CARLTON FIELDS

Applying the CCPA to Health Care: The HIPAA Exemption, Exercise Apps, and Marketing Data

September 10, 2019

Despite its breadth, California's new privacy law, the California Consumer Privacy Act (CCPA), creates an exemption designed around the federal Health Insurance Portability and Accountability Act (HIPAA). That exemption is codified at section 1798.145(c)(1) of the California Civil Code. An organization that is otherwise subject to the CCPA - such as a for-profit entity "operating" in California that collects personal information and has either the information of 50,000 consumers or else annual gross revenues in excess of $25 million - may therefore find shelter under HIPAA. The problem is in determining the actual scope of the CCPA's HIPAA exemption and applying it. Here we provide some guidance for doing so.

The first part of the HIPAA exemption is relatively clear. Subsection (c)(1)(A) exempts a certain kind of information: "protected health information" (PHI) collected by a "covered entity" or "business associate" as those terms are defined in HIPAA. HIPAA, in turn, defines PHI as information relating to the physical or mental health or condition of an individual, or the provision of or payment for health care to an individual, for which there is a reasonable basis to believe it can be used to identify the individual.[1]

Accordingly, an organization's status under HIPAA, and the purpose for which the organization collects data, will affect whether the data will qualify for the CCPA's HIPAA exemption. Assume that an athletic sportswear company that sells product in California has developed a pedometer app that consumers can download to their phone via the Apple App Store or Google Play. The app tracks the number of steps a person takes each day and captures additional information, including the user's name, weight, birthday, calories burned, geolocation, and average pace. That company is probably not a covered entity or business associate under HIPAA and would not be able to avail itself of the CCPA's HIPAA exemption.

But consider a health care system "operating" in California that created an app with the exact same functions, yet made the app available only to its patients in order to monitor their health and treat medical conditions. That organization is a covered entity under HIPAA, the data is probably PHI, and the HIPAA exemption probably applies.

On the other hand, it is less clear if the HIPAA exemption covers a health care provider's marketing data, data from mobile apps, or customer service or call center data that is not also PHI. Such data could include internet "cookies," IP addresses collected from an organization's website, mobile device IDs, recorded phone calls, and email addresses. While the actual text of subsection (c)(1)(B) would seem to cover such information, health care organizations should nevertheless proceed with caution because a regulator may reject that reading in favor of one that creates more protection of consumers.

On its face, the text of section 1798.145(c)(1)(B) appears to exempt not only certain kinds of *information* regulated by HIPAA, but also a certain kind of *organization*, namely, a "covered entity" who maintains patient information in a certain way: "This title shall not apply to any of the following: ... (B) ... a covered entity governed by [HIPAA] ... to the extent the ... covered entity maintains patient information in the same manner as ... [PHI]." In other words, the CCPA exempts an organization that "maintains patient information in the same manner" as PHI under HIPAA. The consequence of this reading is that a health care provider might be exempt as a whole; all of its *non*-health care information might qualify for the CCPA's HIPAA exemption so long as the health care provider protects "patient information" in the right way.

But this reading of the CCPA's HIPAA exemption might not be received well by a judge or assistant state attorney general reviewing a data incident after it has occurred. Hindsight might tempt an unsympathetic reader into limiting the exemption in subsection (B) to "patient information." Perhaps a judge would invoke the purpose of the statute, or the findings and declarations at the beginning of the bill. And while the broader category of "patient information" might include information that is not PHI, there is a lot it would not include. For example, IP addresses, cookies, or marketing data regarding people who have not become patients. In that case, such data would not fall under the HIPAA exemption and would instead be regulated by the CCPA.

The most prudent course may be to assume that the HIPAA exemption will cover only the PHI and patient information of HIPAA-regulated organizations, and to design privacy policies and practices accordingly. Then, if an incident occurs that leads to discussions with regulators or litigation, a health care organization might seek additional shelter under the broader exemption suggested by the actual text. In any event, organizations in the health care sector should review their data inventories carefully and reassess their privacy practices to account for the interaction between HIPAA and the CCPA.

[1] Exempt, too, are aggregate consumer information or de-identified information, "medical information" already covered by California's Confidentiality of Medical Information Act, and certain information collected as part of clinical trials. *See* Cal. Civ. Code § 1798.145(c)(1)(A), (C). (Note, however, that the definitions of deidentified information in the CCPA and HIPAA are not the same.)

Authored By

Michael L. Yaeger

Related Practices

Health Care
Cybersecurity and Privacy

Related Industries

Health Care