# California Attorney General Issues Draft Regulations for CCPA

*October 16, 2019 – Dorsey Health Law*
by Joseph Lynyak, Erin Bryan, Robert Cattanach, and Jamie Nafziger

The Dorsey Health Law blog team keeps readers up-to-date on relevant topics in the health care industry. In order to do so, the members of the blog team communicate regularly with other practice groups within the firm for applicable updates from client publications. For this post, we would like to thank Dorsey's Joseph Lynyak, Robert Cattanach, Jamie Nafziger and Erin Bryan for the following e-newsletter update:

**1. Introduction**

On October 11, 2019, the California Attorney General (the "California AG") issued draft regulations (the "Draft Regulations") pursuant to his authority under the California Consumer Privacy Act of 2018 ("CCPA").[1] The publication of the Draft Regulations commences the public comment period during which numerous interpretative issues relating to the implementation of the CCPA hopefully will be addressed and resolved.

Unfortunately, the California AG chose to limit the Draft Regulations to basic process issues relating to the overall structure of the CCPA, and elected not to address many of the more difficult compliance problems identified by industry participants. More troubling is the inclusion of additional procedural steps that a covered "business"[2] must follow when complying with "requests" for "personal information"[3] ("PI"). (If ultimately adopted, several of these additional compliance obligations could likely create technical and unintended violations of the CCPA.)[4]

This Alert provides an initial analysis of the approach taken by the Draft Regulations, as well as suggestions for participating in the rule-making process.[5]

**2. Discussion**

**Analysis of the Draft Regulations**

The Draft Regulations were issued by the California AG pursuant to authority delegated to him by Section 1798.185 of the CCPA. Notwithstanding the fact that the Draft

## Related People

- Joseph Lynyak
- Erin Bryan

## Related Capabilities

- Healthcare & Life Sciences
- Healthcare Transactions & Regulations
- Healthcare Litigation
- Medical Devices

Regulations are proposals and not yet final, the Draft Regulations establish a "backbone" based upon which covered businesses may begin to evaluate whether their implementation and compliance programs appear reasonable.

The Draft Regulations are comprised of seven "Articles"; Articles 1 and 7 contain definitions and a severability clause, whereas Articles 2 through 6 are the implementing provisions of the CCPA, and address:

- The notification process by covered business to California "consumers" of their rights under the CCPA[6]
- The processing of "verifiable consumer requests"[7]
- The verification of identify for consumer requests[8]
- Special rules for minors' PI,[9] and
- Determining value to comply with the anti-discrimination provisions of the CCPA

Articles 2 through 6 of the Draft Regulations will be addressed separately below.

**A. General**

In numerous provisions scattered across Articles 2 through 6, the Draft Regulations establish varying degrees of care that must be exercised by a business when dealing with a consumer, including identifying the consumer, evaluating the sensitivity of a consumer's request, and responding in a manner that protects a request for data or to delete PI.[10]

In addition, borrowing from federal consumer law that consumer disclosures be "clear and conspicuous," among other things required notices must be easily understood, formatted, and accessible to consumers, and provided in the languages in which a business interacts with consumers.[11]

From a drafting perspective, the Draft Regulations intentionally conflate non-internet-based business operations with partial or sole internet contact between businesses and consumers by interrelating and cross-referencing CCPA obligations. This approach (which may be necessary for brevity's sake yet nevertheless complicated) will require businesses to carefully parse through the Draft Regulations' compliance mandates in order to identify various subcategories of business models that might apply and may require differing compliance obligations.

**B. The Notification Process of a Consumer's Rights**

Article 2 sets forth several disclosures that have to be prepared and provided by a business to a consumer. It is by far the most instructive of the five Articles, and indicates the content that must be included in disclosures provided to consumers.

Article 2 of the Draft Regulations sets forth general principles when providing a disclosures of how a business collects PI, and indicates that a notice must contain the following information:

- A list of the categories of PI about consumers to be collected,
- For each category of PI, the business or commercial purpose(s) for which it will be used,
- If the business sells PI, the link titled “Do Not Sell My Personal Information” or “Do Not Sell My Info,” and
- A link to the business’s privacy policy.[12]

Article 2 imposes an expanded disclosure requirement when describing categories of PI, including a requirement that a business explain the business or commercial purpose for which PI will be collected. Further, a specific prohibition states that if a business intends to expand the scope of PI being collected, it must first provide a new disclosure to the consumer (which confirms that a new disclosure process must be undertaken by a business).[13]

