AHLA WEEKLY

11/1/2019

HIPAA and the CCPA: What Health Care-Related Organizations Need to Know

By Charles E. Harris, II and Elizabeth Mann, Mayer Brown

The California Consumer Privacy Act (CCPA or Act),[1] effective January 1, 2020, strengthens consumer privacy rights for California residents by providing them greater control over and transparency into their personal data. The Act contains an exclusion for health information governed by the federal privacy and security rules promulgated by the U.S. Department of Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act (HIPAA).[2] It also excludes "medical information" subject to California's health privacy law, the Confidentiality of Medical Information Act (CMIA).[3] While these carve-outs are broad, they may not be expansive enough to cover all personal data that entities engaged in health care-related functions regularly collect and process. Indeed, some of these organizations may need to modify their practices to comply with the CCPA. This article discusses the CCPA's core provisions; instances where, despite the exclusions described above, the Act may cover data that health care-related organizations collect; and what steps these entities might take in anticipation of the CCPA.

HIPAA and the CMIA

HIPAA, enacted in 1996, required HHS to create national standards requiring "covered entities," meaning certain health care providers, health plans, and health care clearinghouses, to protect the privacy and security of health information.[4] To fulfill its obligation, HHS promulgated the Privacy Rule (effective in 2003) and the Security Rule (effective in 2005). The Privacy Rule safeguards protected health information (PHI) by regulating how covered entities may use and disclose this information and requiring these entities to put measures in place to protect the privacy of the data.[5] PHI means any individually identifiable information created, maintained, transmitted or received by covered entities that relates to the provision of health care or the payment for health care services. Thus, PHI includes medical records, lab tests, and medical bills. To be sure, health information will normally be considered PHI when it includes common identifiers, such as name, physical and email addresses, birth date, Social Security number, and IP address. The Security Rule, which applies to PHI in electronic form (ePHI), requires covered entities to employ administrative, physical, and technical safeguards to protect the ePHI.[6]

The Health Information Technology for Economic and Clinical Health Act (HITECH), passed in 2009, expanded the reach of HIPAA by extending the applicability of certain Privacy Rule and Security Rule requirements to "business associates" of covered entities and strengthening many privacy and security obligations.[7] "Business associates" are entities that provide services to or perform certain functions for covered entities that involve the use or disclosure of PHI.[8] HHS' Omnibus Rule, effective in 2013, implemented the changes to the Privacy Rule and Security Rule that HITECH initiated.[9] All told, as it stands today, both covered entities and businesses associates must comply with the key requirements of the Privacy and Security Rules as well as HHS' Breach Notification Rule.[10]

The CMIA also prescribes privacy protections for medical information. Medical information, similar to the definition of PHI, means "individually identifiable information, in electronic or physical form, in

possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment."[11] "Individually identifiable" means medical information that contains "personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, [email] address, telephone number, or social security number."[12] A "provider of health care" under Section 56.05 of the CMIA includes a broad range of licensed health care professionals as well as licensed clinics, health dispensaries, or health facilities.[13]

The CCPA

California Governor Jerry Brown signed the amended version of the CCPA on September 23, 2018. It applies to for-profit companies that conduct business in California, that collect and direct the processing of personal information of California residents (which the Act defines as "consumers"), and that satisfy one of the following thresholds: (1) has annual gross revenues over $25 million; (2) sells, buys, or otherwise receives the personal information of 50,000 or more California residents, households, or devices; or (3) derives 50% or more of its annual revenue from selling the personal information of California residents.[14] A California resident, for the purposes of the CCPA, is an individual consumer who is a permanent California resident or who lives outside the state for a temporary or transitory purpose.[15] And "personal information" means "information that identifies, relates to, describes, is capable of being associated with" an individual consumer or household, including name, alias, postal address, IP address, email address, Social Security number or driver's license number, health information, certain physical characteristics, Internet activity data, and employment information.[16]

The CCPA grants California residents new rights with respect to their personal information. Most critically, consumers have the right to, with certain exceptions:

