Published on *The National Law Review* https://natlawreview.com

# California Governor Signs into Law Bills Updating the CPRA and Bills Addressing the Privacy and Security of Genetic and Medical Data, Among Others

Article By:

Hunton Andrews Kurth's Privacy and Cybersecurity

During the week of October 4, 2021, California Governor Gavin Newsom signed into law bills amending the California Privacy Rights Act of 2020 ("CPRA"), California's data breach notification law and California's data security law. Additional bills, amending the California Confidentiality of Medical Information Act ("CMIA") and the California Insurance Code, also were also signed into law. The Governor also signed into law a bill protecting the privacy and security of genetic data processed by direct-to-consumer genetic testing companies and a bill designed to prevent the sale, purchase and use of data obtained by illegal means.

## CPRA Amendment Bills

**AB-694:**

- This bill amends Section 1798.199.40 of the CPRA to clarify that the California Privacy Protection Agency ("CPPA") must issue implementing CPRA regulations the *later* of either (1) July 1, 2021 or (2) within six months of the CPPA providing the California Attorney General with notice that it is prepared to assume rulemaking responsibilities under the CPRA.
- The bill also makes a number of non-substantive changes to the California Consumer Privacy Act ("CCPA")/CPRA.

**AB-335:**

- This bill amends Section 1798.145 of the CPRA to exempt from the opt-out of sale right the sharing of vessel information or ownership information between a vessel dealer and the vessel's manufacturer, to the extent the data is shared for the purpose of effectuating a vessel repair covered by a vessel warranty or recall, provided that the information is not sold, shared or used for any other purpose.
- This bill becomes effective January 1, 2022.

## Genetic Data: California Data Breach Notification and Data Security Law Amendment Bill

**AB-825:**

- This bill amends California's (1) data breach notification law (for both government agencies (Cal. Civ. Code Section 1798.29) and businesses (Cal. Civ. Code Section 1798.82))and (2) data security law (Cal. Civ. Code Section 1798.81.5) to add "genetic data" as a category of personal information that would trigger individual and regulator notification if breached (data breach notification law) and is required to be protected (data security law).

- The bill defines "genetic data" as "any data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material. Genetic material includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids ("RNA"), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom."

## Genetic Data: Genetic Testing Privacy Bill

**SB-41:**

- This bill, effective January 1, 2022, imposes a number of privacy and data security requirements on direct-to-consumer genetic testing companies.

    - The bill defines a "direct-to-consumer genetic testing company" ("DTC Company") as an entity that does any of the following: (1) sells, markets, interprets or otherwise offers consumer-initiated genetic testing products or services directly to consumers; (2) analyzes genetic data obtained from a consumer (unless the analysis is performed by a person licensed in the healing arts for diagnosis or treatment of a medical condition); or (3) collects, uses, maintains or discloses genetic data collected or derived from a direct-to-consumer genetic testing product or service, or is directly provided by a consumer.

    - The bill uses the same definition of "genetic data" as provided for in AB-825.

- Notice: The bill requires DTC Companies to provide:

1. a summary of its privacy practices;

2. a privacy notice that contains complete information about the company's data collection, consent, use, access, disclosure, maintenance, transfer, security and retention and deletion practices (and how to file a complaint alleging a violation of the law); and

3. a notice that the consumer's deidentified genetic or phenotypic information may be shared

with or disclosed to third parties for research purposes.

- Consent: The bill requires DTC Companies to obtain consumers' express consent for the collection, use and disclosure of consumers' genetic data, including separate and express consent for:

1. (1) the use of genetic data through the genetic testing product (including who has access to the data, how genetic data may be shared and the purposes for which the data will be collected);

2. (2) the storage of the consumer's biological sample after the testing required by the consumer has been fulfilled;

3. (3) each use of genetic data *beyond* the primary purpose of the genetic testing;

4. (4) each transfer or disclosure of genetic data or biological sample to third parties *other than* service providers, *including the name* of each third party to which the genetic data or biological sample will be disclosed; and

- The requirement to list the identity of each third party is notable, as it goes beyond that which is required under the CCPA, which requires that only the *categories* of third parties be disclosed to consumers.

5. the marketing by a DTC Company to a consumer based on the consumer's genetic data *or* the marketing by a *third party* based on fact that the consumer used the genetic testing product.

    - DTC Companies do not, however, need to obtain express consent to market to consumers on their *own* website or mobile app based, as long as the ads do not depend on any information specific to the consumer except for the fact that the consumer purchased a product from the DTC Company.

    - Consumers must also be able to revoke their consent, and DTC Companies must destroy such consumers' biological samples within 30 days of any such revocation of consent.

