# OCR addresses business associate concerns for cloud services

Rick L. Hindmand | Friday, October 7, 2016

Today, the Department of Health and Human Services Office for Civil Rights (OCR) issued HIPAA guidance on cloud computing.

This guidance confirms that a cloud services provider (CSP) that creates, receives, maintains or transmits electronic protected health information (ePHI) on behalf of a covered entity is a HIPAA business associate even if all ePHI is encrypted and the CSP does not have the encryption key. A CSP that subcontracts to perform similar functions on behalf of the business associate involving ePHI is also a business associate. In those situations, business associate agreements are required between the CSP and the covered entity or upstream business associate, and the CSP is required to comply with the business associate agreements as well as the HIPAA Privacy, Security and Breach Notification Rules.

OCR specifically reminds covered entities and business associates that using a CSP to maintain ePHI without entering into a business associate agreement violates the HIPAA rules. This follows a string of recent HIPAA resolution agreements for failure to enter into business associate agreements, including a settlement involving storage on a cloud-based server.

OCR recognizes that in some cases a CSP may not know that a covered entity or business associate is using the cloud service in connection with ePHI, and therefore may not be in a position to satisfy its obligations under the HIPAA rules. The guidance clarifies that upon becoming aware that it is maintaining ePHI, a CSP must comply with the HIPAA rules or securely return the ePHI to the customer (or destroy it, if agreed). OCR notes that the 30 day period to correct noncompliance (in order to qualify for an affirmative defense under the HIPAA rules) begins when the CSP knows or should have known that a covered entity or business associate is maintaining ePHI in its cloud. OCR recommends that CSPs document their compliance, or their return or destruction of ePHI.

With respect to ePHI stored or processed overseas, the guidance warns that risks and vulnerabilities can vary greatly and need to be accounted for in risk analysis and risk management as required under the HIPAA security rule.

This guidance provides important reminders for CSPs as well as for covered entities and business associates that utilize the cloud. To learn more about HIPAA compliance and how to keep your business and patient information protected, contact the attorney listed below.

---

**Rick L. Hindmand**