COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 32, Number 38. October 23, 2023
State Laws, FTC Rules Are Changing Privacy Compliance Landscape; Some AI Regs Are Here

By Jane Anderson

The health care privacy landscape is expanding rapidly beyond HIPAA, and compliance professionals should consider new state laws and enforcement actions as well as proposed regulations from the Federal Trade Commission (FTC), two attorneys said.

The definition of "health data" has grown to include data not covered by HIPAA, and state and federal policymakers are taking action to protect the privacy of that data, according to Alice Leiter and Brandon Reilly, attorneys with Manatt, Phelps & Phillips LLP.

"We've got this increasing movement from the HIPAA universe to the non-HIPAA universe," Leiter explained. Even artificial intelligence (AI) and machine learning (ML) are starting to be regulated.

Wearables, health equipment and health apps come to mind as having non-HIPAA-covered health data, but the scope of this data is much broader, Leiter and Reilly said at a webinar sponsored by the HCCA Sept. 28.[1] "Increasingly, almost any data point really could be considered health data, especially when it's combined with another data point," Leiter said. "An example of that would be geolocation data, which on its face might not seem like health data, but if the geolocation data is showing you visiting a health clinic, and particularly a specific kind of health clinic, such as a reproductive health clinic or a mental health or a substance abuse facility, you can see how quickly that enters the realm of consumer health data."

States on the Front Lines

Most privacy professionals are familiar with the California Consumer Privacy Act of 2018, but lawmakers in many states have focused on data privacy, Leiter said. A dozen states have passed laws that protect consumer data, which can include non-HIPAA-covered health information, she said. These include:

- Four states with laws in effect currently (California, Colorado, Connecticut and Virginia);
- Four states with laws that will take effect late this year or in the middle of next year (Utah, with an effective date of Dec. 31; and Oregon, Tennessee and Texas, with effective dates of July 1, 2024); and
- Four states with laws that will take effect in late 2024 or later (Montana, with an effective date of Oct. 1, 2024; Iowa and Delaware, with effective dates of Jan. 1, 2025; and Indiana, with an effective date of Jan. 1, 2026).

These laws apply to all industries. In addition, Connecticut, Nevada and Washington state have approved consumer privacy laws specific to health data, Reilly said, noting that the Connecticut law already has taken effect, while the Washington and Nevada laws will go live in spring 2024.

The laws vary in how they exempt HIPAA-related data and treat HIPAA-covered entities and business associates. "What also varies across these laws is whether, and to what extent, health and medical information might be

included in a definition of what's often called sensitive personal information or sensitive personal data," Reilly explained. "There are also special state requirements for the handling of PHI [protected health information] that's been de-identified under HIPAA."

Finally, many more states are considering legislation that would protect consumer data, including non-HIPAA-covered consumer health data, Leiter said.

Overall, the landscape is becoming very complicated, Reilly said. In the three states that have legislation specific to health data—Connecticut, Nevada and Washington—"the definitions of consumer health data across all of these laws are quite expansive ... in that they don't just pertain to what we traditionally would think about information about an individual's health condition or their heath treatment. They also pertain to information that reveals a health condition or diagnosis and information that can be used to identify or extrapolate a health condition or diagnosis."

Therefore, he said, "data is regulated even if it does not start as something that would be considered health data, but would allow you to make an inference about someone's health condition." For example, if web tracking technology shows that a person reads an ad or an article on diabetes treatment, then big data tools can infer the person has been diagnosed with diabetes, Reilly said. "The fact that the individual just browsed that advertisement or that article is itself potentially consumer health data."

The laws also require informed consent, Reilly said. "It has to be captured separately for different purposes." Finally, these three laws require separate and detailed privacy notices. "In Washington, in particular, they're very clear that you need a separate privacy notice that addresses specifically consumer health data," he said.

The dozen state laws that aren't health-care specific offer various exceptions for covered entities and business associates, Reilly said. In California, for example, HIPAA-covered entities are exempt from the law to the extent they handle PHI and if they handle non-PHI in the same manner as PHI, he said.