BCLP. Client Intelligent

Insights

AB 713 – CCPA'S NEW DE-IDENTIFICATION AMENDMENT IS EFFECTIVE AS OF JANUARY 1 AND MAY REQUIRE OPERATIONAL CHANGES

Feb 01, 2021

Although it received little notice, the CCPA was amended effective January 1, 2021 to clarify and modify the exemption relating to de-identified data, with particular focus on medical data. Specifically, AB 713 amended the CCPA to state that data de-identified under the well-trodden methodologies in HIPAA was in fact exempt from the title. This is an important clarification for HIPAA covered entities and business associates. There has been ongoing uncertainty regarding whether information de-identified in accordance with HIPAA would fall outside the scope of the CCPA, because it is possible that information that meets one of the two HIPAA de-identification standards would not meet the broader and less objective standard set out by the CCPA.[1] In typical fashion, however, the California Legislature did not stop there—rather, AB 713 introduced a new raft of requirements, some of which will apply to entities that were not required to comply with CCPA previously.

First, AB 713 requires a business to disclose (a) *whether* the business discloses or sells personal information de-identified pursuant to HIPAA, and (b) if so, the chosen HIPAA methodology (i.e., Safe Harbor or Expert). This is a substantial change particularly considering that de-identified data has generally been considered outside the scope of the CCPA (subject to the definitional challenges discussed above), and because such disclosures are not required by HIPAA.

Second, while AB 713 provides that data derived from Protected Health Information that is de-identified under HIPAA is excepted,[2] the Amendment also states that re-identified data again is subject to state and federal law including HIPAA, the California analogue, and the Common Rule.[3] Specifically, "[i]nformation that met the requirements of subparagraph (A) [HIPAA de-identification standard] but is subsequently re-identified shall no longer be eligible for the exemption in this paragraph, and shall be subject to applicable federal and state data privacy and security laws, including, but not limited to, the Health Insurance Portability and Accountability Act, the Confidentiality of Medical Information Act, and this title." It is unclear how this statutory pronouncement squares with federal law and, more importantly, to whom the obligation would run (the party that originally provided the de-identified data or instead the recipient that has sought to

re-identify it). It would make sense that CCPA might apply to the parties who taken the steps to re-identify data, but this provision could also be read to impose obligations on the disclosing party as well, which cuts directly against the requirements of HIPAA. Under the HIPAA Safe Harbor standard, "[a] covered entity may determine that health information is not individually identifiable health information" if all identifiers listed in the regulation are removed[4] and the covered entity has no actual knowledge that re-identification is possible. Once this standard has been met, HIPAA does not impose ongoing obligations to monitor use by recipients. Moreover, even if the recipients were to re-identify such information, they would not be subject to HIPAA unless they were otherwise subject to HIPAA as a covered entity or business associate. Thus, the fact that a recipient may later surreptitiously re-identify a data set (perhaps through combination with other sources) likely does not impair the ability of the covered entity to rely on the Safe Harbor exemption for the original transmission.[5]

Third, the Amendment imposes new contracting requirements on parties to transactions involving de-identified data, and novel restrictions on re-identification. In fact, the statute bars re-identification subject to certain purpose-oriented exceptions that are generally aligned with acceptable uses under HIPAA.[6] The Amendment also requires that contracts for the sale of de-identified health must include a prohibition on re-identification if the contract executed on or after January 1, 2021.[7] It is here that the amendment arguably reaches beyond the original jurisdiction of CCPA. The statute purports to apply to all contracts between parties for the sale of de-identified data "where one of the parties is a person residing or doing business in the state."[8] Thus, this new contracting requirement may apply to non-profits, entities not doing business in California, and smaller entities heretofore exempt from the CCPA.

It is unclear how these provisions will be applied and enforced in practice, and/or whether organizations could successfully make the argument that (a) they are not subject to these obligations because they are a HIPAA governed covered entity or business associate (or an entity subject to similar state laws)[9] and, therefore, exempted from the application of the CCPA; or (b) these new obligations conflict with and are potentially overridden by other provisions of the CCPA, such as the exemption that expressly states that "The obligations imposed on businesses by this title shall not restrict a business's ability to: Collect, use, retain, sell, share, or disclose consumers' personal information that is de-identified or aggregate consumer information."[10]

Recommended Actions: Although this amendment creates new ambiguities, it is now in effect. Therefore, organizations should consider taking the following steps:

- Understand whether and how the organization utilizes patient information de-identified in accordance with HIPAA.
- Review and consider updating the business's privacy policy if the business sells or transmits *any* de-identified data and/or determine whether the company intends to rely on an argument

that its activities are otherwise excepted from the obligations of the CCPA.

- Review and update existing templates for prospective (post January 1, 2021) compliance with the contracting standards for the sale of de-identified data.
- Review existing business practices to ensure that the business itself does not re-identify data unless an exemption in AB 713 applies and/or it is using it for a purpose that would be subject to HIPAA or otherwise addressed by existing CCPA compliance efforts.

---

1. "'Deidentified' means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information." Ca. Civ. Code 1798.140(h).

2. Ca. Civ. Code 1798.146(a)(4)(A)(i)-(ii). Indeed, the exception *appears* to go beyond Protected Health Information to include de-identified information "derived from patient information that was originally collected, created, transmitted, or maintained by an entity regulated by the Health Insurance Portability and Accountability Act, the Confidentiality of Medical Information Act, or the Federal Policy for the Protection of Human Subjects, also known as the Common Rule."

3. *Id.* at (B).

4. *See* 45 CFR 514(b)(2)(i)(A)-(R).

5. Indeed, guidance from the Office of Civil Rights on this issue is clear-cut. The covered entity must essentially know that the data actually is not de-identifiable with some degree of specificity. OCR states the knowledge must be "clear and direct."

6. Ca. Civ. Code 1798.148(a).

7. *Id.* at (c).

8. *Id.*

9. Ca. Civ. Code 1798.146(a)(2) – (3).

10. Ca. Civ. Code 1798.145(a)(6).

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535
