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

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

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.

Comparison of requirements under state laws and HIPAA

Although HIPAA and state privacy laws both seek to protect personal information, the approaches have similarities but also significant differences that must be accounted for in building a program to comply with these laws. The remainder of the article will go over the larger concepts that apply to both privacy frameworks but provide a breakdown of differences between HIPAA and state privacy laws.

Data in scope

HIPAA applies to PHI, which is individually identifiable health information created or received by a covered entity and "relates to an individual's past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual."[14] The state privacy laws apply to personal information (also referred to as personal data), which is broadly defined as "information that is linked or reasonably linkable to an identified individual or an identifiable individual."[15] California does list certain data points as personal information, but the list is not meant to be comprehensive.[16] It is also important to note that as of January 1, 2023, the CCPA also applies to personal information collected from employees of businesses that must comply with the law.[17]

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

With the much broader application of state privacy laws, it will be vital for organizations—including covered entities and business associates, particularly in California and Colorado—to account for the non-PHI personal information they hold. Some examples of this may include personal information collected from nonpatients, such as a patient's family members or friends; information collected from patients that is not related to their diagnosis, treatment, or care, such as for fundraising purposes; or personal information held by business associates that work across multiple industries and the personal information was not provided by a covered entity.

Additionally, there will be plenty of organizations that operate in the healthcare space but do not fall into the narrow definition of a covered entity or business associate. Some healthcare providers do not submit standard electronic transactions because they either only receive payment directly from the patient or their services are not covered by insurance (e.g., concierges, doctors, cosmetic surgeons, and therapists). These healthcare providers still collect large amounts of medical information that does not constitute as PHI but would constitute as personal information under state privacy laws.

Therefore, it will be necessary for covered entities, business associates, and other organizations that work in the healthcare space or collect medical information to identify through data mapping the personal information they collect and whether HIPAA or a state privacy law may apply to the data. Data mapping will also be essential for understanding an organization's different categories of data, even beyond the designation of personal information or PHI.

Different categories of data

Covered entities and business associates accustomed to complying with HIPAA are aware that all PHI is treated the same, except for psychotherapy notes.[18] However, state privacy laws do not follow this same model and some personal information is treated as sensitive personal information. The state privacy laws define sensitive personal information or sensitive data slightly differently; however, most sensitive data definitions include personal information "revealing an individual's race, ethnic origin, religious beliefs, sexual orientation, citizenship or immigration status, medical information or information deriving from medical information, specific geolocation, and genetic information."[19] It will be crucial for healthcare organizations that collect this sensitive data to be aware of such collection because it comes with additional legal obligations related to consent, risk, and the data subject's rights.[20]

Organizations should again leverage data mapping to identify these special categories of information. When state laws are applicable, organizations must review the consents they present to patients or consumers and likely update them to address the collection of sensitive personal information. Organizations should also consider the collection of sensitive personal information in their risk management programs.

Notices of collection of data

HIPAA and state privacy laws have similar but very distinct obligations related to notifying data subjects of the collection and use of their data. Under the HIPAA Privacy Rule, covered entities must provide individuals with a Notice of Privacy Practices.[21] A HIPAA Notice of Privacy Practices notifies the individual of all the ways a covered entity may use and disclose their PHI, their rights with regard to that PHI, the covered entity's obligations to comply with the notice and HIPAA's Privacy Rule, and that the individual can lodge a complaint if they believe the covered entity has violated the notice or HIPAA.[22] To the extent the covered entity maintains a website, they are required to post their Notice of Privacy Practices there as well.[23]

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

State privacy laws also require that data controllers provide individuals with a notice regarding using and collecting their personal information. The state privacy laws largely require the notice to contain the categories of personal information processed, the purpose of processing the personal information, how consumers can exercise their data subject rights, the categories of personal information the controller shares with third parties, and a description of the types of third parties the controller shares the personal information with.[24]

In addition to the differences in content, the audiences of these notices may be quite different. Covered entities provide HIPAA Notice of Privacy Practices to patients of a healthcare provider or a plan holder of a health plan. However, the notices required under state privacy laws will likely reach a much larger audience. For example, a covered entity that may also be a controller under a state privacy law because it processes personal information of nonpatients will also have to provide a notice to those nonpatient individuals from which it collects personal information. This may include individuals who visit the covered entity's website just to receive additional information about their services or health plans they offer, or personal information of donors or other business partners, or in the case of California, employees. Additionally, business associates that previously did not have to provide a Notice of Privacy Practices because it is the obligation of a covered entity may now have to provide a privacy notice under state law requirements, as they may also operate as a controller.