Article 2 addresses several subcategories of notices that must be provided. For example, Article 2 addresses the notice that has to be provided regarding the right of a consumer to “opt-out” of the sale of PI (assuming an exception does not apply).[14] Depending upon the nature of the contact between the business and the consumer, a notice of a consumer’s opt-out right must include the following:

- A description of the consumer’s right to opt-out of the sale of their PI,
- The web-based form by which the consumer can submit their request to opt-out online (or, if the business does not operate a website, the offline method by which the consumer can submit their request to opt-out),
- Instructions for any other method by which the consumer may submit their request to opt-out,
- Any proof required when a consumer uses an authorized agent to exercise their right to opt-out, and
- A link or the URL to the business’s privacy policy (or, in the case of a printed form containing the notice, the URL of the webpage where consumers can access the privacy policy).[15]

Another subcategory of notice and disclosure is a notice of financial incentives that describes the incentive being offered, the material terms of the financial incentives and the right of the consumer to withdraw at any time.

Finally, Section 999.308(b) the Draft Regulations requires a detailed and expanded description of a businesses’ privacy policy. The privacy policy must be posted on a business’s website (or posted in a conspicuous place if the business dose not operate a website), and must include:

- The right to know about the collection, disclosure and sale of PI,
- The right to request deletion of PI,
- The right to opt-out of the sale of PI,
- The right to non-discrimination for the exercise of a consumer’s CCPA rights,
- The use of an authorized agent,
- A contact for additional information,
- The date the business’ privacy policy was last updated, and

- If Section 999.317(g) of the Draft Regulations applies, the metrics required or a link to it.[16]

**C. The Processing of Verified Consumer Requests by Covered Business**

Article 3 of the Draft Regulations contains a somewhat complicated set of requirements that vary depending upon the mode of conducting business between a business and a consumer.

As an initial matter, the Draft Regulations indicate that a business must provide two or more methods for submitting requests to know about PI, which must include a toll-free telephone number, along with several other acceptable methods that may be employed. However, while a request to delete PI must include two permissible methods of making the request, a toll-free number (while permissible) is not mandatory.[17] Importantly, any method for making a request must "reflect the manner in which the business primarily interacts with a consumer."[18] If a consumer makes a request that is not a designated methodology selected by the business, the business may choose to treat the request as having been made through a proper channel, or else must contact the consumer and provide specific directions to submit a request properly.[19]

Following the receipt of a request to know or a request to delete, the Draft Regulations add a new procedural step that is not included in the statutory language of the CCPA—which is a requirement within 10 days of the receipt of a request the business must notify the consumer that the request has been received and how the request will be processed. (It appears that this new 10-day notice falls within the CCPA statutory deadline of 45 days to respond and up to a maximum of 90 days[20].)[21]

The Draft Regulations contain detailed instructions for responding to requests to know and request to delete—the emphasis is placed on verification of the identification of the consumer. If verification is not possible, a business may decline to respond to the request, but must notify the consumer that the denial was based upon the failure to properly identify the consumer. In the instance in which the consumer has a password-protected account with a business, the business may provide a secure portal for retrieving the requested data.

In regard to a request to opt-out, a business must provide two alternative methods to submit a request to opt-out, including a mandatory interactive web-based form using a link entitled "Do Not Sell My Personal Information," or "Do Not Sell My Info" on the business's website or mobile application.[22] (Other alternative methods include a toll-free number, a designated email address, a form submitted in person, or an electronic mechanism to indicated the consumer's choice to opt-out.) A business may offer a consumer the option to opt-out of sale of certain categories of PI, provided that the opt-out of the sale of all information is more prominently displayed. A request to opt-out must be acted upon within 15 days of the business's receipt of the request.[23]

Record retention for compliance is set at 24 months (although retention of requests may by necessity be longer if an exemption is asserted, such as the retention of PI based

upon the length of an applicable statute of limitations or threat of litigation being brought against a business for non-compliance).

**D. Verification Alternatives for Properly identifying a Consumer**

Article 4 of the Draft Regulations create a sliding scale of consumer verification standards based upon the sensitivity of PI being requested. Factors include:

- The type, sensitivity, and value of the PI collected and maintained about the consumer (*i.e.*, sensitive or valuable PI requires more stringent verification processes),
- The risk of harm to the consumer posed by any unauthorized access or deletion,
- The likelihood that fraudulent or non-authorized individuals are seeking the PI,
- Whether the PI is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated,
- The manner in which the business interacts with the consumer, and
- The availability of technology for verification.

