumer health data in any manner. This broad definition means that most actions involving consumer health data may be considered a collection. Regulated entities can collect consumer health data only where they have consent for the specific purpose of collection, or require the data in order to provide a product or service the consumer requested. Signed authorization from the consumer is required prior to selling or offering to sell any consumer health data. This consent must be separate from the initial consent needed to collect or share the data.

Unlike other comprehensive state privacy laws, there is no revenue threshold or minimum number of data subjects for applicability. As the law covers any consumer whose data is collected in Washington, it will likely cover non-Washington residents who interact with

Four More States Join Growing U.S. Privacy Landscape with New Legislation

Washington businesses. The MHMDA applies to consumer health data, which is broadly defined as "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."

Under the Washington law, consumers have a right to access their consumer health data and receive a list of affiliates and third parties who receive their data from the controller. Consumers also have a right to withdraw consent to the collection and sharing of their data. Like other state privacy laws, consumers have a right to have their data deleted. Controllers are required to maintain a public consumer health data privacy policy that identifies the categories of health data collected and shared, the categories of sources from which it is collected, the purpose and intended use for the collected data, the categories of third parties and affiliates that receive the data, and how consumers can exercise their rights. The Washington law also makes it unlawful to use geofencing to identify or track consumers seeking health services, collect health data from consumers, or send notifications, messages or ads to consumers related to their health data or services received.

Montana

Key takeaways: The Montana Consumer Data Privacy Act has been passed by the legislature but still awaits the governor's signature. If enacted, the law would take effect on October 1, 2024. The bill is similar to the Connecticut Data Privacy Act, but contains a lower applicability threshold, likely to account for Montana's smaller population.

On April 21, 2023, the Montana legislature passed the Montana Consumer Data Privacy Act. The Act has been sent to Montana Governor Greg Gianforte, who can sign the bill into law, veto the bill, or allow the bill to become law without signature. The Montana Consumer Data Privacy Act ("MCDPA" or "Montana law") is among the stronger state data privacy bills, and contains notable differences from the privacy laws of other states. The MCDPA has a lower applicability threshold, and applies to legal entities conducting business in Montana or producing products or services targeted to Montana consumers that either (1) control or process the personal data of 50,000 or more Montana consumers or (2) control or process the personal data of at least 25,000 Montana consumers and derive 25 percent of their revenue from the sale of personal data. Like all state privacy laws with the exception of California, the bill applies only to consumer data.

While the MCDPA consumer rights are generally consistent with those provided by other states, Montana also requires data controllers to recognize universal opt-out mechanisms, in alignment with Connecticut and California laws. The Montana law will not require controllers to verify opt-out requests, meaning that Montana consumers would not be required to provide information confirming their identity in order to opt out of the sale of their personal data, for targeted advertising, or for certain types of profiling. Until April 1, 2026, controllers in violation of the

Four More States Join Growing U.S. Privacy Landscape with New Legislation

MCDPA will have a 60-day window to cure violations. After April 1, 2026, the Montana attorney general can bring proceedings without notice. The bill does not specify the types of remedies available or provide limits on the monetary penalties that the attorney general may seek.

Tennessee

Key takeaways: The Tennessee Information Protection Act was signed into law on May 11, 2023. It takes effect on July 1, 2025. The bill is similar to the Virginia Consumer Data Protection Act, but includes a first-of-its-kind affirmative defense for violations.

On April 21, 2023, the Tennessee legislature passed the Tennessee Information Protection Act ("TIPA" or "Tennessee law"). The Act was signed into law by the governor on May 11, 2023. The TIPA is fairly similar to Virginia's law, but does differ in several areas. The bill would apply to legal entities conducting business in Tennessee or producing products or services targeted to Tennessee consumers with revenue exceeding $25 million that either (1) control or process the personal data of 175,000 or more Tennessee consumers or (2) control or process the personal data of at least 25,000 Tennessee consumers and derive 50 percent of their revenue from the sale of personal data. The bill applies only to consumer data, and includes consumer rights consistent with those available under other state privacy laws.

The Tennessee law includes a 60-day cure period for violations, after which time the Tennessee attorney general can issue $7,500.00 in civil penalties for each violation of the law, and treble damages for willful or knowing violations. The TIPA is the first state privacy bill to establish an affirmative defense to violations for businesses that adopt privacy programs that reasonably conform to the NIST Privacy Framework or "other documented policies, standards, and procedures designed to safeguard consumer privacy."

Koley Jessen will continue to monitor developments related to these laws and advise as updates become available. If you have questions on whether your business needs to comply with the law or what steps you must take to comply, please contact one of the specialists in Koley Jessen's Data Privacy and Security Practice Area.