For organizations that need to provide a privacy notice under state privacy laws, it will be helpful to include language in that notice that alerts the reader that it does not apply to PHI and that their rights as related to PHI will be found in a separate HIPAA Notice of Privacy Practices.

Data subject rights

HIPAA has established data subject rights, including the right to access, amend, or receive an accounting of an individual's PHI.[25] HIPAA also permits individuals to restrict the disclosure of their PHI in certain circumstances.[26] Many of the state laws permit similar rights regarding personal information, but also include additional data subject rights such as right to deletion and right to opt out of the sale or sharing of their personal information.[27] It can be complicated from a data mapping and categorization standpoint to comply with all the necessary data subject rights without being too expansive. For organizations that hold both personal information and PHI, that organization would have to identify whether the information in question is personal information or PHI and where the data subject is located. If an organization only applies data subject rights from state laws to personal information from those states, and rights from HIPAA to PHI, it could cause a lot of administrative work. For instance, the timeline for responding to a request for access to PHI under HIPAA is 30 calendar days;[28] however, the same timeline for a consumer request to access their information under the CCPA is 45 calendar days, with an additional requirement that the organization acknowledges receipt of the request within 10 business days.[29] Thus, it may be helpful to expand the data subject rights to all personal information, including PHI. Organizations will still have to conduct a case-by-case review of each request, but it can reduce the administrative burden of trying to identify only the applicable data. This approach also reduces regulatory risk because failure to properly respond to data subject rights will open any organization to scrutiny from enforcement agencies such as state attorney generals and the U.S. Department of Health & Human Services Office for Civil Rights (OCR). In particular, patient access to PHI has taken on greater scrutiny from OCR in the last few years, as such patient rights have been the main focus of a number of recent OCR enforcement actions.[30]

However, even if organizations take a broader approach to data subject rights, detailed policies and procedures should still be in place for responding to data subject requests. These procedures should outline the differences in response times, required content of responses, permitted fees, exemptions to a data subject request, and scope of data subject rights.

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

Use and disclosure of the applicable data

Another area where the two privacy schemes diverge is in permitted uses and disclosures of the information collected. State privacy laws are largely concerned with data subjects' rights, not how that information is used or disclosed. Although there are some limitations on the use and disclosure of personal information when the data subject has opted out of the sale or sharing of their personal information under some the state privacy laws, including CCPA and the Colorado Privacy law. Conversely, covered entities and business associates can only use and disclose PHI for specific reasons permitted under the HIPAA Privacy Rule.[31]

This leads to two important considerations for organizations that must comply with both HIPAA and state privacy laws. First, if an organization avails themselves of the exceptions related to holding personal information or patient information in the same manner as PHI under HIPAA, this will significantly limit how non-PHI personal information can be used or disclosed. This will be especially true for business associates subject to business associate agreements that may limit their use of the data even more. Second, when an organization has two different standards for use and disclosure of different types of information, the organization will have to provide adequate training to its personnel. It will be essential that personnel understands that even if personal information can be used or disclosed for certain purposes, those purposes may not be permitted when using or disclosing PHI. This distinction should also be detailed in an organization's policies and procedures.

Conclusion

Although the overall principles of HIPAA and these state privacy laws are very similar and some of the requirements align, compliance with both standards will require a close analysis of a healthcare organization's privacy program. These two privacy schemes also have substantial differences, which complicate the application of their principles and requirements. Therefore, organizations required to comply with both schemes should take steps to have an in-depth understanding of the personal information and PHI the organization holds. Privacy officers should work across departments and have buy-in from leadership to get a true sense of the data the organization maintains that may be subject to state privacy laws. Organizations should also conduct a detailed review of their privacy policies and procedures, as they must update them or create new policies and procedures to account for the state privacy law requirements. This will likely include updates to public-facing documents, such as an organization's privacy policy. Organizations should also provide effective training around expanding data privacy rights and protections to information collected by organizations other than PHI. Organizations required to comply with both schemes should take time to understand when each law will apply, what data they hold, and where the implementation of the legal requirements will require changes in the organization's policies, procedures, and practices.

