Healthcare Organizations' Compliance With the CCPA

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2uiDLOS

The California Consumer Privacy Act (CCPA)[1] is the first piece of legislation in the US to emulate the EU General Data Protection Regulation (GDPR) and be enacted into law. The CCPA is a milestone in what is likely to become a new era of data privacy expectations and regulations in the United States. Momentum to increase private citizens' rights and control over their personal information is already building around the world and with it, enterprises face new burdens. Meeting the requirements of data protection laws in California along with Brazil, Europe, and other regions or countries requires an overhaul of information management practices across numerous functions and business units within impacted organizations.

For organizations in certain industries—specifically financial and healthcare—that are already governed by regulations touching on data privacy or providing for corrective actions (including legal recourse or monetary compensation) for consumers for specific types of data violations or breaches, compliance with these new laws may seem like standard process. But that is not necessarily the case. Focusing on the healthcare industry, organizations are aware of their obligations under the US Health Insurance Portability and Accountability Act (HIPAA)[2] for electronic protected health information (ePHI) and/or under privacy regulations in other jurisdictions such as Canada's Personal Information Protection and Electronic Documents Act or GDPR. Those organizations may view their current compliance efforts as a failsafe for CCPA; however, some of the new obligations under CCPA may require healthcare organizations—including those not based in the United States but serving California residents—to refresh certain policies and procedures.

The CCPA applies to organizations that do business in California and meet one or more of the following:

- Annual gross revenues exceeding US$25 million
- Buys, receives, sells or shares for commercial purposes the personal information of 50,000 or more California consumers, households or devices
- Derives 50 percent or more of its annual revenues from selling consumers' personal information

Louise Rains Gomez
Is a managing director in FTI Consulting's technology segment. Gomez brings more than 10 years of experience in litigation, e-discovery and information governance, with a focus on helping clients reduce costs and alleviate their broad data management challenges.

Thomas Hiney
Is a director in FTI Consulting's technology segment. He provides expertise in privacy program management and optimization, EU General Data Protection Regulation (GDPR) compliance, and US Health Insurance Portability and Accountability Act (HIPAA) risk and gap assessment.

It provides broad, strict protections for the personal data of California residents, including privacy rights centered around notice, access and consent.

Now that the law is in effect, healthcare organizations should be aware of and evaluate possible gaps between HIPAA compliance and the remainder of personal data not covered by HIPAA but in scope per definitions in the CCPA. This includes taking stock of the data footprint (i.e., the full breadth of consumer and sensitive information the organization manages and stores) as it relates to California residents and other notable considerations.

Certain Data Are Not Covered

Under the CCPA, covered[3] activities for entities and business associates collecting and using data include medical information governed by California's Confidentiality of Medical Information Act (part 2.6 [commencing with Section 56] of Division 1),[4] or protected health information (PHI) that is collected by a covered organization governed by the privacy, security and breach notification rules issued by HIPAA (Public Law 104-191)[5] and the US Health Information Technology for Economic and Clinical Health Act (HITECH) (Public Law 111-5).[6] This leaves some potential gaps of information, both medical and nonmedical, that may be subject to CCPA. Healthcare organizations should consider nonmedical information attached to a medical file, medical information used for marketing purposes, and/or medical information used for research and development purposes without explicit authorization/consent.

Risk in Aggregated Data Usage

The issue of de-identified and aggregated data that contain personally identifiable information (PII) further complicates what is and is not covered by the CCPA's HIPAA exceptions. This type of information—data that are aggregated into analytics systems to show high-level trends, business metrics or other non-personally identifiable insights—may be potentially identifiable as personal data. Many organizations currently and regularly use HIPAA-regulated information, such as payment and treatment information, for a variety of reasons. When those data are used for healthcare-related activities such as patient administration or fulfilling a medical claim, it is covered by the HIPAA exemption under the CCPA. But those data are also frequently used to inform other business needs through their aggregation in large-scale analytics and industry benchmarking systems.[7] While de-identified data are exempt from CCPA, ensuring that data are truly de-identified becomes an important process to undertake. This process includes implementing both technical safeguards and procedural safeguards to ensure that the data are specifically prohibited from being re-identified.

