COSMOS
Navigate the Compliance Universe

Compliance Today - June 2022
When healthcare and consumer data rules collide: Compliance with the latest generation of data privacy laws

By Alex Dworkowitz, Brandon Reilly, and Randi Seigel

Alex Dworkowitz (adworkowitz@manatt.com) and **Randi Seigel** (rseigel@manatt.com) are both Partners in the New York City office, and **Brandon Reilly** (breilly@manatt.com) is a Partner in the Costa Mesa, California, office of Manatt, Phelps & Phillips LLP.

- linkedin.com/in/alex-dworkowitz-2872155/
- linkedin.com/in/brandonpreilly/
- linkedin.com/in/randi-seigel-b1676a5/

Alex Dworkowitz

Brandon Reilly

Randi Seigel

We live in a digital world that has continued to grow during the COVID-19 pandemic, when individuals were forced online to work, socialize, and receive healthcare and wellness services. Individuals generate tremendous amounts of personal health data as they share their information through, among other channels, browsing health-related websites, using proprietary applications (apps) and portals, and sharing on social media platforms. Many individuals appreciate the ease of sharing data, accessing the information, and receiving treatment and health-related services in the comfort of their home; it is, thus, no surprise that this has driven healthcare providers and plans to increasingly advance their digital footprint.

In the past few years, health providers and plans have been partnering with telemonitoring providers and traditionally consumer-facing digital health apps to create richer data sets from which to mine data to improve their offerings and patient or member experience, turning many consumer-facing apps into business associates. As a result, consumer or personal information (PI) data, which historically was subject to limited regulation, now may also become subject to the Health Insurance Portability and Accountability Act of 1996, as amended, and its implementing regulations (collectively referred to as HIPAA). In some cases, PI data also may be subject to the emerging generation of consumer privacy and protection laws, such as the currently in-effect California Consumer Privacy Act (CCPA) or similar laws coming in 2023 such as the Virginia Consumer Data Protection Act; Colorado Privacy Act; and the CCPA's successor, the California Privacy Rights Act. Importantly, these laws are likely to be further modified through amendments and forthcoming regulations, and other states are expected to pass similar laws, including potentially in New York, Washington, and Massachusetts.

Similarly, healthcare providers and health plans that have comfortably used, shared, and safeguarded protected health information (PHI) data under HIPAA now have to evaluate whether they are also subject to the CCPA and other state laws, given that the organizations collect PI through a multitude of methods, including their website and social media platforms or other operations like brick-and-mortar pharmacies that provide consumer products in addition to dispensing prescriptions.

It's complicated: A case study

Figuring out what laws and regulations apply to what data is complicated. Take for instance the following arrangement: A health plan makes a consumer-facing app available to its members as a value-added benefit and pays for the app subscription for its members. If the member chooses to take advantage of this benefit, the member must download the app and enter their information. The app, using the information the member shares, then confirms with the plan via limited identifiers, sometimes even using a deidentified token, that this person is indeed a member; the app may or may not share information regarding the members' use of the app with the health plan. Is the app really a business associate of the health plan in this instance? If so, is all the app's data regarding this member now considered PHI subject to HIPAA? What if the member unenrolls from the plan but wants to continue to use and pay for the app? Can the app make the previously entered information available to the former member without the member providing consent to the health plan? And is the former member's PI now subject to, for instance, the CCPA?

When does HIPAA apply to healthcare data?

HIPAA regulates PHI and defines PHI as "individually identifiable health information" transmitted or maintained in any form or medium, excluding limited classes of information, such as information held "in education records covered by the Family Educational Rights and Privacy Act" and "employment records held by a covered entity in its role as employer."[1] "Individually identifiable health information," in turn, is health information that:

> 1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
> 2. Relates to the 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; and
>   i. That identifies the individual; or
>   ii. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

In general, most healthcare data held by covered entities—healthcare providers, health plans, and healthcare clearinghouses—is PHI. Some healthcare data may be excluded from the PHI definition if properly deidentified, while other data may fall within one of the limited exceptions to PHI.

Thus, covered entities are very comfortable with the framework where nearly all healthcare data they hold is subject to HIPAA's privacy and breach reporting requirements, and, if the data is in electronic form, it is subject to HIPAA's security requirements as well. Most covered entities view any healthcare data through this lens and are hesitant to categorize any healthcare data as non-PHI (also referred to in this article as PI).