MORRISON FOERSTER

California Governor Signs CCPA Amendments into Law

02 Oct 2020

Privacy + Data Security

Client Alert

This week, California Governor Gavin Newsom signed two much-needed California Consumer Privacy Act (CCPA) amendments into law. The updates ensure that the CCPA's existing partial exemptions for employment and business-to-business (B2B) data will continue for *at least* one additional year and expand the CCPA's exemptions regarding patient medical information. However, the amendments also impose new disclosure and contractual obligations on businesses that sell or disclose de-identified patient information.

Below is our detailed breakdown and analysis of these amendments, including the key changes that will impact organizations' collection, use, and sharing of Californians' personal information (PI).

A.B. 1281 – Extending Partial Exemptions for Employee and "B2B" Data

A.B. 1281 extends for one additional year the CCPA's one-year moratoria (previously set to expire on January 1, 2021) on:

1. Most of the CCPA's individual rights, with the exception of the rights to opt out of sale and non-discrimination, as they pertain to B2B consumers. This exclusion applies when:

- The personal information at issue reflects a written communication, verbal communication, or transaction between the business and consumer;
- The consumer is acting as an employee, owner, director, officer, or independent contractor of an entity; **and**
- The communication or transaction occurs solely within the context of the business conducting due diligence regarding the entity or the business providing or receiving a product or service to or from the entity.

2. Personal information pertaining to job applicants, employees, owners, directors, officers, medical staff, or contractors of a business from much of the CCPA's scope, provided that the personal information is collected and used "solely within the

Contacts

Kristen J. Mathews
(212) 336-4038
kmathews@mofo.com

Joseph Roth Rosner
(213) 892-5314
jrosner@mofo.com

Robert N. Famigletti
(212) 336-4004
rfamigletti@mofo.com

context of the person's role" as an employee, applicant, etc. The CCPA still requires a business to provide such individuals with a privacy notice and clarifies that the exemption does not apply to the CCPA's private right of action following a data security incident.

The exact duration of these partial exemptions remains uncertain, however, because the newly enacted law will **only become operative if voters *reject* the California Privacy Rights Act of 2020 (CPRA)** , the California ballot initiative slated to appear on the November 2020 ballot. If voters approve the CPRA, it will significantly amend the CCPA, including by extending the partial employee and B2B exemptions by **two years, until January 1, 2023**. If the CPRA is not approved, A.B. 1281 will extend the partial employee and B2B exemptions by **one year, until January 1, 2022**.

The full text of A.B. 1281 can be found here.

A.B. 713 – Amending the CCPA's Exemptions Regarding Medical Information and Health Privacy Laws

A.B. 713, which becomes operative immediately, addresses the CCPA's exemptions and requirements related to both patient medical information and businesses that are subject to the Health Insurance Portability and Accountability Act (HIPAA), California's Confidentiality of Medical Information Act (CMIA), and other laws relating to medical privacy and human subject research.

The amendment creates new disclosure obligations for businesses that sell or disclose de#identified patient information, and it establishes requirements for contracts involving the sale or disclosure of such de-identified data.

1. Expanded De-identification and HIPAA Exceptions

The CCPA currently does not apply to any PI that is "de-identified" as broadly defined in the Act. *See* Cal. Civ. Code §§ 1798.140(h), 1798.140(o)(3). HIPAA, in contrast, permits the de#identification of Protected Health Information (PHI) only via two specific methods: reliance upon an expert statistical determination or the removal of certain enumerated personal identifiers from the PHI (the "Safe Harbor" method). *See* 45 C.F.R. § 164.514(a)-(b).

With the enactment of A.B. 713, the CCPA no longer applies to any information that is *both*: (i) derived from PHI, medical information covered by CMIA, or identifiable private information under with the Federal Common Rule for human research

subjects *and* (ii) de-identified pursuant to HIPAA standards. This change may help reduce the compliance burden for businesses who are not regulated by HIPAA but who receive HIPAA de-identified information for their own research or business improvement purposes.

In addition, whereas the CCPA formerly did not apply to HIPAA Covered Entities (healthcare providers, health insurance plans, or healthcare clearinghouses) nor to PHI that is collected by a Covered Entity or its Business Associate (i.e., a HIPAA-regulated service provider), A.B. 713 exempts Business Associates to the extent that they maintain, use, and disclose PHI in accordance with HIPAA.

2. Restrictions on Re-identification and Contract Requirements

A.B. 713 requires that CCPA-covered businesses must not re-identify or attempt to re-identify any information that was de-identified pursuant to HIPAA standards, except as permitted by HIPAA, federal human subject research regulations, or as otherwise required by law.

The amendment does, however, **permit re-identification of de-identified patient information, pursuant to a contract**. Such a contract must provide that: (1) the purposes of the data processing shall be limited only to testing, statistical analysis, or validation of the de-identified data, and (2) the de-identified data must be returned or destroyed at the end of the term of the contract.

Further, beginning January 1, 2021, any **contract for the sale or license of de-identified patient information must prohibit any re-identification or attempt at re-identification**. The contract must restrict the purchaser or licensee of the de-identified patient information from further disclosing the de-identified information to any third party, unless the third party is contractually bound by the same or stricter restrictions.

3. New Disclosure Obligations for De-identified Patient Information

A.B. 713 also requires a CCPA-covered business that sells or discloses de-identified patient information to disclose the following in its online privacy notice:

i. A statement that the business sells or discloses de-identified patient information, and

ii. Identification of which HIPAA-permitted methods were used to de-identify the patient information (either the “Safe Harbor” method or the statistical expert determination method).

A.B. 713 does not specify that the business *itself* must have carried out the de-identification for this notice requirement to apply. Thus, it appears this disclosure requirement applies to any business that purchases or receives de-identified patient information from a third party before carrying out an onward sale or disclosure.

4. Updated Clinical Research Exceptions

Prior to the enactment of A.B. 713, the CCPA did not apply to information "collected" as part of a clinical trial subject to Institutional Review Board (IRB) oversight, international clinical guidelines, or FDA rules. Under A.B. 713, the CCPA no longer applies to information "collected, *used, or disclosed*" for "research" purposes, as defined in the HIPAA rules, so long as such research is conducted in accordance with the data protection requirements of HIPAA, IRB oversight, international clinical guidelines, or the FDA rules.

The full text of A.B. 713 can be found here.

Visit our CCPA Resource Center for important CCPA and CPRA updates and compliance resources. For a detailed analysis of the CPRA, please see our previous client alerts here and here.