

Health Information Compliance Alert

See 2 Recent State Offerings That Go Beyond HIPAA

Tip: With breach reporting, timing is everything.

The onset and improvement of health IT over the past decade have made healthcare more efficient and enriched the coordination of care between providers. However, the digitalization of the industry has come at a cost for providers that impacts them both financially and professionally.

Practices must now vigilantly update their software and hardware, maintain stronger physical controls of their devices and offices, and be aware of and manage numerous regulations all while trying to ensure the care and privacy of their patients.

Through HIPAA, the HHS governs the privacy and security of patients' protected health information (PHI), but some states require even stricter protocols than the federal offerings.

Look at these two states that take HIPAA to the next level.

California: The California Consumer Privacy Protection Act (CCPA) is slated to become operational in January of 2020, but according to language in the Act, it won't necessarily impact covered entities (CEs), who are covered under other laws like HIPAA, the Gramm-Leach-Bliley Act, the Driver's Privacy Protection Act and the California Financial Information Privacy Act. However, CEs and their business associates (BAs) still might find themselves in hot water, depending on their data breach activity.

"This is an important carve-out for financial, insurance and healthcare industries that are already heavily regulated in their respective sectors," says attorney **Karina Puttieva** from national law firm **Nixon Peabody LLP** in their NP Privacy Partner blog. "But the carve-out comes with two caveats. First, the CCPA still applies if these entities engage in activity that falls outside their sectoral privacy regulation. And second, these entities are not exempt from the data breach class action provision of the CCPA."

Colorado: On Sept. 1, the state of Colorado upped its ante and implemented the harshest breach notification law in the nation. "The new law requires organizations to maintain a policy for disposing documents with consumer data and notify Colorado residents of any potential personal information exposure no later than 30 days after discovering a data breach," indicates attorney **Cynthia J. Larose** of **Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, PC** in online analysis of the law. "The 30-day notification window does not provide for any specific exemptions (such as HIPAA) and is the shortest of any U.S. state."