MERCER
MAKE TOMORROW, TODAY

LAW & POLICY GROUP | GRIST

CALIFORNIA'S DATA PRIVACY LAW APPEARS NOT TO REACH HIPAA-COVERED GROUP HEALTH PLANS, BUT OTHER IMPACTS UNCLEAR

By Mercer's Catherine Stamm and Katharine Marshall
April 8, 2019

California's sweeping new data privacy law, effective Jan. 1, 2020, gives the state's residents new rights over the use of their personal information. Under the California Consumer Privacy Act (CCPA), (AB 375 / Ch. 55, amended by SB 1121 / Ch. 735, consumers have the right to know what personal information businesses collect, where the information comes from, what it's used for, and how it's shared. Consumers also have the right to stop or limit the collection, use, sharing or selling of their information.

Employers have raised concerns about the breadth of the new requirements and questioned its impact on their employee benefit programs. The law applies to a broad spectrum of personal information but specifically carves out an exception for medical information and health care providers governed by the California Confidentiality of Medical Information Act (CCMIA) as well as protected health information (PHI), covered entities and business associates subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA)'s privacy, security and notification rules, among other exceptions.

Some aspects about the scope of CCPA remain unclear. Nothing in the law specifically addresses the CCPA's application to employee information collected by employers for employment-related purposes, including the administration of benefits not subject to HIPAA. Employers will want to watch for clarifying amendments as well as regulations from the state attorney general's office, expected before the law's implementation date. In the meantime, this GRIST offers a brief overview of key provisions.

COVERED ENTITIES

The law applies to for-profit organizations that do business in California, collect or process consumer personal information and satisfy at least one of the following:

- Bring in more than $25 million in annual gross revenues
- Annually buy, sell, receive or share for commercial purposes the personal information of 50,000 or more consumers, households or devices
- Derive at least half of their annual revenue from selling consumers' personal information

The law also applies to any entity controlling or controlled by an organization subject to the law with which it shares common branding.

COVERED INFORMATION

The law defines "personal information" broadly. It includes information that can identify, relate to, describe, or be associated or reasonably linked, directly or indirectly, with a particular consumer or household. This includes common identifiers like name, address, driver's license number and social security number but also aliases, screen names, property records, biometric data, geolocation data, purchasing history, internet activity, and professional or employment-related information. It also includes any inferences that can be drawn from these identifiers.

Limits and exclusions. The definition excludes publicly available information lawfully obtained from federal, state, or local government records. De-identified or aggregate consumer information isn't considered publicly available and therefore could fall within the definition.

The law also excludes PHI collected by a covered entity governed by the CCMIA or HIPAA's privacy, security and breach notification rules. Covered entities under HIPAA include employer-sponsored group health plans. While employers generally aren't covered entities, an employer often must comply with HIPAA obligations on behalf of group health plans it sponsors.

The new California law's reach is limited in a number of other ways and explicitly avoids interference with other federal laws, including the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, and the Driver's Privacy Protection Act.

CONSUMER RIGHTS

The law grants consumers the right to:

- Request disclosure of the categories and specific pieces of personal information collected, the categories of sources from which that information is collected, the business purposes for collecting or selling the information and the categories of third parties with which the information is shared
- Request deletion of personal information
- Request that a business that sells the consumer's personal information or discloses it for a business purpose disclose to the consumer the categories of personal information collected, sold or disclosed and the categories of third parties to which the information was sold or disclosed
- Opt out of the sale of personal information

An entity that buys personal information has no right to sell it to another without first providing the consumer explicit notice and an opportunity to opt out of the sale.

ANTI-DISCRIMINATION PROVISION

The law prohibits covered businesses from discriminating against consumers for exercising any of the rights provided. This includes denying goods or services, charging a different price, providing a different quality of goods or services, and even suggesting the consumer will receive a different price, level or

quality of goods or services. However, a covered business can charge a different price or provide a different level of goods or services if the difference is reasonably related to the value provided to the consumer by the consumer's own data.

BUSINESS REQUIREMENTS

A covered business that collects personal information must tell the consumer at or before the point of collection what information will be collected and why and explain the right to have the information deleted. Covered businesses that sell personal information to third parties must provide notice that the information may be sold and offer consumers an opportunity to opt out.

A covered business can offer financial incentives for the collection, sale or deletion of personal information but can't sell the personal information of someone under 16 without the individual's (or their guardian's) express consent.

Covered businesses must respond to a verifiable consumer request to access personal information promptly and free of charge. The law also prescribes requirements for receiving, processing and satisfying consumer disclosure requests, opt-out requests, and requests to delete personal information.

EMPLOYER NEXT STEPS

From a group health plan perspective, the law appears to have limited reach. While waiting for clarifying regulations, companies that meet the law's definition of a covered business will want to discuss with legal counsel the extent to which the law might cover non-HIPAA-protected personal information of employees residing in California. Employers may also wish to confirm that their HIPAA privacy and security policies and practices are current.

RELATED RESOURCES

Non-Mercer Resources

- California Consumer Privacy Act, AB 375 / Ch. 55, amended by SB 1121 / Ch. 735 (California Legislature, June 28, 2018)
- California Confidentiality of Medical Information Act (California Legislature)
- HIPAA Resource Page (HHS)

Mercer Law & Policy Resources

- 2019 Outlook for More HIPAA Changes (Feb. 6, 2019)

Other Mercer Resources

- Mercer Health & Benefits Legislative & Regulatory Compliance Solutions

Note: Mercer is not engaged in the practice of law, accounting or medicine. Any commentary in this article does not constitute and is not a substitute for legal, tax or medical advice. Readers of this article should consult a legal, tax or medical expert for advice on those matters.