HHS Issues HIPAA Guidance Related to Cloud Services

By: David Saunders and Heidi Wachs

The Department of Health and Human Services (HHS) has published formal guidance that makes clear that most Cloud Servicer Providers (CSPs) that create, receive, maintain or transmit electronic Protected Health Information (ePHI) are Business Associates and thus governed by HIPAA. While the overall conclusion, that CSPs that handle ePHI are Business Associates, is not particularly revolutionary, HHS's formal guidance provided details as to HHS' evaluation of CSPs, which those who work with CSPs and handle ePHI should take note of.

The full text of HHS's CSP guidance can be accessed here.

CSPs are HIPAA Business Associates

HHS has concluded that most CSPs that create, receive, maintain or transmit electronic Protected Health Information (ePHI) are Business Associates. This is true even where a CSP only receives encrypted ePHI and lacks the encryption key for the data (what HHS refers to as "no-view CSPs"). HHS also clarified that a CSP that stores ePHI for any purpose other than for temporary storage incident to a data transfer does not fall within the "conduit" safe harbor of HIPAA. However, where a CSP only receives de-identified data, the CSP will not be considered a HIPAA Business Associate by HHS.

As Business Associates under HIPAA, CSPs are required to comply with HIPAA, including but not limited to the establishment and maintenance of physical, administrative and electronic safeguards for ePHI. CSPs are also subject to HIPAA's Breach Notification Rules. However, a "CSP is not responsible for the compliance failures that are attributable solely to the actions or inactions of the customer." This fact is important because HHS allows CSPs and their customers to allocate HIPAA compliance obligations with respect to certain HIPAA Security Rule requirements.

The example given by HHS regarding the division of compliance obligations is where the customer implements its own authentication controls for access to ePHI and the CSP only provides no-view services. Under these circumstances, according to HHS, the CSP would not also have to adopt its own authentication procedures. A word of caution a CSP customers however, "where the contractual agreements between a CSP and customer provide that the customer will control and implement certain security features of the cloud service consistent with the Security Rule, and the customer fails to do so, OCR will consider this factor relevant during any investigation into compliance of either the customer or the CSP." CSP customers should therefore be mindful of taking on HIPAA obligations associated with cloud services.

Business Associate Agreements And Other Safeguards

Because HHS has concluded that most CSPs that handle ePHI are Business Associates, HHS is requiring Covered Entities and Business Associates that share ePHI with CSPs to have HIPAA-compliant Business Associate Agreements (BAA) with the CSPs.

In addition to having a BAA with CSPs, HHS has charged Covered Entities and Business Associates with conducting their own risk analysis and developing appropriate risk management policies around the use of a CSP and its services. Specifically, in its new guidance, HHS requires that Covered Entities and Business Associates "conduct risk analyses to identify and assess potential threats and vulnerabilities" related to services obtained through a CSP. HHS has identified service level agreements with CSPs as one potential area of focus. HHS has instructed Covered Entities and Business Associates to ensure that the service level agreements are "consistent with the BAA and the HIPAA Rules." However, HHS' guidance also states that "[t]he HIPAA Rules do not expressly require that a CSP provide documentation of its security practices or otherwise allow a customer to audit its security practices." It would thus seem that audit rights, which are frequently part of service level agreements, may not be necessary to comply with the HHS" mandated risk assessment.

HHS' guidance also expressly permits the access of ePHI from mobile devices and the storage of ePHI on servers outside of the United States, provided that the CSP is complying with HIPAA.

Contact Us

David P. Saunders, Partner

Phone: 312 923-8388 Email: dsaunders@jenner.com Download V-Card

Heidi L. Wachs, Special Counsel

Phone: 202 639-6081 Email: hwachs@jenner.com Download V-Card