Lowenstein Sandler

Privacy & Cybersecurity

January 11, 2021

As of January 1, the California Consumer Privacy Act Regulates De-identified Patient Information: Prompt Action Required

By Mary J. Hildebrand CIPP/US/E

What You Need To Know:

- **Beginning on January 1, 2021, any contract for the sale or license of de-identified patient information as defined by CCPA in which one of the parties resides in California or does business in the state must incorporate specific provisions, including a prohibition on re-identification.**
- **Businesses that sell or disclose de-identified patient information that is exempt from the CCPA must include certain notifications in their privacy policies.**
- **Policies, practices, and training programs must be revised to ensure compliance with the CCPA's regulation of de-identified patient information.**

Signed into law in September 2020, AB 713 aimed to clarify certain exemptions from the California Consumer Privacy Protection Act (CCPA) in order to ease compliance challenges encountered by companies in life sciences, biotech, health care, and related industries. However, in aligning the CCPA more closely with the Health Insurance Portability and Accountability Act, as amended by the HITECH Act (HIPAA); the Confidentiality of Medical Information Act (CIMA); the Federal Policy for the Protection of Human Subjects (Common Rule); and other laws relevant to human subject research, AB 713 also had another, rather unexpected effect: It imposed new obligations not only on CCPA-regulated businesses but on others engaged in the sale or license of de-identified patient information–even parties not otherwise subject to the CCPA.

As of January 1, 2021, **all** organizations, including life sciences companies, health-tech companies, data brokers, and others that use, process, or commercialize de-identified patient information as defined in AB 713, must comply with the CCPA's requirements concerning its disclosure, sale, license, and applicable privacy policies.

It is critical for any company that sells, purchases, or licenses such de-identified patient information, regardless of *any nexus to California,* to revisit and update its data diligence methodology and contracts to protect its rights and mitigate potential liability.

CCPA Exemption of De-identified Information

The CCPA's initial definition of "de-identified information" clashed with HIPAA's well-established protocols. Consequently, organizations that sought to use or disclose patient data de-identified under HIPAA standards assumed the risk that personal information regulated by the CCPA was still included.

AB 713 clarifies that de-identified patient information is exempt from the CCPA if such data is originally derived from consumers' protected health information collected by entities

regulated under HIPAA, CIMA, or the Common Rule, and is not subsequently re-identified or subjected to any re-identification attempts (De-identified Patient Data). Notwithstanding this broad exemption, AB 713 now extends CCPA regulatory authority to De-identified Patient Data.

CCPA Regulation of De-identified Patient Data

HIPAA stringently regulates the process of de-identifying patient data, but businesses that comply with HIPAA standards are not restricted in their use and disclosure of such information. By imposing new contractual and notice requirements on all entities that sell, license, or disclose De-identified Patient Data, the CCPA is moving into uncharted territory. Remarkably, these requirements apply not only to businesses regulated by the CCPA, but also to parties not otherwise subject to the CCPA.

The CCPA requires that any contract for the sale or license of De-identified Patient Data, where one of the parties is a person residing or doing business in California, shall prohibit the purchaser or licensee from:

1. Re-identifying, or attempting to re-identify, the natural person associated with the De-identified Patient Data
2. Further disclosing the De-identified Patient Data to any third party *unless* the third party is contractually bound by restrictions and conditions the same as or stricter than those of the seller or licensor of the De-Identified Patient Data

Under the CCPA, "re-identify" means the process of reversing de-identification techniques, including, but not limited to, the addition of specific pieces of information or data elements that can, individually or in combination, be used to uniquely identify an individual, or the usage of any statistical method, contrivance, computer software, or other means that have the effect of associating De-identified Patient Data with a specific identifiable individual. These contractual obligations are not limited to businesses regulated by the CCPA, and the re-identification processes described in AB 713 are common to many industries.

Additionally, businesses that sell or disclose De-identified Patient Data are required to disclose in their online privacy policies that the organization engages in such sale or disclosure, and specify whether the patient information was de-identified pursuant to the HIPAA safe harbor or expert determination methods.

What's Next?

AB 713 was enacted on an emergent basis to ensure that medical research was not adversely impacted by ambiguities in the original statute. As with many CCPA amendments, however, AB 713 has a broader reach. This amendment is not limited to businesses regulated by the CCPA but may apply to any organization engaged in the use, processing, or commercialization of De-identified Patient Data. The California Consumer Privacy Rights Act, passed in 4Q 2020, establishes a centralized agency with responsibility for enforcing the CCPA, so companies that use De-identified Patient Data must expect regulatory scrutiny and become prepared. To protect their rights and mitigate liability, any entities with potential exposure should immediately undertake a reevaluation of their data diligence processes and contract terms.

For more information on this latest development, contact **Mary J. Hildebrand**, Partner, Chair, and Founder of Lowenstein Sandler's Privacy & Cybersecurity group.

About Us
In today's digital world, where data has become a key asset for conducting business, companies continue to face greater privacy and cybersecurity challenges. At Lowenstein Sandler, our Privacy & Cybersecurity team helps clients navigate the rapidly evolving, increasingly complex privacy and security law landscape in the United States, the EU, and around the world. We deliver innovative privacy and security solutions that meet our clients' critical business needs including the commercialization of data assets in a legally compliant manner. Our targeted counsel is relevant to companies across diverse industry sectors, and public and private companies from start-ups to global enterprises.

Contact

Please contact the listed attorney for further information on the matters discussed herein.

MARY J. HILDEBRAND CIPP/US/E
Partner
Chair, Privacy & Cybersecurity
T: 973.597.6308
mhildebrand@lowenstein.com