WARD AND SMITH, P.A.
ATTORNEYS AT LAW

Impact of Cloud-Based Software Service Providers on HIPAA Covered Entities and Business Associates

Written By **Angela P. Doughty, CIPP/US** (apd@wardandsmith.com)
October 31, 2016

The message from patients to healthcare providers is clear: increase the quality of health services while decreasing cost. The message from the federal government to healthcare providers and their business associates is even clearer pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"): protect patient data or face serious financial penalties.

In response to these pressures, healthcare providers and their business associates are increasingly relying on cloud-based software service providers ("CSPs") as a way to manage, store, access, and transmit enormous quantities of health information while cutting costs and enhancing coordination and communication among providers to improve patient care.

Until recently, in the absence of clear guidance from the Department of Health and Human Services ("HHS"), most healthcare providers (and CSPs themselves) relied upon the "conduit exception" to conclude that CSPs were not business associates under HIPAA. This exception exempts service providers of HIPAA covered entities (and their business associates utilizing these services) from the business associate standard if the service provider merely acts as a "conduit" for protected health information ("PHI"). Examples of such PHI conduits are the US Postal Service, certain private couriers, and their electronic equivalents providing transmission-only services.

HHS's New Guidance on CSPs

HHS Guidance published this month now makes it clear that CSPs offering a variety of services, from basic online data storage to entire electronic medical record systems and computing infrastructures, fall outside of HIPAA's “conduit exception.”

Accordingly, **CSPs that qualify as HIPAA business associates must now comply with HIPAA and its regulations, including without limitation the Privacy Rule, the Security Rule, and the Breach Notification Rule ("HIPAA Rules")**. Additionally, HIPAA covered entities that utilize CSPs must now consider the CSPs to be their business associates and must enter Business Associate Agreements with them. Failure to comply with HIPAA Rules can result in considerable penalties.

HHS's rejection of the conduit exception for CSPs is broad and includes CSPs that lack an encryption key for encrypted electronic PHI ("ePHI") they store and maintain. That is, even if a CSP cannot actually access or view the ePHI it stores (so-called "no-view services"), the CSP still qualifies as a business associate and must

comply with the HIPAA Rules.

To maintain flexibility in these relationships, the HHS Guidance notes that where CSPs are providing no-view services, the requirements under the HIPAA Rules can be satisfied by the combined actions of both the HIPAA covered entity and the CSP. For example, a CSP offering no-view services can be responsible for encryption access, and the covered entity using the CSP's services can be separately responsible for user authentication, and both of these actions combined may satisfy the requirements under the HIPAA Rules.

Nevertheless, regardless of the way the responsibilities are delegated or divided, a Business Associate Agreement is required to ensure that the CSP does not impermissibly use or disclose ePHI. Depending on the nature and complexity of the relationships, covered entities and business associates may also want a Service Level Agreement with the CSP to further detail each party's responsibilities. Service Level Agreements can address a number of issues, such as system availability and reliability, backup procedures for data recovery, delegation of security responsibilities, data retention, and termination of the relationship. The Service Level Agreement terms must remain consistent with the parties' Business Associate Agreement and the HIPAA Rules.

HHS does allow for one small exception to the general rule that CSPs are HIPAA business associates: a CSP that only receives and maintains ePHI that has been "de-identified" in compliance with the HIPAA Rules does not qualify as a business associate; and, as such, a Business Associate Agreement is not required. Under HIPAA, information is de-identified if it does not identify any individual and the covered entity has no reasonable basis to believe it can be used to identify an individual.

Implications for Healthcare Providers, Business Associates, and CSPs

HHS's Guidance on CSPs means that if a healthcare provider or other HIPAA covered entity or a business associate of a HIPAA covered entity uses a CSP to maintain, process, store, or transmit ePHI that has not been de-identified, the CSP must be treated as a business associate and the covered entity must require a HIPAA compliant Business Associate Agreement with the CSP before utilizing the CSP's services. Covered entities may also want to explore Service Level Agreements to further clarify the parties' financial and legal responsibilities for the ePHI.

HHS’s Guidance also means that every CSP must analyze the services it provides to HIPAA covered entities (and business associates thereof) and determine whether it will now be considered a business associate under HIPAA; and, if so, implement HIPAA policies and procedures to comply with the HIPAA Rules.

Conclusion

Failure on the part of a covered entity, business associate, or CSP to comply with applicable HIPAA obligations could result in significant penalties. To illustrate such risk, the HHS Guidance cites a case that settled in July, 2016, where it was discovered that, in addition to other potential violations, ePHI was being stored on the Oregon Health & Science University's cloud-based server without a Business Associate Agreement in place with the CSP. Following HHS's investigation, the University agreed to pay $2.7 million in fines to HHS to resolve the matter.

Despite the risks, the HHS Guidance does have a silver lining. It confirms that healthcare providers can utilize cloud computing, which may mean improvements in efficiency, decreases in cost, and ultimately, advancements in patient care. All of these positive results will depend upon covered entities and CSPs working collaboratively to ensure that proper privacy and security measures are in place.

--