- request that a covered business delete any personal information that the business has collected from them,[17]
- request that a covered business that collects personal information disclose the categories of and specific personal information the business collected in the preceding 12 months, the categories of sources from which, and third parties from whom, the business collected the personal information and the business or commercial purpose for collecting or selling personal information,[18]
- request that a covered business that sells or discloses their personal information identify the categories of personal information that the business collected and sold in the previous 12 months, the categories of third parties to whom the business sold the information or the categories of personal information that the business disclosed about them for business purposes,[19] and
- direct that a covered business that sells personal information to third parties not to sell their personal information (known as the "right to opt-out").[20]

Furthermore, a covered business must not discriminate against consumers because they exercised any of the rights set forth above by, among other things, denying or charging different rates for goods or services or offering a different level or quality of goods or services.[21]

The CCPA also places certain compliance obligations on covered businesses. For instance, a covered business must:

- provide consumers a toll-free telephone number or website to allow them to request the information discussed above,[22]

- disclose requested information to consumers for free and generally within 45 days (consumers may request information twice within a 12-month period),[23]
- update their online privacy policy or website to explain certain consumer rights outlined above, list the categories of personal information the business will and have collected, sold, or disclosed for business purposes in the preceding 12 months, and indicate how they will use consumers' personal information,[24]
- train employees responsible for handling consumer inquiries about the business's privacy practices, its compliance with the CCPA, and how to direct consumers to exercise their rights under the Act,[25] and
- provide a link on their website to enable consumers to opt out of the sale of their personal information.[26]

Also, covered businesses will effectively need to update their vendor agreements to contain prescriptive provisions prompted by the CCPA's requirements.[27]

Another critical feature of the Act is that it establishes a framework for California residents to bring a lawsuit against a business if the consumer's personal information "is subject to an unauthorized access . . . or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices."[28] A consumer may recover the greater of (1) statutory damages no less than $100.00 per incident and no more than $750.00 or (2) actual damages.[29] But before bringing a lawsuit that seeks statutory damages on an individual or class-wide basis, a consumer must provide notice to the business specifying how it violated its duty to protect personal information and allow the business 30 days to cure the defect.[30] No action will lie if the business cures the alleged violation, provided that the consumer does not later determine that the business did not, in fact, cure the defect or it continues to violate its obligations.[31] No notice, however, is required before a consumer brings a lawsuit to recover *actual* damages resulting from a business's violation.[32]

The CCPA's Health Care-Related Exclusions

The CCPA has two broad exclusions related to health data, each of which references both the CMIA and HIPAA. The Act, states, in pertinent part:

> This title shall not apply to any of the following:
>
> (A) Medical information governed by the [CMIA] or [PHI] that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by [HHS] [i.e., the Privacy, Security, and Breach Notification Rules].
>
> (B) A provider of health care governed by [section 56.05 of the CMIA (*see* above)] or a covered entity governed by the privacy, security, and breach notification rules issued by [HHS], to the extent the provider or covered entity maintains patient information in the same manner as medical information or [PHI] as described in subparagraph (A) of this section.[33]

To analyze these exclusions, it helps to isolate them by those that derive from the CMIA and those that derive from HIPAA.

The CMIA Exclusions

The CCPA carves out (1) "medical information" (defined above) governed by the CMIA, and (2) "provider[s] of health care" to the extent they protect "patient information" in the "same manner as medical information."[34] The exclusion for medical information is wide-ranging as the CMIA defines the term to include both data "in possession of" and "derived from" a multitude of individuals and

entities (i.e., health care providers, Knox-Keene licensed health insurers, pharmaceutical companies, and their contractors).[35] The exclusion related to patient information seems coextensive with the first exclusion, unless "patient information" could be defined more broadly than "medical information." While neither the Act nor the CMIA define "patient information," the CMIA defines "patient" as "any natural person . . . who received health care services from a provider of health care and to whom medical information pertains."[36] Given this definition, it looks as if most information about a "patient" would overlap with the term "medical information." Besides, it is difficult to imagine when and why a health care provider would maintain patient information in a different manner than it maintains medical information.