In the case of a customer that holds a password-protected account with a business, the business may require the customer to verify the customer's identity through the account. However, if a request is made, the business must also require that the customer reverify the customer's identification before disclosing or deleting PI.[24]

The Draft Regulations establish a sliding scale of verification steps depending upon whether a request is made for categories of PI or specific items of PI. In the case in which a consumer has a password-protected account with a business, the business may employ its existing verification procedures when responding to a consumer's request. In the case of a request to identify categories of PI when a consumer either does not have a password-protected account or no account with a business, the a business must identify a consumer with a "reasonable degree of certainty"—which is defined to mean matching a consumer with at least two data points of identification. In the case a consumer either does not have a password-protected account or no account with a business and specific items of PI are requested, the standard for verification is a "reasonably high degree of certainty"—which is defined to mean at least three pieces of PI provided by the consumer plus a verification signed by the consumer under penalty of perjury.[25]

Article 4 also identifies several steps that a business should undertake to verify a consumer's identity, based upon the factual matter whether the consumer has an account with the business. This combination of qualitative and quantitative factors may require individual attention to a consumer's request, and in any event may present challenges for developing automated response applications.[26]

In the case of a request to delete PI, the Draft Regulations would require that the standard and verification methodology would vary depending upon the sensitivity of the PI and the risk of harm to the consumer.

Finally, when a consumer employs an agent to make a request, the business may

require that the authorization be made in writing and that the consumer verify his/her identity directly with the business.

**E. Protection of Minors and Their PI**

Article 4 of the Draft Regulations is relatively straightforward in regard to a business obtaining the consent of a parent of a child for the child's PI below the age of 13, but requires that the parent (or guardian) adequately verify the status of the parent or guardian. Verification alternatives include:

- Providing a consent form to be signed by the parent or guardian under penalty of perjury and returned to the business by postal mail, facsimile, or electronic scan,
- Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder,
- Having a parent or guardian call a toll-free telephone number staffed by trained personnel,
- Having a parent or guardian connect to trained personnel via video-conference,
- Having a parent or guardian communicate in person with trained personnel, and
- Verifying a parent or guardian's identity by checking a form of government-issued identification against databases of such information.[27]

Unfortunately, Article 5 is silent in regard to any process by which a business might reasonably identify that a minor is communicating with the business. Whether the business can rely upon parental oversight of a minor's use of the internet is not addressed.[28]

**F. Complying with the anti-discrimination provisions of the CCPA**

Section 1798.125 of the CCPA prohibits a business from discriminating against a consumer because the consumer exercised a privacy right conferred by the CCPA, such as by opting-out from the sale of PI. However, a business may offer a price or service differential for not exercising CCPA rights if it is reasonably related to the value of the consumer's PI.

Article 6 of the Draft Regulations requires that, when setting a price differential, a business must use one of the following valuation methodologies:

- The marginal value to the business of the sale, collection, or deletion of a consumer's data or a typical consumer's data,
- The average value to the business of the sale, collection, or deletion of a consumer's data or a typical consumer's data,
- Revenue or profit generated by the business from separate tiers, categories, or classes of consumers or typical consumers whose data provides differing value,
- Revenue generated by the business from sale, collection, or retention of consumers' PI,
- Expenses related to the sale, collection, or retention of consumers' PI,
- Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference,

- Profit generated by the business from sale, collection, or retention of consumers' PI, or
- Any other practical and reliable method of calculation used in good-faith.[29]

The quantification and justification of a value may prove to be problematic to businesses when used to support differing pricing between consumers exercising or not exercising CCPA rights. For example, in the case of a business that employs voluminous data sets, revenue generated by individual consumers may be difficult to correlate a pricing differential that is more than nominal. Further, whether supportive economic evidence is necessary may present a cost factor that smaller businesses may find unrealistic.

**Providing Input During the Public Comment Period**

When issuing the Draft Regulations for public comment, the California AG announced that his office would be holding hearings December 2nd in Sacramento, December 3 in LA, December 4th in San Francisco and on December 5th in Fresno. Comments on the Draft Regulations can be provided at those hearings, via mail or via e-mail.

**Observations**

The Draft Regulations add new obligations and varying qualitative standards for compliance that may present practical compliance difficulties to covered businesses. Although the process and disclosure clarifications provide a clearer roadmap when preparing a project plan for compliance, efforts will have to be undertaken to ensure that a business's policies and procedures include the numerous compliance obligations set forth in the Draft Regulations analyzed herein.

While as noted above the Draft Regulations attempt to provide a compliance structure for CCPA notices and processing of requests from consumers, the primarily failure of the Draft Regulations is the failure to address reliable interpretations of unresolved issues set forth in the CCPA, such as the various exemptions contained in the CCPA. This may mean that businesses seeking to make use of exemptions or partial exemptions will be forced to submit focused interpretative requests to the California AG. (Whether the California AG will be responsive to requests for interpretations remains to be seen.)

