COSMOS
Navigate the Compliance Universe

Compliance Today - May 2023

Kara L. Hilburger (khilburger@octillolaw.com, linkedin.com/in/kara-hilburger-b2434240/) is Managing Director at Octillo, Buffalo, NY.

Alexis L. Rose is an Attorney.

Addressing the gap: Understanding the mismatched requirements between HIPAA and state privacy laws

by Kara L. Hilburger and Alexis L. Rose

The United States has long taken a sector-specific approach to data privacy, which differs from other regions, such as Canada and the European Union, which take a broader approach. In recent years, U.S. Congress struggled to arrive at a federal law that would apply data privacy principles and rights more generally.[1] Therefore, several states passed and implemented general data privacy laws in the absence of progress at the federal level. Specifically, the states of California, Colorado, Utah, Connecticut, and Virginia passed general data privacy laws. These state privacy laws create a complicated layer for organizations already complying with sector-specific privacy laws, including HIPAA. This article will discuss how these state laws interact with HIPAA, including HIPAA-related exceptions to the laws. In addition, it will provide an overview of some key differences between the various state privacy laws and HIPAA that may require organizations to reevaluate how they address their privacy obligations.

Overview of state laws and HIPAA interactions

HIPAA applies to collecting protected health information (PHI) by covered entities and business associates. Covered entities are health plans, healthcare clearinghouses, and healthcare providers that submit standard electronic transactions.[2] Business associates are organizations that maintain, collect, use, or disclose PHI on a covered entity's behalf.[3] Healthcare organizations that do not fit the definition of covered entity or business associate, and thus have not had to comply with HIPAA when handling medical information, will also have to consider the applicability of state privacy laws due to their much wider scope.

The state privacy laws apply generally to businesses (referred to as controllers under some laws) operating in the applicable states that either meet certain revenue thresholds or collect a certain amount of personal information.[4] For example, the California Consumer Protection Act (CCPA), recently amended by the California Privacy Rights Act, applies to for-profit organizations that either make $25 million in annual revenue, collect personal information from 100,000 or more residents of the state, or derive 50% of their revenue from sale or sharing of consumer personal information.[5] Some of the new state laws, such as in Virginia, Colorado, and Connecticut, apply to organizations that collect personal information about 100,000 or more residents of the state, [6] or derive revenue from the sale of personal information of 25,000 or more individuals, but do not maintain a general revenue-related threshold.[7]

Healthcare organizations should first determine if they meet the general revenue and/or data collection

thresholds to determine if a state privacy law applies to their organizations, including those defined as covered entities and business associates under HIPAA. Some organizations may not meet the threshold requirements because they are smaller and do not collect the necessary amount of personal information. Additionally, some healthcare organizations may be excluded from the applicable law because they operate as a nonprofit.[8]

Healthcare-related exceptions

Organizations that meet the thresholds under an applicable state law should next evaluate if a health information-related exception applies to the organization. Some of the state law exceptions that may apply to organizations in the healthcare space include research data governed under the Common Rule, substance use disorder information governed under 42 C.F.R. Part 2, or medical information governed by a state's medical confidentiality laws. However, this article focuses on the HIPAA exceptions in state privacy laws.

All five state privacy laws have exceptions related to HIPAA, but not all exceptions apply in the same way. For example, Utah, Connecticut, and Virginia laws all have HIPAA-related exceptions that apply to covered entities and business associates already complying with HIPAA.[9] However, the California and Colorado privacy laws contain HIPAA exceptions that are data-centered rather than organization-centered exceptions.[10] Stated differently, the exception applies to the type of data processed by the organization rather than the organization as a whole. The Colorado Privacy Act, for example, states that the law does not apply to PHI held by a covered entity or business associate, or other personal information the covered entity or business associate holds in compliance with HIPAA requirements.[11] The Colorado law also provides an exception for uses and disclosures of PHI that are done in compliance with the "[u]ses and disclosures for which an authorization or opportunity to agree or object is not required" section of the HIPAA Privacy Rule.[12] California's law also makes an exception for personal information held by covered entities and business associates that is maintained in compliance with HIPAA or California's Confidentiality of Medical Information Act, but this only applies to patient information, not all personal information.[13] Therefore, covered entities or business associates operating in California or Colorado will not be able to utilize the HIPAA-related exception in a blanket fashion and will have to identify their non-PHI personal information and apply the state privacy law requirements to that data unless another exception applies.