DLA PIPER

ACCELERATE

Key points about data privacy rules and healthcare information

We live in an age of innovations in healthcare IT, greater consumer interest in wearables, and evolving use and sharing of electronic medical records. All these factors mean that scrutiny of the collection and use of health information is on the rise. Companies whose business involves the use, collection or processing of health information should be aware of developments in regulations related to the protection of that information.

What type of health information is protected?

There is no single law that governs personal information in the US. One effect of this is that there is no single definition or description of what type of health information is protected. For example, the primary federal law, the Health Insurance Portability and Accountability Act (HIPAA), applies to individually identifiable health information that has been created by or on behalf of healthcare providers or health insurance plans in the provision of, or payment for, healthcare products and services. While other federal and state laws apply similar but distinct definitions of the health information subject to their rules, the HIPAA definition of "PHI" or "protected health information" is the most common but by no means the only one.

What rules apply?

Any health information that identifies a person's past, present, or future health care or payment for that care is subject to HIPAA. HIPAA overrides state rules that are not more protective, and represents the baseline level of compliance. In those situations where HIPAA may not apply, courts have increasingly leveraged the HIPAA regulations (discussed below) to establish the applicable standard of care.

Although HIPAA is the most important rule concerning health information in the US, the FTC has jurisdiction over consumer-generated health information, such as via fitness trackers and personal health record providers. Although the FDA has been largely silent on the protections applicable to health data within medical devices, there is increasing coordination between the FDA and other parts of the Health and Human Services agency responsible for PHI.

Finally, state laws such as the Texas Medical Privacy Act and the California Confidentiality of Medical Information Act continue to apply, notwithstanding the preemptive nature of HIPAA.

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) regulates the privacy, security and breach notice obligations concerning PHI collected by "covered entities" and their "business associates." A covered entity is typically a healthcare provider or a health insurer, including employers that have self-funded employee health benefit plans. A business associate (BA) is most often a service provider that supports the covered entity's health-related functions. These activities by a BA can be more obvious (such as medical transcription or billing services) or less so (remote maintenance/support to a software application processing patient data or simply providing a cloud hosting solution for the covered entity to use). While a covered entity is subject to all of HIPAA requirements, business associates must conform to a subset of those requirements.

As mentioned above, HIPAA sets a federal minimum level of protection for patient data in most healthcare settings. The HIPAA statute has spawned several other regulations, the most common of which are referred to as the Privacy Rule, the Security Rule and the Breach Notification Rule. The Privacy Rule centers on the ways in which organizations subject to HIPAA may use and disclose PHI, as well as the rights of patients. The Security Rule sets a security framework equally applicable to any sized organization subject to HIPAA. The Security Rule outlines required and addressable safeguards that fall into administrative, technical and physical categories; the Rule does permit an organization to implement these safeguards in a manner proportionate to its size, resources and so forth. Finally, the Breach Notification Rule establishes self-reporting obligations in the event that a security incident has resulted in the compromise of the confidentiality or security of patient data.

What is a business associate agreement?

An additional aspect of the HIPAA Privacy Rule is that it outlines most of the content that must be within a business associate agreement (BAA). A BAA is a set of legal terms that can be an addendum to an existing agreement or a stand-alone document applicable to a series of underlying agreements. These are most commonly between a covered entity and a BA (as a supplement to the main services agreement), but can also exist when one BA has engaged another BA as a subcontractor to the first. The essence of the legally required provisions is that they the use and disclosure of PHI to certain narrow parameters. The parties are free, however, to add their own terms in areas such as risk allocation, which is why most BAAs from covered entities include uncapped indemnification provisions, while the BA seeks to apply a cap on liability generally.

What sort of enforcement exists?

Until about 2012, there was very little enforcement. However, the arrival of the Breach Notification Rule, which obligates organizations to self-report data breaches, changed things. Between 2015 and 2016 alone, HHS enforcement climbed over 200 percent; average fines/settlements amounted to US$2 million in 2016. Most enforcement is by HHS, but state attorneys general have concurrent authority to enforce with respect to the residents of their jurisdiction.