The proposed inclusion of non-statutory response times and qualitative standards discussed herein are particularly problematic and could be the subject of a challenge by industry stakeholders that may determine that compliance with these additional requirements is unrealistic and beyond the delegated authority of the California AG. Additionally, industry stakeholders are likely to raise concerns about the proposed requirement that businesses treat user-enabled anti-tracking privacy controls as equivalent to a verifiable opt-out request.

Finally, as is frequently the case, completely new regulatory schemes that are initially finalized and issued are rarely modified until their effectiveness is evaluated—which in the case of the Draft Regulations may mean extended period of time. We strongly recommend that businesses consider submitting comment letters to the California AG—

either directly or through intermediaries. (Of course, attorneys at Dorsey are available to assist in this task.)

*  *  *

Please note that this Alert is an initial analysis of the issues and concerns raised by the Draft Regulations, but is not intended to constitute a comprehensive identification of concerns that businesses will face in their compliance efforts. It is likely that covered businesses will identify other significant compliance issues, and those concerns should be addressed wither through the comment or interpretative administrative processes.

We are available to discuss any questions or comments.

[1] Section 1798.100 *et seq.* of the California Civil Code.
[2] Section 1798.140(c) of the CCPA.
[3] Section 1798(o) of the CCPA.
[4] As stated in the Draft Regulations, a violation of the Draft Regulations will be deemed a violation of the statutory requirements of the CCPA. *See*, Section 999.300(b) of the Draft Regulations (*available at:* https://oag.ca.gov/privacy/ccpa).
[5] https://oag.ca.gov/privacy/ccpa.
[6] Section 1798.140(g) defines a "consumer" as a California resident. (Note, however, that AB 25, which was signed by the California Governor, for a 1-year period temporarily exempts most employee-related data from coverage under the CCPA.
[7] Section 1798.140(y) of the CCPA.
[8] Section 1798.185(a)(7) of the CCPA.
[9] Section 1798.120(c) of the CCPA.
[10] The Draft Regulations generally use the defined terms a "request to know" and a "request to delete" to mean a communication from a consumer relating to PI and the exercise of the consumer's privacy rights. *See*, Sections 999.301(n) and (o) of the Draft Regulations.
[11] Disclosures must be readily available with individuals with disabilities, which in the internet world has created significant litigation risk for non-compliance. *See*, Section 999.305(d) of the Draft Regulations.
[12] Section 999.305(b) of the Draft Regulations.
[13] Section 999.305(a)(4) of the Draft Regulations.
[14] Unfortunately, the Draft Regulations completely ignore how the exercise and disclosure of the various exceptions contain in the CCPA should be handled.
[15] Section 999.306(c) of the Draft Regulations.
[16] It should be noted that these categories contain numerous items of required disclosure; a business preparing its privacy policy should ensure that it has included all required items.
[17] A request to delete must entail a two-step process: first, a request to delete PI, and second, a separate confirmation that deletion of PI has been requested.
[18] Section 999.312(c) of the Draft Regulations.
[19] Section 999.312(f) of the Draft Regulations. (For large businesses, this latter requirement could present considerable training challenges.)

[20] Section 999.313(a) of the Draft Regulations. *Compare with*, Section 1798.130(a)(2) of the CCPA.

[21] This shortening of the response time may be particularly burdensome to large businesses that elect to centralize their CCPA responses.

[22] The Draft Regulations are notably silent when differentiating between internet websites and mobile applications; compliance with both alternative communication modes could present technology challenges to businesses if more than a link to a website is required in the case of a mobile application.

[23] Section 999.315(e) of the Draft Regulations. In a clear change from the statutory requirements of the CCPA, Section 999.315(h) indicates that a request to opt-out need not meet the standard of a verified consumer request, which may complicate compliance and training policies and procedures.

[24] Section 999.324(a) of the Draft Regulations.

[25] Sections 999.324 and 999.325 of the Draft Regulations.

[26] Sections 999.323, 999.324 and 999.325 of the Draft Regulations.

[27] "(b) When a business receives an affirmative authorization pursuant to subsection (a) of this section, the business shall inform the parent or guardian of the right to opt-out at a later date and of the process for doing so on behalf of their child pursuant to section 999.315." Section 999.330 of the Draft Regulations.

[28] Article V of the Draft Regulations. This likely means that the default language is that contained in the CCPA, which imposes special opt-in requirements for minors when a business has "actual knowledge that a consumer is less than 16 years of age."

[29] Section 999.337(b) of the Draft Regulations.