Published on *The National Law Review* https://natlawreview.com

Health Sector Does Not Completely Avoid the CCPA by HIPAA Exemption

Article By:

Tara N. Cho

Nadia G. Aram

As the countdown to the January 1, 2020 effective date for the CCPA quickly approaches, healthcare entities and businesses in the health sector should exercise caution not to rely too heavily on the law's HIPAA-related exceptions as a complete pass to avoid complying with the CCPA. The CCPA is the most comprehensive and toughest privacy law in the U.S. to date. Although a California law, the CCPA imposes stringent requirements on businesses nationwide that collect personal data from Californians (and meet certain thresholds). Those requirements include a number of on-going obligations to consumers and are accompanied by strong enforcement powers for non-compliance as well as a private right of action for certain data breaches. HIPAA does not provide a private right of action. While the CCPA exempts certain entities and data governed by HIPAA from CCPA's scope, healthcare entities and related service providers should evaluate their systems, processes and data repositories to determine what (if any) personal information they collect is not outside the CCPA's reach. They could find themselves with certain data subject to the CCPA and some outside of its scope. What does this mean for the healthcare industry? Perhaps it's time to start thinking in terms of "HIPAA Plus" in a healthcare setting. Regulators, if the CCPA heralds a trend, are imposing new obligations related to the other personal data a healthcare entity, health plan, or related business maintains about a particular patient, employee, website visitor, or other person.

The CCPA broadly defines "personal information" to include 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." Personal information under the CCPA includes data elements commonly considered protected information under most state security and data breach laws such as Social Security numbers, certain demographic information, financial account information and biometric data. However, the CCPA also calls out Internet browsing and search history, IP addresses, and personal information used to create consumer profiles (e.g., purchasing preferences, behavior, psychological trends, attitudes, abilities, and similar inference-based characteristics), which have not been historically considered "personal information" in the U.S.

The CCPA does offer some reprieve for the healthcare industry from the breadth of what is "personal information" under the CCPA by providing the following exemptions:

- **Non-Profits: Certain** non-profits are exempt from the CCPA if the company does not fall within the definition of a "business," which means the entity is "organized or operating for the profit or financial benefit of its shareholders or other owners."

- **Medical Information or PHI:** The law does not apply to "medical information" governed by the California Confidentiality of Medical Information Act ("CMIA") or "protected health information" ("PHI") governed by HIPAA, that is collected by a HIPAA covered entity or business associate. •

- **HCPs or Covered Entities:** A "provider of healthcare" (as defined by the CMIA) and HIPAA covered entities (healthcare provider, healthcare clearinghouse, or health plan) are also exempted from the law, if such entities maintain patient information as though it was subject to the CMIA or HIPAA. Notably, "business associates" under HIPAA are not exempted alongside HIPAA covered entities under the CCPA.

- **Research Data:** Information collected as part of a clinical trial is also excluded from the CCPA when the trial is subject to the Common Rule. Although the Common Rule applies to federally-funded research studies, most drug and device manufacturers and other entities conducting studies involving human research subjects voluntarily adhere to requirements of the Common Rule. Absent additional guidance hopefully yet to come this year from the California legislature or California Attorney General clarifying aspects of the CCPA, it is unclear whether the CCPA exemption will only apply to institutions receiving federal research funding.

- **De-Identified Data:** The CCPA does not apply to "deidentified" data; however, while similar in concept to the HIPAA equivalent, the standards for de-identification under HIPAA and the CCPA do not entirely overlap. As a result, it is possible that data that meets the HIPAA de-identification standard may not meet the CCPA exemption for deidentified data.

Despite these noted exemptions, healthcare entities, health plans and other businesses operating in the healthcare sector likely create, maintain or otherwise process personal information that falls outside these exemptions. Therefore, businesses should evaluate data processing activities across operations to identify any such outliers. For example, the following data types could be subject to the CCPA:

- Personal information (not regulated by the CMIA or HIPAA) collected through websites, health apps, health portals, and other digital technology or connected devices

- Personal information processed by the non-healthcare components of a HIPAA hybrid entity or information processed between a non-profit institution and its CCPA-covered affiliates, partners or related entities

- Pending the fate of a proposed amendment that may exclude certain employee data, personal information about employees (and dependents) collected or processed in an employer function as opposed to a HIPAA-covered health plan (e.g., information related to life insurance, short-term disability claims, certain wellness programs, workers' compensation) as well as general employee information such as Social Security numbers, tax IDs, drivers' license numbers, biometric or demographic information (e.g., employment applications, tax forms, or other employee records)

- Personal information collected through in-person conferences, fundraisers, marketing events or similar activities

- Personal information processed for research that falls outside the CCPA's clinical research exemption (e.g., potentially data collected for privately-funded clinical trials, investigator and study staff information)

These are only a handful of possible examples of data that may fall outside the CCPA exemptions most applicable for the health sector. Therefore, while the California legislature has limited time left in session to make final decisions on proposed amendments to the CCPA and guidance from the California Attorney General is still pending, now is the time to take action despite unanswered questions and varied interpretation of this new law. All businesses, including healthcare entities, should take steps to: 1) identify data processing activities across their operations to determine what data (if any) is subject to the CCPA and where exemptions may apply; 2) coordinate with relevant stakeholders to form your strategic approach to compliance (e.g., will you take steps to meet an exemption, segment data such that the CCPA requirements only apply to a sub-set of information, or prioritize implementation with a risk-based approach); and 3) evaluate current policies, procedures and contracts for any necessary updates to comply with the CCPA (especially public facing online policies where lack of compliance may be quickly apparent). These are but a few of the recommended steps toward full-scale compliance. A waitand-see approach may not be the best strategy to respond to this broad-reaching privacy law given the often extensive background preparation involved for many businesses to comply with the CCPA and the number of "copy cat" laws pending in other states. The CCPA also has 12-month "look back" terms, and so has the potential to apply retroactively unless California's legislature or Attorney General intervene by way of amendments to, or regulations under, the CCPA.

Copyright © 2024 Womble Bond Dickinson (US) LLP All Rights Reserved.

National Law Review, Volumess IX, Number 256

Source URL:https://natlawreview.com/article/health-sector-does-not-completely-avoid-ccpa-hipaa-exemption