Privacy Alert
March 2021

New Requirements for Health Care Companies: CCPA and Proposed HIPAA Privacy Rule Changes

Recent changes to the California Consumer Privacy Act (CCPA) and proposed changes to the Standards for the Privacy of Individually Identifiable Health Information under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act) may ease certain privacy compliance requirements for health care companies but may also require changes in policies and contracts for compliance.

Gov. Gavin Newsom last September approved amendments to AB 713, a bill passed by the California State Legislature in 2019 to amend the CCPA. The amendments to the CCPA, which became effective as of Jan. 1, clarify the CCPA's exemption for deidentified health information, expand the scope of the medical research exemption, and create a new exemption for HIPAA business associates that is in line with existing exemptions for HIPAA-covered entities and for entities regulated by California's Confidentiality of Medical Information Act (CMIA). The amendments do impose new requirements on companies that disclose or sell deidentified health information.

The Department of Health & Human Services (HHS) issued a Notice of Proposed Rulemaking on Jan. 21 to modify the HIPAA Privacy Rule. HHS states that the proposed modifications would eliminate standards that impose unnecessary burdens while "continuing to protect the privacy and security of individuals' protected health information [PHI]." Covered entities and business associates may need to amend contracts and update policies and procedures if the proposed changes become part of the Privacy Rule. While some of these changes under the CCPA and HIPAA give health care companies more clarity and leeway with respect to their data use practices, these companies should be aware that this leeway comes with new contract and notice obligations.

Key Takeaways:

- The CCPA now contains an exemption for deidentified patient information that aligns with the HIPAA standard, but some companies in the health care sector will be subject to additional notice and contract requirements.
- AB 713 broadens the CCPA's exemption for medical research.
- HIPAA business associates now enjoy an exemption similar to those for HIPAA-covered entities and businesses regulated by CMIA, which could greatly expand the amount of health data that is exempt from CCPA regulation.
- Companies with HIPAA obligations may need to amend contracts and revise policies and practices if proposed modifications to the HIPAA Privacy Rule are finalized.

Attorney Advertising

CCPA and Deidentified Information

As originally enacted, the CCPA contained an exemption for deidentified data, but this exemption didn't align with HIPAA's deidentification standard. Now, as amended by AB 713, health information is exempt from CCPA regulation if it is (1) deidentified in accordance with HIPAA and (2) derived from information originally collected, created, transmitted or maintained by an entity regulated by HIPAA, CMIA or the Federal Policy for the Protection of Human Subjects, also known as the Common Rule.

AB 713 also contains a prohibition on reidentifying information, with exceptions for treatment, payment and health care operations as defined in HIPAA; public health activities; research conducted in accordance with the Common Rule; testing, analysis or validation of deidentification, or related statistical techniques (subject to certain contractual restrictions); and requirements of applicable law. HIPAA does not contain a direct prohibition against reidentification, so companies that have historically associated deidentified health information with elements of other data sets will need to evaluate their procedures to make sure they don't run afoul of the CCPA's new restrictions.

Companies that sell or disclose deidentified patient information are subject to additional requirements. These companies must state in their privacy policies that they sell or disclose this type of information, and they must specify whether the information was deidentified in accordance with the HIPAA expert determination method or the HIPAA safe harbor method.

Additionally, contracts for the sale or license of deidentified patient information must include:

- A statement that deidentified patient information is being sold or licensed
- A statement that reidentification is prohibited except for the reasons specified above
- A requirement that the purchaser or licensee of the deidentified patient information may not redisclose it except to a third party bound by the same or stricter restrictions and conditions, unless redisclosure is otherwise required by law

HIPAA does not contain similar requirements for contracts, so many agreements and service arrangements may need to be modified to comply with the CCPA as amended.

Business Associate Exemption Under the CCPA

AB 713 exempts a HIPAA business associate from CCPA regulation to the extent the business associate maintains, uses and discloses patient information in the same manner as information regulated by HIPAA or CMIA. This means, for example, that an entity that serves as a business associate of a HIPAA-covered entity may be able to apply the CCPA exemption for business associates to health data that it maintains in other contexts, such as information it maintains on behalf of a provider of a consumer-facing wearable or mobile health app.

