wiley

NEWSLETTER

All Data Is Not HIPAA Data – Healthcare Covered Entities Should Pay Close Attention to State Privacy Laws Regulating the Health IoT Ecosystem

July 2021

Privacy In Focus®

From fitness bands and mobile applications (apps) to Bluetooth-enabled heart rate monitors and glucose pumps, Internet of Things (IoT) healthcare technologies have firmly cemented their place in the daily lives of Americans. Due in part to the COVID-19 pandemic, Americans have widely and rapidly embraced consumer-directed healthcare apps and devices to monitor their wellness – either in lieu of or in conjunction with professional medical interactions. Market analysts report a precipitous rise in the popularity of connected health and wellness devices from just one year earlier, with a reported $6.7 billion invested in the first quarter of 2021, up from $3.1 billion invested in the first quarter of 2020.

With increased IoT growth on the horizon, it is crucial that healthcare actors understand their privacy obligations with respect to data collected from consumer-directed healthcare apps and devices. While seemingly straightforward, this task is complicated by the disconnect between personal information protected under the Health Insurance Portability and Accountability Act (HIPAA) and personal information protected under state privacy laws.

HIPAA Applicability and Protections

The HIPAA Privacy Rule serves as a federal baseline for privacy protections that must be afforded to certain categories of healthcare data, known as Protected Health Information (PHI). PHI refers to

Authors

Antonio J. Reynolds
Partner
202.719.4603
areynolds@wiley.law

Tawanna D. Lee
Consulting Counsel
202.719.4574
tdlee@wiley.law

Practice Areas

FTC Regulation
Health Care
Privacy, Cyber & Data Governance
State Attorneys General

individually identifiable health information that is transmitted by or maintained in electronic media or any other form or medium. PHI receives HIPAA Privacy Rule protections (including prohibitions and limitations on data disclosure) only if it is created, used, or maintained by a Covered Entity (CE), which includes health plans, healthcare clearinghouses, and healthcare providers who transmit health information in electronic form in connection with a covered transaction. Importantly, the HIPAA Privacy Rule *does not* apply in the following circumstances: (1) the health data at issue does not constitute PHI; and (2) the PHI is collected, used, or maintained by a non-Covered Entity (except for a Business Associate, as that term is defined in 45 C.F.R. § 160.103).

With the increased use of consumer-directed healthcare apps and devices, providers and patients often assume that all collected healthcare data is safeguarded by the HIPAA Privacy Rule. This is not the case. As an *actor*-centered rule, the HIPAA Privacy Rule does not afford protection to all healthcare data regardless of its source and use. Rather, only PHI collected, used, or maintained by Covered Entities is subject to the HIPAA Privacy Rule's requirements. Presently, most wearable devices, healthcare applications, and health IoT devices do not involve receipt, review, collection, or maintenance of health data by a Covered Entity. Instead, these consumer-driven products involve collection and storage of consumer-inputted data by device manufacturers and developers, who are not themselves Covered Entities. Without the Covered Entity nexus, this data remains unprotected. This is true regardless of the fact that this same data would be protected if provided to a Covered Entity. Thus, it is important to remember that the HIPAA Privacy Rule's protections only apply to *certain types* of healthcare data possessed by *certain actors*. When healthcare data is not within the possession of a Covered Entity (or a Covered Entity possesses non-PHI data), the data falls through the cracks of federal privacy regulation.

Healthcare Adjacent Data and State Law Privacy Protections

Healthcare data that does not constitute PHI or is not used by Covered Entities for clinical care is sometimes referred to as healthcare adjacent data. This is data that falls outside the bounds of HIPAA. Data collected by wearables, health IoT devices, and healthcare applications often fall within this category.

Healthcare adjacent data can create significant confusion among providers and consumers. Providers and consumers may erroneously believe that the HIPAA Privacy Rule's protections apply to this data. This creates a false sense of security for consumers because they believe their data is subject to stringent privacy regulations that, in fact, are not applicable. Instead of federal privacy protections, consumers are left at the mercy of the device's or app's privacy policy, which can change over time and may allow downstream disclosure and use of sensitive health data.

