GT GreenbergTraurig
Kate Black ■ Blackk@gtlaw.com ■ 415.655.1296

CCPA Snapshot for Health and Life Sciences Companies

The CCPA is a new consumer privacy law in California. The CCPA requires most businesses to protect the personal information of Californian consumers. The core requirements of the CCPA include:

- Providing individuals with access and deletion rights over their personal information,
- Allowing individuals to opt out of any data sales and data transfers for monetary value,
- Creating a private right of action for consumers, including employees, if a data breach impacts their personal information.

Learn more about the CCPA's requirements here.

Health and Life Sciences companies are not fully exempt from the CCPA.
Personal information processed by health care and life sciences companies is exempt from the CCPA if it's 'protected health data', which includes:

- health information protected by HIPAA or the CMIA,
- clinical trial data collected under the Common Rule, or
- data maintained by a Covered Entity “in the same manner” as PHI under HIPAA.

Where health regulations stop, the CCPA steps in to further protect individual privacy. Personal information that is not protected health data will be subject to the CCPA. Common examples of personal information processed by health care and life sciences companies that will be subject to the CCPA include:

- Employee, applicant, and contractor data,
- Website data such as web traffic information such as IP address, and
- Marketing, social media, and public relations data.

Data de-identified under HIPAA may be subject to the CCPA.
Long story short, some de-identified PHI may also be subject to the CCPA’s requirements. While both HIPAA and the CCPA have exceptions for datasets that have been de-identified, the de-identification standards in the CCPA and HIPAA are not well aligned. As a result, there may be situations where data may be considered de-identified according to HIPAA’s Privacy Rule, yet not de-identified under the CCPA’s definition.

In order to be considered de-identified under the CCPA, information must meet two requirements. First, it must be stripped of identifiers so that it cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular individual. Second, the company must implement all of the following organizational measures:

- implement technical safeguards to prohibit re-identification of the consumer;
- implement business processes that prohibit re-identification and prevent inadvertent release of de-identified information;
- implement business processes to prevent inadvertent release of de-identified information; and
- make no attempt to re-identify the information.

The higher deidentification standards in the CCPA make it likely that some HIPAA de-identified data sets are still be considered personal information, effectively "falling out" of the protected health data exemption and into the CCPA's requirements.

Key steps to begin CCPA Compliance.
There are a few key steps that health care and life sciences companies can take to understand their compliable obligations under the CCPA:

- Determine the full scope of personal information outside of HIPAA but falling under the CCPA.
- Review your approach to de-identification and determine if it meets the CCPA standard.
- Map how your company processes personal information, and/or shares it with third parties.