Major Ambiguities Remain, but Health Care Vendors Should Focus on California Consumer Privacy Act (CCPA) Preparedness

Are you a health care vendor that does business in California? If so—and keep in mind that the concept of "doing business" in California may be broader than you expect—there are new, expansive data privacy requirements that might start keeping you awake at night.

California created waves in the information privacy space with its enactment of the California Consumer Privacy Act of 2018 (the "Act") last summer. The Act, which will be operative beginning January 1, 2020, was hurriedly enacted to prevent a proposed ballot initiative from going to voters in November 2018. That process created a number of significant ambiguities, which remain present in the Act.

There are significant questions regarding what types of businesses will be subject to the broad-reaching obligations of the statute and forthcoming regulations. Businesses that have, thus far, managed to avoid the application of the similar EU General Data Protection Regulation (the "GDPR") may nonetheless fall within the scope of the Act and confront new and expanded compliance obligations similar to those imposed by the GDPR. Based on the current wording of the statute, a "business" subject to the Act's requirements includes a for-profit entity that (i) collects the personal information of California residents, (ii) determines the purposes and means of processing that information, (iii) does business in California and, among other potential triggers, (iv) has annual gross revenues in excess of an inflation-adjusted amount of $25 million. It remains to be seen whether the forthcoming regulations will define the scope of revenue (which, at present, does not appear to be limited to a business's California revenue), the meaning of information "processing," and other related concepts.

With respect to applicability, the statute also contains a carve-out for commercial conduct that takes place "wholly outside of California. The present definition of this concept contains somewhat contradictory language, and it is not yet clear what any amended or clarified language will look like.

Businesses potentially subject to the Act should also be wary of the way that the Act ambiguously defines "personal information." The Act does not apply to medical information governed by HIPAA, which will provide some relief to many health care vendors. However, the Act does apply to other categories of personal information, including IP addresses and other information concerning consumers' (including patients') interaction with a business's website. Even more significantly, the Act appears to apply to (i) employee personal information contained in employment records and (ii) the personal information of client officers and employees that a business gathers in providing services to, and interacting with, its clients (i.e., not traditional "consumer" interactions). Absent some clarification to the contrary in any further statutory amendments or in the forthcoming regulations, health care vendors should prepare to comply with the Act in connection with these particular categories of information.

Due to the current broad scope of the Act, the potential applicability to information collected or disclosed in 2019, and the fact that the Act has significant "teeth" from an enforcement standpoint, health care vendors should not wait for these concepts to be fully refined. Rather, they should prepare now to comply with the Act's core requirements by taking the following actions, among others:

- Determine what personal information the business collects, how it collects it, where it stores it, and how it manages, uses, and discloses the information, as well as any service providers that collect or receive information on its behalf (including determining whether any disclosures of information could be deemed the “sale” of information under the Act)
- Provide appropriate mechanisms through which consumers can make permitted requests of the business
- Prepare to evaluate, document, and respond to consumer requests for access to information the business has collected on each consumer
- Prepare to respond to requests for disclosure of details concerning consumer information collected, sold, or disclosed for other business purposes
- Provide consumers with required mechanisms to opt out of the sale of their information, if applicable (or opt in, for consumers who fall within the age requirements)
- Prepare to respond to consumer requests for deletion of information about them, including understanding available exceptions to the deletion requirement
- Add appropriate compliance requirements to contracts with downstream service providers who collect or receive personal information
- Update privacy notices/policies to include information required under the Act
- Train designated personnel on compliance with the Act

Chambliss will continue monitoring CCPA and other developments in the information privacy area. Should you have questions about the Act or preparations for compliance, contact Cal Marshall or any member of our Health Care Section.