- Disclosure Restrictions: Subject to certain exceptions, DTC Companies cannot disclose consumers' genetic data to (1) any entity that is responsible for administering or making decisions regarding health insurance, life insurance, long-term care insurance, disability insurance or employment; or (2) any entity that provides advice to an entity that is responsible for performing these functions.

Service Provider Contracts: The law requires contracts between DTC Companies and service providers to prohibit the service provider from:

1. retaining, using or disclosing the biological sample, extracted genetic material, genetic data or any information regarding the identity of the consumer (*including* whether that consumer has solicited or received genetic testing) for any purpose (including any commercial purpose) other than for the specific purpose of performing the services specified in the contract; and

2. associating or combining the biological sample, extracted genetic material, genetic data or any information regarding the identity of the consumer (*including* whether that consumer has solicited or received genetic testing, as applicable) with information (a) the service provider has received from or on behalf of another person or persons or (b) has collected from its own interaction with consumers or as required by law.

- Consumer Rights: DTC Companies must develop procedures and practices to enable consumers to exercise the following rights:

1. access to their genetic data;

2. deletion of their consumer account and genetic data (except for genetic data that is required to be retained to comply with applicable legal and regulatory requirements);

3. destruction of their biological sample; and

4. non-discrimination for exercising the above rights (including denial of goods or services, charging different prices for goods and services, providing (or suggesting) a different level or quality of goods or services or considering the exercise of consumer rights as a basis for suspicion of criminal wrongdoing or unlawful conduct).

- Security: DTC Companies must implement and maintain reasonable security procedures and practices to protect a consumer's genetic data against unauthorized access, destruction, use, modification, or disclosure.

- Exemptions: The bill does not apply to:

1. providers of health care governed by the CMIA;

2. covered entities or business associates governed by HIPAA;

3. medical information governed by CMIA or protected health information governed by HIPAA;

4. scientific research or educational activities conducted by certain educational institutions;

5. the California Newborn Screening Program;

6. tests conducted exclusively to diagnose whether an individual has a specific disease (subject to certain conditions);

7. genetic data used or maintained by an employer, or disclosed by an employee to an

employer, to the extent necessary to comply with applicable law;

8. data made available to the public by the consumer; and

9. deidentified data (that meets the requirements for deidentification under the law).

- Penalties for Non-Compliance: The law will be enforced by the California Attorney General or certain district attorneys or city prosecutors. Penalties for negligent violations of the law can result in civil penalties up to $1,000 (plus court costs). Willful violations of the law can result in civil penalties of at least $1,000 up to $10,000 (plus court costs).

## Medical Data: CMIA and Californian Insurance Code Amendment Bill

**AB-1184:**

- This bill amends the CMIA and California Insurance Code to require health care service plans or health insurers to accommodate requests for confidential communication of medical information regardless of whether there is a situation involving "sensitive" services (g., mental health, sexual health) or a situation in which disclosure would endanger the individual.

- This bill also amends the CMIA and California Insurance Code to prohibit a health care service plan or health insurer from requiring a protected individual, as defined, to obtain the policyholder, primary subscriber or other enrollee's authorization to receive sensitive services or to submit a claim for sensitive services if the protected individual has the right to consent to care. The bill also requires health care service plans and health insurers to direct all communications regarding a protected individual's receipt of sensitive services directly to the protected individual, and prohibits the disclosure of that information to the policyholder, primary subscriber, or any plan enrollees without the authorization of the protected individual. Further, the bill requires health care service plans to notify subscribers and enrollees, and health insurers to notify insureds, that they may request a confidential communication in a specified format and how to make the request. The bill also requires health care service plans and health insurers to provide this information in a specified manner, including on the internet website of the health care service plan or health insurer.

- This bill becomes effective July 1, 2022.

## Illegally Obtained Data

**AB-1391:**

- This bill makes it unlawful to sell data, or sell access to data, that has been obtained or accessed as a result of a crime. It also makes it unlawful to purchase or use data from a source that a person knows or reasonably should know has obtained or accessed data through the commission of a crime.

    - The bill uses the broad definition of "data" that is found in the California penal code (and goes beyond personal information): "a representation of information, knowledge,

facts, concepts, computer software, or computer programs or instructions," which may be "in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device."

- A violation of the bill does not constitute a crime.

Copyright © 2025, Hunton Andrews Kurth LLP. All Rights Reserved.

National Law Review, Volume XI, Number 287

Source URL:https://natlawreview.com/article/california-governor-signs-law-bills-updating-cpra-and-bills-addressing-privacy-and