> "DIGITAL HEALTH ORGANIZATIONS…WILL NEED TO WORK WITH DATA PRIVACY EXPERTS TO IMPLEMENT TOOLS AND PROCESSES THAT WILL ALLOW THEM TO ENSURE THAT THEIR USE OF DE-IDENTIFIED DATA IS COMPLIANT."

De-identified data usage in healthcare creates some murky waters around privacy.[8] Personal data in aggregated analytics systems may be tied back to an individual, meaning data sets are not always fully anonymized as expected. This complicates how data governed by CCPA can be used in aggregated analytics systems—and how they can be accessed, reviewed or removed from those systems in response to a data subject request (DSR).[9] For example, if a data subject in California exercised his or her right to issue a DSR (e.g., to request access to his or her data or request for the data to be deleted), the organization is required under CCPA to fulfill the request. This includes locating and extracting that individual's personal data from aggregated data sets, which would be both a complicated effort and one that could potentially affect the integrity and accuracy of the analytics. Digital health organizations, and any others that rely heavily on de-identified data for business insights, will need to work with data privacy experts to implement tools and processes that will allow them to ensure that their use of de-identified data is compliant, and to have the ability to reverse engineer it as needed to fulfill DSRs.

Legal Risk

While HIPAA does not include a private right of action for citizens, many privacy regulations—including CCPA and GDPR—do. Individuals or classes may pursue legal recourse against healthcare organizations for violations involving data stolen or improperly accessed in unencrypted and unredacted form if the breached data are not subject to the caveats for exemption under HIPAA or other laws.

New Breach Notification Requirements

There are also some new considerations for healthcare organizations regarding notice of a data breach event. HIPAA requires governed entities to notify patients when their unsecured PHI is accessed or disclosed outside of any authorizations the patients may have signed. HIPAA includes several exceptions to this rule. The first applies to unintentional acquisition, access or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate if it was made in good faith and within the scope of authority. The second exception applies to the inadvertent disclosure of PHI by an authorized party to another authorized party or organized healthcare arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the privacy rule. The final exception applies in the event that a good-faith belief exists that the unauthorized person to whom the disclosure was made would not have been able to retain the information.

The issue becomes murkier if a breach falls within one of the previous exceptions, and the breached data are also under the jurisdiction of other privacy laws. Such an event may trigger additional notification requirements. The CCPA follows California's existing data breach notification laws[10] in which notification obligations are only triggered for breaches involving personal information. This is defined as a first name or initial and last name in conjunction with a social security number, driver's license number, California identification card number, account number or financial card number in combination with a password, medical information, health insurance information, or information collected through an automated license plate recognition system.

California Assembly Bill (AB)-1130, The Notification Bill, an amendment to CCPA, expands the definition of personal information by adding "other government-issued identification numbers" and "unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, or other unique physical representation or digital representation of biometric data."[11] Organizations must understand and be prepared to comply with these added obligations.

> "ANY BUSINESS UNITS OR EMPLOYEES WHO DEAL WITH PERSONAL INFORMATION NEED TO BE AWARE OF THE VARIANCES BETWEEN HIPAA AND CCPA."

Third-Party Notification

Previously under HIPAA, organizations were not required to alert customers to use of a third party as long as that party signs a business associate agreement (BAA). This changed with CCPA. Healthcare organizations will now need to notify customers and obtain informed consent to allow any third parties to access, receive, process, use or store personal data. Like the breach notification requirements, there may be some exceptions to this rule for information covered under other regulations.