The HIPAA Exclusions

The Act also carves out (1) PHI collected by covered entities or business associates subject to the Privacy, Security, and Breach Notification Rules, and (2) covered entities governed by these implementing regulations to the extent they protect "patient information" in the "same manner" as PHI.[37] The PHI-related exclusion is seemingly as broad as the medical-information-related exclusion, given that it covers data created, maintained, transmitted, or received by covered entities, as well as such information shared with business associates. Also, like above, it seems that the definition of PHI encompasses patient information, and, even if it somehow does not, most covered entities likely treat patient information and PHI the same.

Health Care-Related Data Possibly Subject to the CCPA

The major difficulty for covered entities stemming from the text of the CCPA's carve-out is that it does not create a blanket exclusion for health care-related organizations that must comply with HIPAA and its implementing regulations or the CMIA. Instead, it omits only medical information or PHI from the Act's coverage, leaving in play data that does not fall within the definition of those terms. Here are some instances, with examples, when data created, maintained, transmitted, or received by health care organizations may still fall under the Act:

Data unrelated to the provision of health care or the payment for health care services. Health care-related organizations are launching blogs and Internet marketing campaigns to drive potential patients to their websites and to foster an interactive online community of brand loyalists. For example, a major managed health care company created a marketing campaign called "We Dare You," whereby followers visited the company's website to read about monthly "dares" to make one small healthy change or enter contests. The company's privacy policy states that it "uses various technologies . . . to gather information from our website visitors such as pages visited and how often they are visited, and to enable certain features on this website." While this online tracking data is not PHI (or medical information) that, among other things, is linked to an individual's health care, the information arguably constitutes personal information under the CCPA.[38]

Health data that is de-identified in accordance with the Privacy Rule may nonetheless be subject to the CCPA. The CCPA does not "restrict a business's ability" to "collect, use, retain, sell, or disclose consumer information that is deidentified."[39] Under the Act, de-identified is defined as "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 the business: (1) has implemented processes and technical safeguards to *prohibit re-identification* and inadvertent release of the information and (2) makes no attempt to reidentify the information.[40] To constitute de-identified health information under the Privacy Rule, data must not identify an individual and there must be no reasonable basis to believe that the information can be used to identify an individual. In other words, the information must not be "individually identifiable."[41] Health information that has been de-identified in accordance with the Privacy Rule is not considered PHI, and it is probably not considered medical information under CMIA either.[42]

Where the discrepancy lies is that the Privacy Rule does not prohibit re-identification like the CCPA. It provides that "[a] covered entity may assign a code or other means of record identification to allow information de-identified . . . to be re-identified by the covered entity" if the entity complies with certain conditions.[43] The instances when health care organizations allow for the re-identification of data are undoubtedly rare. However, there could be cases where de-identified health information would not fall within the exclusions described above (as it is not PHI or medical information) or the definition of de-identified under the CCPA—but would fall under the definition of personal information under the Act. For example, the Healthcare Cost and Utilization Project developed the State Inpatient Databases (or SID), which are de-identified databases that contain hospital discharge data from people in 49 states, including such demographic characteristics as sex, age and, for some states, race.[44] This SID data arguably represents personal information under the CCPA if it is in a form that allows someone to reidentify the data.[45]

Data sets created from health data may be subject to the CCPA. Many health care organizations, namely health plans, use health data collected from wearables to understand how to drive consumer value, identify unmet needs, enhance risk assessments, and improve products and services. These organizations ordinarily treat wearable data as well as any separate data sets they create from the data as PHI or medical information governed, respectively, by HIPAA and the CMIA. While we mostly disagree with this position, some commentators have argued that the discrete data sets created from the wearable data are not PHI or medical information and should thus be considered personal information under the CCPA. This is because, first, the definition of personal information, by reference, includes "medical information" and "health insurance information."[46] In addition, personal information includes "[i]nferences drawn" from such information to "create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."[47]

