Published on *The National Law Review* https://natlawreview.com

Healthcare Entities Must Still Comply with 2023 Privacy Laws

Article By:

John E. Wyand

Gicel Tomimbang

As we head into the fourth quarter, US businesses need to assess their progress in preparing for sweeping changes to the California Consumer Privacy Act ("CCPA") that become effective January 1, 2023, and with compliance with four new state consumer privacy laws (in Colorado, Connecticut, Utah and Virginia) that become effective throughout 2023 (collectively, "2023 Privacy Laws"). To help businesses prepare for the requirements of the 2023 Privacy Laws, Team SPB prepared guidance materials, including high level workstreams, covering the following topics: (1) Preparing for 2023 State Privacy Laws; (2) HR and B-to-B Data CCPA/CPRA Compliance Primer; (3) Lessons from the First CCPA Civil Penalty Case; and (4) Takeaways from the First Draft of Revised CCPA/CPRA Regulations.

The 2023 Privacy Laws have carve-outs directly applicable to businesses that must comply with the Health Insurance Portability and Accountability Act ("HIPAA") (i.e., covered entities and business associates). For instance, at a high level, as directly related to HIPAA:

- The CCPA, as amended by the California Privacy Rights Act ("CPRA"), exempts protected health information ("PHI") under HIPAA, as well as HIPAA covered entities to the extent they are maintaining patient information according to HIPAA requirements.

- The Virginia Consumer Data Protection Act ("VCDPA") does not apply to qualifying HIPAA covered entities and business associates, or to PHI, as the terms are defined under HIPAA. The VCDPA also exempts from its requirements healthcare data that has been de-identified according to HIPAA standards, information used for public health purposes authorized by HIPAA, or information originating from, and intermingled to be indistinguishable from PHI maintained by a covered entity or business associate. The exemptions under the Utah Consumer Privacy Act ("UCPA") and Connecticut's Privacy Law ("CTPA") largely track the VCDPA.

- The Colorado Privacy Act ("CPA") does not apply to information and documents created by a covered entity to comply with HIPAA. Note that this is broader than under the CCPA/CPRA and the VCDPA exemptions.

Nevertheless, businesses that must comply with HIPAA must still comply, to some extent, with the requirements of the 2023 Privacy Laws, particularly with regard to data that is not PHI. For example, the employee information maintained by covered entities for Human Resources purposes is not PHI. Likewise, certain health-related information collected from employees, such as information regarding maternity status for purposes of administering leave benefits or COVID-19 status for workplace safety, are also likely not PHI, and therefore, are outside the bounds of exemptions of the 2023 Privacy Laws for information maintained in accordance with HIPAA requirements. As a starting point, healthcare entities should do the following with regard to health-related information that is not PHI:

0. ***Know what health-related data you maintain.*** Start by performing an inventory of all health-related information your business maintains, and identify which information qualifies as PHI under HIPAA, and which do not. In general, the information that is PHI is exempted from the requirements of the 2023 Privacy Laws, but the non-PHI information is not.

- ***Provide a full privacy policy to data subjects that incorporates all the content requirements for privacy policies under the 2023 Privacy Laws.*** Healthcare entities must provide a pre-collection notice informing data subjects (e.g., consumers and employees) of the categories of personal information ("PI") to be collected and the purposes for collection. ***This is a separate notice from the HIPAA-required Notice of Privacy Practices ("NPP").*** The pre-collection notice must be easily understandable (i.e., written in plain language) and must inform data subjects of the statutorily enumerated categories of PI that are collected, including categories of sensitive PI (e.g., health-related information). In some instances, such as under the CCPA/CPRA, businesses must also disclose whether the categories of PI are sold or shared, the length of retention of the categories of PI and, if the business sells or shares PI, a link (or URL address) to the opt-out notice. If the business allows third parties to control the collection of PI (e.g., benefits providers), the notice shall also include the names of the third parties or information about their business practices. Note that, the CCPA/CPRA requirements for HR data, which are effective on January 1, 2023, requires the provision of a full privacy policy to HR data subjects (e.g., current and former employees, job applicants, contractors, etc.) that incorporates all the content requirements for privacy policies enumerated in the implementing regulations. This means that in addition to drafting and implementing a general privacy policy and NPP, covered entities must also prepare an HR privacy policy.

- ***Implement a mechanism through which data subjects may submit requests to exercise their rights under the 2023 Privacy Laws.*** Healthcare entities must develop and implement a mechanism for receiving privacy rights requests from individuals and HR data subjects, and a process for responding to the same. ***These mechanisms are in addition to the HIPAA requirements for receiving and responding to patient rights requests (e.g., right of access requests).*** This means that businesses must complete a data inventory of data across their systems, and identify outflows to vendors and others, so they can meaningfully respond to requests. Healthcare entities will likely want a different request flow, or even request process, to distinguish between traditional consumer requests, HR data subject requests, and HIPAA rights requests. Therefore, as to receiving privacy requests, healthcare entities must develop and implement at least three (3) workflows for receiving and responding to privacy requests: (1) a general consumer privacy rights requests flow; (2) an HR data subject privacy rights request flow; and (3) a HIPAA patient rights requests flow. Furthermore, privacy rights vary slightly between the 2023 Privacy Laws. For example, the

right to know what categories of PI were collected about an individual by a business in the twelve (12) months prior to the request date is only available to California residents. And so, healthcare entities, especially ones that must comply with the privacy requirements in multiple jurisdictions, will need to determine how they will approach honoring privacy rights requests across the different states.

Although healthcare entities benefit from carve-outs under the 2023 Privacy Laws for PHI, they still have obligations as to information that is not PHI. It will be interesting to see how healthcare entities will balance their HIPAA obligations the requirements of the 2023 Privacy Laws for information that is not PHI.

National Law Review, Volumess XII, Number 266