Further, by assuming the HIPAA Privacy Rule applies to all healthcare data, providers may inadvertently neglect to comply with (i) state law requirements that govern healthcare adjacent data, and (ii) more stringent state law requirements that preempt the HIPAA Privacy Rule. State privacy laws are currently the main source of regulation for healthcare adjacent data, and apply much more broadly than HIPAA (e.g., most state privacy laws are not limited to Covered Entities). A provider's assumption that HIPAA applies to all data (including

non-PHI data) collected from a wearable or healthcare device may result in liability under state law for failure to comply with more stringent (or different) standards.

This is particularly true where a healthcare wearable or app comingles PHI and non-PHI data before transmission to a Covered Entity. In that scenario, only the PHI data would be protected by HIPAA and the non-PHI data would be subject to state law regulation only. These different regulatory structures based on the type of data and the type of actor can make it difficult to identify the regulatory schemes applicable to each piece of data.

Moreover, providers must also be aware that the HIPAA Privacy Rule can be preempted by more stringent state laws. As noted previously, the HIPAA regulations serve as a floor for privacy protections. If a state imposes heightened privacy standards, the minimum HIPAA Privacy Rule requirements no longer apply. This means that providers must closely analyze state law regulations to determine whether state law standards preempt baseline HIPAA requirements for any subset of PHI. For example, the California Consumer Privacy Act (CCPA) excludes from its scope PHI collected for treatment, payment, or healthcare operations. Accordingly, PHI that is collected, maintained, or used by Covered Entities for treatment, payment, or healthcare operations is subject to the HIPAA Privacy Rule and not the heightened CCPA requirements. Providers, however, must then identify PHI that is not used for treatment, payment, or healthcare operations and recognize that this subset of data is subject to more stringent CCPA requirements.

Filling the Gap – Federal and State Enforcement Actions

Federal and state regulations are not the only safeguards applicable to consumer health data. Enforcement agencies such as the Federal Trade Commission (FTC) and state Attorneys General (AGs) have undertaken active monitoring and oversight efforts to ensure healthcare adjacent data is still protected, despite slipping through federal regulatory frameworks.

The FTC's primary enforcement authority stems from Section 5 of the FTC Act, which allows the FTC to initiate an enforcement action for unfair or deceptive acts or practices in or affecting commerce. Recent FTC actions have emphasized that symmetry must exist between a healthcare application's privacy policies and its actual use of consumer health data. In January 2021, for example, Flo, Health Inc. settled allegations by the FTC that it impermissibly shared users' sensitive health data with third-party analytics and marketing services in contravention of its published privacy practices. In the settlement, the FTC imposed on Flo, among other remedies, a unique notice requirement by mandating that Flo notify affected users about the disclosure of their personal information. In addition, two FTC commissioners wrote a partial concurrence and partial dissent in which they advocated use of the Health Breach Notification Rule. This rule, which has not been used by the FTC to date, requires vendors of unsecured health information to notify users and the FTC if there has been an unauthorized disclosure. The Flo case highlights the FTC's commitment to proper data usage and the potential for new and emerging remedies as these cases continue to evolve. As providers navigate the murky waters of healthcare data privacy and security, it is crucial that they comply with FTC and other federal guidance to avoid enforcement actions.

Similarly, state AGs are holding healthcare companies accountable for their data privacy practices. In September 2020, for instance, the California Attorney General's Office reached a settlement with Glow, an ovulation and period-tracking app. The AG accused Glow of failing to protect users' sensitive data by (1) including a partner connect feature that automatically granted requests between partners to link their data without authorization from the user whose data was about to be shared; and (2) allowing users to change account passwords without confirming the old password. These practices contravened Glow's privacy policies and violated numerous California laws, including California's unfair competition law and California's Confidentiality of Medical Information Act. Glow's failure to protect healthcare data resulted in a $250,000 civil penalty, along with other remedies.

Thus, identifying the proper privacy frameworks for healthcare data is essential to ensure compliance with state and federal privacy laws and, correspondingly, avoid civil enforcement actions by state and federal agencies.

Conclusion

At any point in time, providers may be operating under one or multiple privacy frameworks due to the interplay between federal and state privacy laws. It is crucial that providers identify which framework(s) the data falls within and the applicable requirements with respect to the healthcare data under each privacy structure. Assuming that HIPAA provides a one-size-fits-all privacy landscape for PHI and healthcare adjacent data is a mistake that can expose companies to enforcement actions, liability, and significant fines – particularly in light of the flurry of enforcement activity from federal, state AG, and other agencies.

© 2021 Wiley Rein LLP