Bridging the Gaps

There are a number of best practices organizations can implement to assess where their HIPAA practices fall short of enabling CCPA compliance. These include:

- **Training and education**—Any business units or employees who deal with personal information need to be aware of the variances between HIPAA and CCPA. Teams should be trained on CCPA and any additional measures needed to maintain compliance for data belonging to California residents.
- **Data mapping**—A clear map of where the organization stores personal data (across digital and hard copies), for how long, and how those data are used or shared with other parties should be prepared. It should include an extensive understanding of the regulatory risk exposure with respect to those data and how the compliance obligations impact products, services, business processes, internal systems, external third-party relationships, etc.
- **Refreshing privacy notices**—Legal counsel and privacy experts should be employed to develop compliant privacy notices that supplement existing HIPAA notices. These should include a description of consumer rights under the law, a comprehensive list of third parties to whom the business sells personal information and categories of third parties to whom the business discloses personal information for business purposes.
- **Managing data sales**—Clear and conspicuous consent requests should be provided and a "Do Not Sell My Personal Information" link should be included on the organization's website homepage. A process for handling do-not-sell requests should be implemented, and it should be easy for consumers to navigate. Vendor contracts should be reviewed to ensure that the sale/use of personal information is limited within the confines of the new CCPA nuances and that data rights requests implicating this information can be responded to and executed in a timely manner.

Operationalizing responses to DSRs—A toll-free telephone number and/or email address where individuals may submit data access requests and/or privacy complaints should be provided. Responding to these contacts can require substantial effort. A standardized workflow for fielding requests within the designated 45-day timeline should be developed. An outline for response should be prepared, including steps to authenticate the person(s) making the request and the process flow for handling access and deletion of data according to the request.

> "HEALTHCARE ORGANIZATIONS SUBJECT TO CCPA CANNOT RELY ON HIPAA AS A FAILSAFE FOR CCPA COMPLIANCE."

Conclusion

Healthcare organizations subject to CCPA cannot rely on HIPAA as a failsafe for CCPA compliance. These organizations must ensure that existing procedures are aligned with new requirements for data that are not covered and exempt by other regulations. Enterprises, led by legal and compliance teams, must be proactive and seek support from data privacy experts who can identify the gaps, advise on pitfalls and provide best practices. Investing in a strong data privacy posture now will better position organizations as new state, federal and international laws emerge.

Endnotes

1 State of California Department of Justice, California Consumer Privacy Act (CCPA), *https://oag.ca.gov/privacy/ccpa*
2 US Department of Health and Human Services, *Summary of the HIPAA Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html#targetText=The%20Privacy%20Rule%20protects%20all,health%20information%20(PHI).%22*
3 California Legislative Information, SB-1121 California Consumer Privacy Act of 2018, 24 September 2018, *https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121*

4 California Legislative Information, "Chapter 2. Disclosure of Medical Information by Providers," *https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=56.10.&lawCode=CIV*

5 US Department of Health and Human Services, HIPAA for Professionals, *https://www.hhs.gov/hipaa/for-professionals/index.html#targetText=To%20improve%20the%20efficiency%20and,unique%20health%20identifiers%2C%20and%20security*

6 US Department of Health and Human Services, "Public Law 111-5," 17 February 2009, *https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf*

7 Datavant, "The Fragmentation of Health Data," *https://datavant.com/2018/08/01/the-fragmentation-of-health-data/*

8 Drees, J.; "De-Identified Patient Data: Treasure Trove for Research or Privacy Nightmare?" Becker's Healthcare, 11 September 2019, *https://www.beckershospitalreview.com/ehrs/de-identified-patient-data-treasure-trove-for-research-or-privacy-nightmare.html*

9 Data Guidance and Future of Privacy Forum, "Comparing Privacy Laws: GDPR v. CCPA," *https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf*

10 California Legislative Information, "Health and Safety Code—Chapter 2. Health Facilities," *https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=HSC&sectionNum=1280.15*

11 California Legislative Information, AB-1130 Personal Information: Data Breaches, 14 October 2019, *https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1130*