Tips

- An organization's leadership and management should determine—at the start of updating its privacy program—what approach it wants to take. Does it want to run parallel privacy programs or treat all personal information as PHI?
- Organizations should work with legal counsel to assess which state privacy laws, if any, will apply to their organization. Organizations should document this assessment.
- Organizations should involve stakeholders from across the organization to fully understand the scope of personal information the organization collects.
- Business associates that determine they are subject to a state privacy law should decide whether they are a

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

business/controller or service provider/processor, as business associates may be subject to many more obligations under the state privacy laws than they were under HIPAA.

Takeaways

- Organizations will have to make an informed decision on how to structure their privacy programs when subject to both HIPAA and state privacy laws.
- Data mapping will be a critical exercise to determine what personal information a healthcare organization collects that is distinct from protected health information (PHI).
- There are many similar requirements between HIPAA and state privacy laws that have subtle yet vital differences.
- Training of personnel handling personal information that previously did not handle PHI will be critical.
- Organizations should review their privacy notices, policies, and procedures to update and implement them appropriately if subject to a state privacy law.

1 American Data Privacy and Protection Act, H.R. 8152, 117th Congress, introduced June 21, 1022, https://www.congress.gov/bill/117th-congress/house-bill/8152.
245 C.F.R. §160.103.
345 C.F.R. §160.103.
4 California Consumer Privacy Act of 2018, Civ Code Title 1.18.5, §1798.140(d) (2018).
5 California Consumer Privacy Act of 2018, Civ Code Title 1.18.5, §1798.140(d) (2018).
6 Colorado Privacy Act, § 6-1-1304; Connecticut Act Concerning Personal Data Privacy and Online Monitoring §2; and Virginia Consumer Data Protection Act §59.1-572(B).
7 Colorado Privacy Act, § 6-1-1304; Connecticut Act Concerning Personal Data Privacy, § 2, Virginia Consumer Data Protection Act, §59.1-572(B).
8 California Consumer Privacy Act of 2018, Civ Code Title 1.18.5, §1798.140(n) (2018).
9 Virginia Consumer Data Protection Act §59.1-572(B); Connecticut Act Concerning Personal Data Privacy and Online Monitoring Sec. 3; Utah Consumer Privacy Act 13-61-201(2)(e)-(f).
10 California Consumer Privacy Act of 2018, Civ Code Title 1.18.5, §1798.145(c)(1)-(2) (2018); Colorado Privacy Act, 6-1-1304(2)(a).
11 Colorado Privacy Act, 6-1-1304(2)(h).
1245 C.F.R. 164.512.
13 California Consumer Privacy Act of 2018, Civ Code Title 1.18.5, §1798.145(c)(1)(B).
1445 C.F.R. 160.103.
15 Colorado Privacy Act, 6-1-1303(17).
16 California Consumer Privacy Act of 2018, Civ Code Title 1.18.5, §1798.140(v)(1).
17 California Privacy Rights Act of 2020, Sec. 3(A)(8) (ver. 3).
1845 C.F.R. §164.509(a)(2).
19 Colorado Privacy Act, 6-1-1303(24).
20 Colorado Privacy Act, 6-1-1308(7).
2145 C.F.R. §164.520(a).
2245 C.F.R. §164.520(b).
2345 C.F.R. §164.520(c)(3)(i).
24 Virginia Consumer Data Protection Act §59.1-574(C).
2545 C.F.R. §164.524-8.

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

2645 C.F.R. §164.522.
27 Connecticut Act Concerning Personal Data Privacy and Online Monitoring Sec. 3.
2845 CFR § 164.524(b)(2).
29 California Consumer Privacy Act of 2018, Civ Code Title 1.18.5, §1798.130(a)(2).
30 U.S. Department of Health & Human Services, Office for Civil Rights, "Eleven Enforcement Actions Uphold Patients' Rights Under HIPAA, news release, July 15, 2022, https://www.hhs.gov/about/news/2022/07/15/eleven-enforcement-actions-uphold-patients-rights-under-hipaa.html.
3145 C.F.R. §164.502-514.

This publication is only available to members. To view all documents, please log in or become a member.

Become a Member Login

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.