Inconsistent HIPAA and CCPA De-Identification Standards Create Compliance Challenges

December 4, 2019

Daniel F. Gottlieb | Mark E. Schreiber

SUMMARY

A potential disconnect between the HIPAA de-identification standard and California Consumer Privacy Act (CCPA) definition of de-identified may pose hurdles for HIPAA covered entities, their business associates and other data aggregators. Businesses can protect themselves by taking key steps to reduce the risk of CCPA exposure when licensing or otherwise disclosing HIPAA de-identified data.

IN DEPTH

There is a potential disconnect between the Health Insurance Portability and Accountability Act of 1996 (HIPAA) de-identification standard and the California Consumer Privacy Act (CCPA) definition of de-identified data. The HIPAA Privacy Rule uses the term "de-identified" to refer to data that is not protected health information (PHI) for purposes of HIPAA. The CCPA uses the term "deidentified" to refer to data that is no longer personal information under the CCPA. For simplicity, this *On the Subject* uses the hyphenated "de-identified" spelling to refer to both.

The different de-identification language used in the CCPA creates a risk for HIPAA covered entities and business associates and other data aggregators that a data set de-identified under the HIPAA standard would be deemed to include personal information about California consumers under the CCPA. The disconnect imposes practical and compliance burdens on businesses that license or otherwise sell HIPAA de-identified data that is not adequately de-identified under the CCPA.

This *On the Subject* discusses steps that businesses can take to reconcile the HIPAA and CCPA de-identification requirements and reduce the risk of CCPA exposure when licensing or otherwise disclosing HIPAA de-identified data. These steps include:

- Updating HIPAA expert determinations to address CCPA
- Updating privacy and security policies to reflect the technical and procedural safeguards under the CCPA definition of de-identified data
- Using documentation to support the conclusion that the CCPA definition of de-identified data has been

satisfied.

These steps can help businesses avoid the notice, "do not sell," opt-out and other requirements of the CCPA.

Background

The recent statutory amendments to the CCPA adopted by the California legislature and proposed regulations issued by the California Attorney General have not clarified whether health information that has been de-identified in accordance with the HIPAA Privacy Rule meets the CCPA's definition of de-identified information. As the January 1, 2020, CCPA effective date rapidly approaches, HIPAA business associates and other businesses that aggregate and de-identify protected health information (PHI) are uncertain whether their HIPAA de-identified data sets with information about California consumers are personal information under the CCPA, and if so, what they must do to de-identify the data in accordance with the CCPA. HIPAA de-identified data is not PHI, and as such, may or may not meet either of the CCPA exemptions for PHI (even though the data was PHI before being de-identified). For more information about the amendments and proposed regulations, see our recent *On the Subjects* here and here, respectively.

HIPAA De-Identification Standard

The HIPAA Privacy Rule provides a standard for de-identification of PHI, which generally states that health information is not PHI if it does not identify an individual and there is no reasonable basis to believe that it can be used to identify an individual. The standard provides two methods—safe harbor and expert determination—by which health information can be designated as de-identified for purposes of the standard and thus used and disclosed outside the Privacy Rule's protections for PHI. Under both methods, de-identified data retains some risk of identification of the individuals (*e.g.*, patients of a healthcare provider) who are the subject of the information.

Neither method requires removal of identifiers of healthcare providers or others who serve the individuals who are the subject of de-identified information. Accordingly, HIPAA de-identified data may be de-identified with respect to patients, but may include names, national provider identifiers or other identifiers of healthcare providers or covered entity workforce members. CCPA does not except personal information about providers or workforce members from its definition of personal information, however.

Safe Harbor Method

To meet the safe harbor method, a HIPAA covered entity or business associate must remove 18 identifiers of the individual, or of relatives, employers or household members of the individual, including:

- Names
- Certain geographic subdivisions smaller than a state
- Elements of dates more specific than year
- Telephone numbers
- Email addresses
- Biometric identifiers
- Any unique identifying number, characteristic or code (except for certain permitted record re-identification codes that are not derived from or related to the individual).

In addition, the covered entity (or business associate) creating the de-identified information must not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information. One academic study using 1990 Census data estimated that the risk of re-identification of individuals in a HIPAA safe harbored data set is 0.04%.

Expert Determination De-Identification Method

A covered entity or business associate may also determine that health information is not PHI if an expert determines that the risk is *very small* that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information. The expert must have appropriate knowledge of and experience with statistical and scientific principles and methods for rendering information not individually identifiable. The expert must document the methods and results of the analysis that justify the determination.

De-Identification Under the CCPA

The CCPA generally defines personal information to mean "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Information is de-identified under the CCPA if "the 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 de-identified information:

1. Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
2. Has implemented business processes that specifically prohibit reidentification of the information.
3. Has implemented business processes to prevent inadvertent release of deidentified information.
4. Makes no attempt to reidentify the information."

Unlike other CCPA provisions, which specifically refer to HIPAA by cross-reference to the HIPAA regulations in the Code of Federal Regulations, the CCPA definition of de-identified data does not include a cross-reference to the Privacy Rule's de-identification standard. Instead, the CCPA definition of de-identified data is the reverse of the CCPA definition of personal information plus the four enumerated safeguards against re-identification.

Arguments for HIPAA De-Identification Equivalency to CCPA De-Identification

A business that maintains HIPAA de-identified data has reasonable arguments that the data also meets the CCPA definition of de-identified data, assuming that the business complies with the four safeguards. For example, the business may assert that data that meets the "very small risk of re-identification" requirement of HIPAA's expert determination method also "cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer" as required by the CCPA. A business can point to the analysis in its expert determination and also to the extraordinary efforts that a data set recipient would need to take to re-identify the data, meaning that it could not "reasonably" identify the individual. Further, a business's privacy policies and procedures limiting disclosure and re-identification of de-identified data can document that the business satisfies the four technical and procedural safeguards against re-identification.