***

Some commenters have expressed concern that certain exclusions set forth in the definition of PHI under the Privacy Rule might bring certain data that health care-related organizations regularly process within the coverage of the CCPA. We do not share that concern because, although this excluded data may not be PHI, it is nonetheless medical information under the CMIA. As noted above, the Act excludes PHI "or" medical information.[48] For example, the Privacy Rule states that PHI excludes "individually identifiable health information" contained in "employment records held by a covered entity in its role as employer."[49] But the CMIA, in many respects, provides stronger privacy protections for medical information than HIPAA. In this case, the CMIA, in contrast to the Privacy Rule, requires employers who receive medical information to "establish appropriate procedures to ensure the confidentiality and protection from unauthorized use and disclosure of that information."[50] That said, there is an open question as to whether the CCPA applies to employee data. In fact, a bill to amend the CCPA is pending before the California legislature that would expressly exempt most employee data from the Act's application.[51]

Potential Compliance Steps

Here are some initial steps health care-related organizations can take to evaluate whether they need to comply with the Act and become CCPA-ready.

Are you a covered business? Determine if you are a covered business under the Act (discussed above).

Know your personal data and if it is governed by the CCPA. Identify and catalogue any personal data of California residents that your business collects, processes, discloses, and stores, including any data sets derived from the information, and determine how the data flows through the

organization. This inventory would allow the company to more effectively evaluate whether it is subject to the CCPA. If an organization determines that it is subject to the Act, but also covered by HIPAA or CMIA, then consider what personal information the organization collects that might be covered by the Act's carve-outs.

Review and update operational policies and procedures. Organizations that collect and process personal information covered by the CCPA should review policies and procedures for handling such data and revise the policies and procedures, as necessary, to comply with the consumer requests and directions discussed above.

Update privacy policies, websites, and training. As discussed above, covered businesses should update their privacy policies or websites, among other things, to explain the consumer rights under the CCPA. They should also revise their websites to allow consumers to request information about their personal data and to opt out of the sale of their information. As also mentioned above, these companies will need to train the appropriate employees on the CCPA.

Notice to vendors. Covered businesses should inform vendors that provide services requiring them to process personal information subject to the CCPA of the need to comply with the Act. As noted above, the organizations may also need to update their vendor agreements to include specific terms requiring vendors to comply with consumer instructions.

Monitoring and auditing. Covered companies should establish proper procedures to monitor and audit their compliance with the CCPA and update their policies and procedures based on the information that they learn.

***

It is worth noting in closing that, on October 11, 2019, California Attorney General Xavier Becerra released proposed regulations for the CCPA.[52] The current iteration of the regulations address how businesses can comply with various aspects of the Act, including: (1) notifications to consumers of their rights under the Act; (2) handling consumer requests regarding personal information; (3) verifying consumer requests; (4) protecting personal information of minors under 16 years of age; and (5) specifics regarding the anti-discrimination provisions. The proposed regulations do not mention the carve-outs discussed above.

About the Authors:

Charles E. Harris, II (charris@mayerbrown.com): Charles E. Harris, II is a partner in Mayer Brown's Chicago office. A portion of his varied practice focuses on advising clients regarding health care-related privacy and cybersecurity compliance matters and breach response. In particular, Charles has assisted insurers, higher education institutions, service providers, and health care organizations in complying with the HIPAA Privacy, Security, and Breach Notification Rules. Also, notably, Charles has passed the Certified HIPAA Privacy Security (CHPSE) exam. Prior to joining Mayer Brown, Charles served as a law clerk to the late Judge David D. Dowd Jr., of the United States District Court for the Northern District of Ohio.

