If You Think that the CCPA's HIPAA Carve-Out Has Your Organization Fully Covered, Think Again

By Dan Marvin

On January 1, 2020, the California Consumer Privacy Act (CCPA) takes effect, ushering in a new era of privacy rights in the United States. The CCPA is intended to provide residents of California with the rights to: (i) know what personal information is being collected about them; (ii) know whether their personal information is sold or disclosed and to whom; (iii) say no to the sale of personal information; (iv) access their personal data; (v) request that a business delete any personal information about a consumer collected from that consumer; and (vi) not be discriminated against for exercising their privacy rights. The CCPA broadly defines "personal information" as information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Businesses have been grappling with putting procedures in place to ensure that consumer requests can be responded to timely and properly – no small feat for companies that maintain reams of data in different places throughout the country.

Many healthcare providers and organizations have taken comfort in the so-called "HIPAA Carve-Out" of the CCPA, which states that the CCPA does not apply to "protected health information" that is collected by a HIPAA covered entity or business associate. Pursuant to HIPAA, "protected health information" generally is that which relates to the past, present, or future health status of an individual and is created, collected, or transmitted, or maintained in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. However, it cannot be overlooked that many HIPAA covered-entities may be, and probably are, in possession of "personal information" as defined by the CCPA which is NOT "protected health information" as defined by HIPAA.

Indeed, there are many ways in which hospitals and other health care providers collect information about consumers unrelated to the provision of health care services, even when those consumers are also patients. For example, certain information may be collected from consumers for marketing purposes, or website cookies might be collected for one reason or another. This type of personal information would be subject to the CCPA. Or perhaps a patient of a hospital provides personal information (including payment card information) when paying for a meal in the cafeteria, or volunteering for certain hospital charity events. Moreover, there is always the possibility that protected health information, which has been de-identified pursuant to HIPAA and is therefore no longer considered as such, may still be considered "personal Information" pursuant to the CCPA. And of course, the issue of how employee information will be treated under the CCPA (including health information unrelated to treatment) is still being figured out, though for at least the next year, such information is excluded from the CCPA for all businesses.

Most healthcare providers are long on the way to figuring out the interplay between HIPAA and the CCPA. For others, the road is a bit longer, but for all, ensuring full compliance with both statutes is essential.