Nevada Enacts Expansive New Consumer Health Privacy Act

On June 5, 2023, the Nevada Legislature passed an amended version of Senate Bill 370 (SB 370 or the Act), which imposes new requirements on the collection, use and sale of consumer health data. The bill was signed on June 22, 2023, and will take effect on March 31, 2024. Modeled after Washington's My Health, My Data Act, SB 370 applies to all entities that conduct business in Nevada or provide products or services that are targeted at consumers in Nevada *and*, either alone or with others, determine the purpose and means of processing, sharing, or selling consumer health data. For example, an employer that retains employee medical records would likely be subject to SB 370. Additionally, digital wellness services, gyms and fitness companies might also have obligations under the Act.

Consumer Rights

The Act gives consumers rights over their health information that they didn't have prior to its passage. These include the right to access a list of all third parties their health data has been sold to or shared with; the right to stop a business from processing, sharing or selling their health data; the right to have health data deleted; and the right to confirm if a covered business under the Act is sharing, collecting or selling their health data.

In the event a consumer wants their health data deleted, covered businesses must delete data and notify affiliates, contractors and processors of the deletion request within 30 days. Responses to consumer requests are required without undue delay and no later than 45 days after the request is authenticated.

Once the law takes effect, the state attorney general may impose financial penalties for noncompliance. A violation of the Act is considered a deceptive trade practice under Nevada law. Notably, unlike the Washington My Health, My Data Act, there is no private cause of action.

Covered Entity Requirements

SB 370 generally prohibits the collection and sharing of consumer health data without the consumer's affirmative, voluntary consent (with separate consents required for collection and sharing) and will prohibit the sale of consumer health data without the consumer's written authorization.

Consumer health data includes, without limitation:

(a) Information relating to:

(1) Any heath condition or status, disease or diagnosis;

(2) Social, psychological, behavioral or medical interventions;

(3) Surgeries or other health-related procedures;

(4) The use or acquisition of medication;

(5) Bodily functions, vital signs or symptoms;

(6) Reproductive or sexual health care;

(7) Gender-affirming care;

(b) Biometric data or genetic data related to the information listed above;

(c) Information related to the precise geolocation information of a consumer that a regulated entity uses to indicate an attempt by a consumer to receive health care services or products; and

(d) Any information described in paragraphs (a), (b) or (c) that is derived or extrapolated from information that is not consumer health data, without limitation, proxy, derivative, inferred or emergent data derived through an algorithm, machine learning or other means.

Covered organizations are also prohibited from geofencing healthcare facilities (within 1,750 feet) for the purpose of tracking and identifying consumers receiving or seeking healthcare, sending health data or healthcare-related notifications, messages or advertisements to consumers or collecting health data from consumers. Geofencing is a type of location-based marketing and advertising. Geofencing software uses GPS, radio frequency identification, Wi-Fi or cellular data to detect a virtual geographic boundary. It will then send advertisements to those devices exiting or entering the geofence boundary.

Exceptions

Some exceptions to the act include law enforcement agencies and their contractors and entities that are covered by the Health Insurance Portability and Accountability Act (HIPPA) and the Gramm-Leach-Bliley Act (GLBA). Notably, SB 370 does not exempt nonprofits.

Key Takeaways

Organizations subject to the Act's new consumer health data privacy requirements should consider the following recommendations:

- Determine whether your organization collects data that is included in SB 370's definition of consumer health data before the Act takes effect.
- Update your organization's privacy policies and notice materials to reflect SB 370's new consumer rights.
- Ensure your organization is not using consumer health data in ways that are not contemplated by public-facing privacy policies.

Bond attorneys regularly assist and advise clients on an array of data privacy matters. If you have any questions about health privacy, please contact an attorney in Bond's cybersecurity and data privacy practice.

**Special thanks to Summer Law Clerk Selin Ince for her assistance in the preparation of this memo. Selin is not yet admitted to practice law.*

BOND SCHOENECK & KING ATTORNEYS