Even if the business maintains linking codes that enable the re-identification of de-identified data subjects, the business may argue that the data cannot reasonably be associated with or linked to California consumers if the business secures the re-identification key from de-identified data users in accordance with the four safeguards.

CCPA Implications for Licensing Personal Information

If a business subject to the CCPA maintains HIPAA de-identified data that does not meet the CCPA definition and thereby includes "personal information" about California consumers, then the business would need to honor California consumers' rights under the CCPA and otherwise comply with the CCPA. These include the right to opt-out of the sale of personal information and the right to request deletion of personal information, each of which may create significant practical problems for the business.

The business also may be required to register as a data broker with the California Attorney General as a condition to license or otherwise disclose the data for cash or other consideration. Under the CCPA, a data broker is a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. Accordingly, if a HIPAA covered entity has direct relationships with patients or other individuals, and a business associate only has an indirect relationship through the covered entity, then the business associate may be a data broker.

Even if the business does not "sell" personal information (because it meets the CCPA definition of de-identified

data), it must still make an affirmative statement in its privacy policy that it "does not sell and will not sell personal information," according to the proposed CCPA regulations.

Right to Opt-Out

The CCPA requires a business to provide a notice to California consumers, at or before the time of collection of a consumer's personal information, that describes the categories of personal information to be collected and the purposes for which the personal information will be used. Based on the proposed regulations issued by the Attorney General, a business that does not collect personal information directly from consumers does not need to provide a notice at collection to the consumer, but would need to notify the consumer that the consumer has the right to opt out of the sale of the consumer's personal information before selling the consumer's personal information. Thus, before a data aggregator could license (or otherwise disclose) HIPAA de-identified data that includes personal information about California consumers for monetary or other consideration, the business would need to notify the consumers of their right to opt out of the sale of personal information.

Based on the proposed regulations, the business may deliver the notice of the right to opt-out by either (1) contacting the consumer directly and providing notice of the right to opt-out of the sale of personal information, or (2) contacting the source of the personal information to confirm that the source provided a notice at collection to the consumer in accordance with the proposed regulations, and to obtain signed attestations from the source describing how the source gave the notice at collection and including an example of the notice.

Neither of these two notice methods is practical for many service providers that receive PHI from multiple HIPAA covered entity data sources and then create de-identified data as a business associate. The business associate may not have a convenient way to contact consumers directly, and the covered entity data sources may not want to notify their patients that a business associate is commercializing their personal information. Other business associates may enter into end user license agreements or other forms of user agreements with California consumers.

Right to Request Deletion of Personal Information

Subject to certain exceptions, the CCPA provides California consumers with the right to request that a business delete personal information collected or maintained by the business. A business has 45 days to respond to a request to delete personal information and may request a 45-day extension. Unless the business has a basis to deny the request, it must take one of the following actions:

- Permanently and completely erase the personal information on its existing systems (provided that it may delay deletion of personal information on an archived or back-up system until the system is next accessed or used).

- De-identify the personal information in accordance with the CCPA definition of de-identification (assuming that there is a difference between HIPAA and CCPA standards).
- Convert the personal information into "aggregate consumer information," which CCPA defines as "information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device." In other words, the HIPAA-de-identified data set could not have individual patient-level data about California consumers.

If a business maintaining HIPAA de-identified data must honor deletion requests from California consumers, the deletion requests will create various practical challenges for the business. For example, deletions will make it more difficult to undertake longitudinal data analyses unless the analyses meet an exception (such as the exception for research conducted with informed consent). High volumes of deletions also could affect data licenses that require minimum numbers of data subjects or records in the licensed data.

Practical Steps to Mitigate the Risk that HIPAA De-Identified Data Is Personal Information Under CCPA

A business maintaining HIPAA de-identified data with data subjects who are California consumers should consider the following techniques to mitigate the risk that individuals or the California Attorney General would deem the data to include personal information under the CCPA:

- If the business has obtained an expert determination that a data set is de-identified under HIPAA, consider re-engaging the expert to update the determination to include a conclusion that the data set also meets the CCPA definition of de-identified data (or obtain a new opinion reflecting the conclusion from an expert in statistical disclosure control principles).
- Update relevant privacy and security policies, procedures and practices to reflect the four safeguard requirements in the CCPA definition of de-identified data, including the business's technical safeguards and business processes that prohibit re-identification, its business processes to prevent inadvertent release of data, and an affirmation that it makes no attempt to reidentify the data.
- Amend data license agreements and other contracts with third parties to prohibit re-identification of California healthcare providers and other California consumers (to the extent that they do not already prohibit re-identification to comply with a HIPAA de-identification method or for commercial reasons).
- Remove identifiers of physicians and other California consumers who served patients and are identified in the data (unless the business will provide notice of opt-out rights, honor opt outs and comply with other applicable CCPA requirements).
- Obtain a memo or other document from legal counsel to memorialize the legal analysis and safeguards supporting the conclusion that data is de-identified in accordance with the CCPA.

The McDermott Difference

If you maintain HIPAA de-identified data concerning California consumers, don't hesitate to reach out to the authors of this *On the Subject* or your regular McDermott lawyer to consider steps to mitigate risk that the data will be deemed personal information.

GET IN TOUCH

Daniel F. Gottlieb
View Profile

Mark E. Schreiber
View Profile