Elizabeth Mann (emann@mayerbrown.com): Elizabeth Mann co-leads Mayer Brown's significant Health Care practice. She concentrates her practice on health care transactional and litigation matters. For many years, Elizabeth has advised a nationwide health care organization that insures, delivers, and administers clinical care in 50 states. This organization is reimbursed by both private and public payors. She has advised this organization with respect to regulatory, contracting, reimbursement, ERISA compliance, and litigation matters. Elizabeth is familiar with the significant regulatory changes resulting from the enactment and implementation of the ACA, and the ongoing

change requirements resulting from the expansion of government coverage under both Medicare and Medicaid. She advises participants in all aspects of the health care system, including insurers, provider groups, group purchasing organizations, hospital systems, pharmacy benefit managers, and providers of senior care living facilities and medical services. Elizabeth has a great deal of experience advising purchasers of, lenders to and investors in, health care organizations concerning both the target's regulatory compliance and relevant trends in the health care industry. She has advised concerning investments in hospital systems, provider organizations, drug and device companies, and health care payors.

Endnotes:

[1] Cal. Civ. Code § 1798.100 *et seq*.

[2] 42 U.S.C. § 1320d *et seq*.

[3] Cal. Civ. Code § 56.05 *et seq*.

[4] *See* Pub. L. No. 104-191, 110 Stat. 193645; *see also* 45 C.F.R. § 160.103.

[5] *See id*. §§ 160, 164.

[6] *See id*. §§ 160, 162, 164.

[7] *See* 42 U.S.C. §§ 17921–17954.

[8] 45 C.F.R. § 160.103.

[9] 78 Fed. Reg. 5566 (Jan. 25, 2013).

[10] *See* 45 C.F.R. §§ 164.400-414.

[11] Cal. Civ. Code § 56.05(j).

[12] *Id*.

[13] *Id*. § 56.05(m).

[14] *Id*. § 1798.140(c).

[15] *Id*. § 1798.140(g).

[16] *Id*. § 1798.140(o).

[17] *Id*. § 1798.105(a).

[18] *Id*. §§ 1798.110(a), 1798.130(a)(3).

[19] *Id*. §§ 1798.115(a), 1798.130(a)(4).

[20] *Id*. § 1798.120(a).

[21] *Id*. § 1798.125(a).

[22] *Id*. § 1798.130(a).

[23] *Id*. §§ 1798.100(d), 1798.130(a).

[24] *Id*. §§ 1798.100(d), 1798.130(a).

[25] *Id*. § 1798.130(a).

[26] *Id*. § 1798.135(a).

[27] *See*, *e.g.*, *id*. § 1798.105(a) (when consumers request the deletion of their personal information, a business "shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information").

[28] *Id*. § 1798.150(a)(1).

[29] *Id*.

[30] *Id*. § 1798.150(b).

[31] *Id*.

[32] *Id*.

[33] *Id*. § 1798.145(c)(1)(A) (internal citations omitted).

[34] *Id*. § 1798.145(c)(1).

[35] *Id*. § 56.05(j).

[36] *Id*. § 56.05(k).

[37] *Id*. § 1798.145(c)(1).

[38] *Id*. § 1798.140(o)(1)(A) (personal information includes "information regarding a consumer's interaction with an Internet Web site").

[39] *Id*. § 1798.145(a)(5).

[40] *Id*. § 1798.140(h).

[41] 45 C.F.R. § 164.514(a).

[42] *See London v. New Albertson's, Inc*., No. 08-CV-1173, 2008 WL 4492642, at *5 (S.D. Cal. Sept. 30, 2008) ("The Court concludes that by the plain language of the statute prohibiting only the subsequent use or disclosure of 'medical information,' Plaintiff has failed to allege a claim for relief under the CMIA for Defendants [sic] use and sale of de-identified information").

[43] 45 C.F.R. § 164.514(c).

[44] *See* https://www.hcup-us.ahrq.gov/sidoverview.jsp#data.

[45] Cal. Civ. Code § 1798.140(o)(1)(C) (personal information includes "[c]haracteristics of protected classifications under California or federal law").

[46] *Id*. § 1798.140(o)(1)(B) (incorporating id. § 1798.80(e)).

[47] *Id*. § 1798.140(o)(1)(K).

[48] *Id*. § 1798.145(c)(1)(A).

[49] 45 C.F.R. § 160.103.

[50] Cal. Civ. Code § 56.20.

[51] *See* AB 25, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB25.

[52] *See* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf.