California Association of Health Plans

CAHP LEGISLATIVE INFORMATION

AB 713 (Mullin)
Chapter 172, Statutes of 2020

As a service to our members, the California Association of Health Plans produces guidelines designed to assist in the interpretation and implementation of new laws, and to promote full compliance with those laws. This document, however, is not intended to be authoritative. Any questions about official interpretations of the law should be directed to the appropriate state regulatory agency such as the Department of Managed Health Care or the Department of Health Care Services, as well as your legal counsel.

CALIFORNIA CONSUMER PRIVACY ACT OF 2018

BACKGROUND

Assembly Bill 713 was introduced by Assemblymember Kevin Mullin to establish new exemptions from the California Consumer Privacy Act (CCPA) as it relates to certain types of medical information, including exemptions for information that has been deidentified under specified federal requirements, and medical information collected as part of regulated research activities. CAHP supported AB 713 along with a broad coalition of health care organizations representing biotech, hospitals, device manufacturers and the Chamber of Commerce.

AB 375 (Chau, Chapter 55, Statutes of 2018) enacted provisions of the CCPA into law in order to avoid a ballot initiative on the same subject promoted by Californians for Consumer Privacy. The version of CCPA enacted via AB 375 grants a set of rights to consumers with regard to their personal information, including enhanced notice and disclosure rights regarding information collection and use practices, access to the information collected, the right to delete certain information, the right to restrict the sale of information, and protection from discrimination for exercising these rights.

An immediate compliance issue for health plans and others was the differential treatment of deidentified health information regulated under HIPAA (Health Insurance Portability and Accountability Act). The CCPA's existing definition of deidentified data is not harmonized with the HIPAA standard. In order to avoid disruption, AB 713 expressly recognizes the HIPAA de-identification standard as an acceptable standard for deidentification of health information under the CCPA, thereby eliminating potential legal uncertainty.

AB 713 also expands the existing clinical trial exemption by exempting additional types of research conducted in accordance with the federal Common Rule, International Council for Harmonization Good Clinical Practices guidelines or US FDA requirements. This measure also exempts Business Associates that are regulated under HIPAA, just like their Covered Entity counterparts. HIPAA-regulated Business Associates provide services to Covered Entities (doctors, nurses and other providers) and are already extensively regulated under HIPAA and under Business Associate Agreement contracts.

AB 713 had no opposition and enjoyed nearly unanimous support in both houses of the Legislature.

REQUIREMENTS

Amends Section 1798.130 of, and adds Sections 1798.146 and 1798.148 to, the Civil Code, relating to consumer privacy

Specifically, AB 713 does the following:

1) Exempts from the CCPA information that is deidentified in accordance with the requirements for deidentification set forth under specified provisions of HIPAA, and that is derived from patient information that was originally collected, created, transmitted, or maintained by an entity regulated by HIPAA, the CMIA, or the Common Rule, as specified.

2) Requires a business that sells or discloses information that is exempted from the CCPA pursuant to 1) above to disclose on its online privacy policy whether the business sells or discloses deidentified patient information derived from patient information, and if so, whether that patient information was deidentified pursuant to one or more of the following: the deidentification methodology commonly known as the "HIPAA expert determination method," as specified; or the deidentification methodology commonly known as the "HIPAA safe harbor method," as specified.

3) Exempts from the CCPA a business associate of a covered entity governed by HIPAA, to the extent the business associate maintains, uses, and discloses patient information only in accordance with the legal requirements of the privacy, security, and breach notification rules applicable to PHI under HIPAA.

4) Exempts from the CCPA information that is collected, used, or disclosed in research, as defined, including, but not limited to, a clinical trial, and that is conducted in accordance with applicable ethics, confidentiality, privacy, and security rules of HIPAA, the Common Rule, good clinical practice guidelines issued by the International Council for Harmonisation, or human subject protection requirements of the FDA.

5) Defines "patient information" as meaning identifiable private information, protected health information, individually identifiable health information, or medical information, as each of those terms are defined.

6) Prohibits a business or other person from reidentifying information that has met the requirements of 1) above, except for one or more of the following purposes:
a) Treatment, payment, or health care operations conducted by a covered entity or business associate acting on behalf of the covered entity;
b) Public health activities or purposes, as specified in federal law;
c) Research, as defined;
d) Pursuant to a contract that expressly engages a person or entity to attempt to reidentify the information in order to conduct testing, analysis, or validation of deidentification, or related statistical techniques, if the contract bans any other use of the reidentified information and requires the destruction of the information upon completion of the contract; and,
e) If otherwise required by law.

7) Requires information that has been reidentified pursuant to 6) above to be subject to applicable federal and state data privacy and security laws, including, but not limited to, HIPAA, the CMIA, and the CCPA.

8) Requires any contract for the sale or license of deidentified information, where one of the parties is a person residing or doing business in the state, to include the following, or substantially similar, provisions:
a) A statement that the deidentified information being sold or licensed includes deidentified patient information;
b) A statement that reidentification of the deidentified information by the purchaser or licensee of that information is prohibited; and,
c) A requirement that, unless otherwise required by law, the purchaser or licensee of the deidentified information may not further disclose the deidentified information to any third party unless the third party is contractually bound by the same or stricter restrictions and conditions.

9) Contains an urgency clause that will make this bill effective upon enactment