Research Exemption Under CCPA

AB 713 provides a broader exemption for research than the CCPA's original exemption for clinical trial data. Under AB 713, information collected, used or disclosed in connection with research (as defined under HIPAA) that is subject to the Common Rule, ICH guidelines or the human subject protection requirements of the FDA is exempt from CCPA regulation.

Proposed Modifications to the HIPAA Privacy Rule

In its NPRM, HHS proposes to amend the Privacy Rule by:

- Adding definitions for the terms electronic health record (EHR) and personal health application.
- Modifying provisions on individuals' right of access to PHI by:
  - Strengthening individuals' rights to inspect their PHI in person, which includes allowing individuals to take notes or use other personal resources to view and capture images of their PHI
  - Shortening covered entities' required response time to no later than 15 calendar days (from the current 30 days), with the opportunity for an extension of no more than 15 calendar days (from the current 30-day extension)
  - Clarifying the form and format required for responding to individuals' requests for their PHI.
  - Requiring covered entities to inform individuals that they retain their right to obtain or direct copies of PHI to a third party when a summary of PHI is offered in lieu of a copy

  - Reducing the identity verification burden on individuals exercising their access rights
  - Creating a pathway for individuals to direct the sharing of PHI in an EHR among covered health care providers and health plans by requiring covered health care providers and health plans to submit an individual's access request to another health care provider and to receive back the requested electronic copies of the individual's PHI in an EHR
  - Requiring covered health care providers and health plans to respond to certain records requests received from other covered health care providers and health plans when directed by individuals pursuant to the right of access
  - Limiting the individual right of access to direct the transmission of PHI to a third party to electronic copies of PHI in an EHR (this proposal was added in response to a 2020 opinion by the U.S. District Court for the District of Columbia finding that HHS had exceeded its statutory authority under the HITECH Act by expanding individuals' rights to direct copies of their PHI to third parties in the 2013 HIPAA Omnibus Rule)
  - Specifying when electronic PHI (ePHI) must be provided to the individual at no charge
  - Amending the permissible fee structure for responding to requests to direct records to a third party (also in response to the 2020 opinion by the D.C. court)
  - Requiring covered entities to post estimated fee schedules on their websites for access to and disclosures of PHI, and to provide upon request individualized fee estimates and itemized bills related to requests for copies of PHI;
- Amending the definition of health care operations to clarify the scope of permitted uses and disclosures for individual-level care coordination and case management that constitute health care operations.
- Creating an exception to the "minimum necessary" standard for individual-level care coordination and case management uses and disclosures that would apply regardless of whether such activities constitute treatment or health care operations.
- Clarifying the scope of covered entities' abilities to disclose PHI to certain third parties that provide health-related services.
- Replacing the privacy standard that permits covered entities to make certain uses and disclosures of PHI based on their "professional judgment" with a standard permitting such uses or disclosures based on a covered entity's good faith belief that the use or disclosure is in the best interests of the individual. The proposed standard is more permissive in that it would presume a covered entity's good faith, but this presumption could be overcome with evidence of bad faith.
- Expanding the ability of covered entities to disclose PHI to avert a threat to health or safety when a harm is "serious and reasonably foreseeable," instead of the current stricter standard, which requires a "serious and imminent" threat to health or safety.
- Eliminating the requirement to obtain an individual's written acknowledgment of receipt of a direct treatment provider's Notice of Privacy Practices (NPP).
- Modifying the content requirements of the NPP to clarify individuals' rights with respect to their PHI and how they can exercise those rights.
- Expressly permitting disclosures to Telecommunications Relay Services (TRS) providers who assist persons who are deaf, hard of hearing, deaf-blind or who have a speech disability, and modifying the definition of business associate to exclude TRS providers.
- Expanding the permission to use or disclose PHI of armed forces personnel to cover all uniformed services personnel.

HHS is accepting comments on the NPRM through March 22. If HHS issues a final rule following the comment period, covered entities and their business associates would likely have no more than 60 days following its publication to bring their policies and practices into compliance with the Privacy Rule as modified.

Some of the proposed modifications, particularly the shortening of the time period for responding to access requests, would require covered entities to review and potentially revise their business associate agreements, their internal policies and procedures, and their consumer-facing privacy notices. Given the relatively short time period to come into compliance, companies with HIPAA obligations would do well to begin to review relevant policies and contracts now so that they can be prepared to quickly implement any necessary changes.

Related Professional

Angela Matney. . . . . amatney@loeb.com