IPMPC
International Pharmaceutical &
Medical Device Privacy Consortium

December 6, 2019

Mr. Xavier Becerra
California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street, First Floor
Los Angeles, CA 90013

By Email to: PrivacyRegulations@doj.ca.gov

Re: CCPA Proposed Regulations

Dear Attorney General Becerra,

The International Pharmaceutical & Medical Device Privacy Consortium ("IPMPC") welcomes the opportunity to provide comments on the proposed regulations under the California Consumer Privacy Act (CCPA).

The IPMPC is comprised of chief privacy officers and other data privacy and security professionals from a number of research-based, global pharmaceutical companies and medical device manufacturers.[1] The IPMPC is the leading voice in the global pharmaceutical and medical device industries to advance innovative privacy solutions to protect patients, enhance healthcare, and support business enablement.[2]

The IPMPC is concerned that some of the requirements in the proposed regulations go beyond the requirements laid out in the statute and create burdensome obligations for businesses

[1] IPMPC members may also operate related businesses, including CLIA laboratories.

[2] More information about IPMPC is available at https://www.ipmpc.org/. This filing reflects the position of the IPMPC as an organization and should not be construed to reflect the positions of any individual member.

without creating proportional benefits for consumers. In particular, we are concerned with the following requirements related to the notice at collection of personal information:

- Section 999.305(b)(2) would require that the notice state the business or commercial purposes for which the information will be used "for each category of personal information." This requirement will lead to significant redundancy and unnecessary length of privacy notices. In many cases, all categories of information collected from a consumer are used for the same set of purposes. For example, a company providing voluntary patient support programs will require (at least) a patient's name, contact information, medical information, and health insurance information. Rather than permitting a company to say "We collect your name, contact information, medical information, and health insurance information to provide our voluntary patient support program," the regulations appear to require a company to provide the notice in this format:

  > We collect your name to provide our voluntary patient support program.
  > We collect your contact information to provide our voluntary patient support program.
  > We collect your medical information to provide our voluntary patient support program.
  > We collect your health insurance information to provide our voluntary patient support program.

  The amount of repetitive text required above would only increase once disclosures about sources of information and any information sharing are added.

  Businesses should be permitted to aggregate or group the categories of personal information when the information that must be disclosed is the same. Requiring differentiation by category of personal information will lead to long, repetitive notices that will be difficult for consumers to understand.

- 999.305(b)(4) requires that the notice include a link to the business's CCPA privacy policy or the web address of the policy. This paragraph should be amended to make clear that in the case of employees, this requirement can be satisfied by directing individuals to the relevant employee privacy policy, whether online (including on a company's internal extranet) or offline (e.g., in an employee manual).

In addition to the above concerns with the notice at collection of personal information, the IPMPC is also concerned with the requirement that "[i]f the business intends to use a consumer's personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose" (emphasis added). This requirement for explicit consent is unnecessary where the consumer's intentions are clear from his or her actions.

The IPMPC encourages the Department of Justice to publish samples of the various types of notices and responses to "requests to know" that would be required under the proposed regulations. This will aid businesses in their compliance efforts.

Finally, the IPMPC notes that there are various circumstances in which a business is not permitted to disclose specific pieces of information in response to a consumer's request to know. In particular, Section 999.313(c)(3) states that "[a] business shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks" (emphasis added). We suggest modifying the underlined text to read: "a substantial and articulable, or otherwise unreasonable, risk." Moreover, we encourage the Department to add "medical information" and other data elements the unauthorized disclosure of which could trigger a breach notification requirement under California law to the list of data elements in Section 999.313(c)(4) that do not require disclosure in response to a request to know specific pieces of information.

We thank you for the opportunity to provide these comments.

Sincerely,

Peter A. Blenkinsop
IPMPC Secretariat