OCR releases HIPAA guidance on cloud computing services

October 20, 2016

Recently, the U.S. Department of Health and Human Services Office for Civil Rights (OCR) published guidance regarding Health Insurance Portability and Accountability Act (HIPAA) issues related to cloud computing and the use of cloud service providers (CSPs).

The Guidance notes that cloud computing may take many forms but that CSPs "generally offer online access to shared computing resources with varying levels of functionality depending on the users' requirements, ranging from mere data storage to complete software solutions (e.g., an electronic medical record system), platforms to simplify the ability of application developers to create new products, and entire computing infrastructure for software programmers to deploy and test programs."

The Guidance confirms that, as expected, a CSP is a Business Associate under HIPAA when engaged by a Covered Entity or Business Associate to create, receive, maintain or transmit electronic protected health information (ePHI) on its behalf. Previously, there had been some question in the industry regarding whether that would be the case if the CSP only had access to encrypted ePHI and did not possess the encryption key (referred to as "no-view" CSP services). The Guidance answers this question, stating: "Lacking an encryption key does not exempt a CSP from business associate status and obligations under the HIPAA Rules." Thus, a CSP is considered a Business Associate even if it possesses ePHI in a no-view services arrangement. The Guidance further states: "… a CSP providing no-view services is not exempt from any otherwise applicable requirements of the HIPAA Rules. However, the requirements of the Rules are flexible and scalable to take into account the no-view nature of the services provided by the CSP."

Eleven Frequently Asked Questions are included in the guidance to provide additional detail regarding HIPAA issues related to cloud computing. Noteworthy highlights of these FAQs include:

- The Guidance cautions that Covered Entities and Business Associates using a CSP "should understand the cloud computing environment or solution offered by a particular CSP so that [it] … can appropriately conduct its own risk analysis and establish risk management policies" related to the CSP. The Guidance refers Covered Entities and Business Associates to the cloud computing guidance from the National Institute of Standards and Technology (NIST) at SP 800-144 and SP 800-145.
- As a Business Associate, a CSP must comply with the applicable HIPAA security, privacy and breach regulations. However, the Guidance notes that when a CSP is providing only "no view" services, certain Security Rule requirements that apply to the ePHI maintained by the CSP may be satisfied for both parties through the actions of one of the parties. In particular, where only the customer controls who is able to view the ePHI maintained by the CSP, certain access controls, such as authentication or unique user identification, may be the responsibility of the customer, while others, such as encryption, may be the responsibility of the CSP.
- The Guidance notes that Service Level Agreements (SLAs) are commonly entered into with CSPs as a contract governing the arrangement. OCR warns that SLAs must be consistent with the terms of the Business Associate Agreement (BAA) between the parties and the applicable HIPAA rules.
- A CSP will generally not be considered a "mere conduit" to qualify for the conduit exception under the HIPAA rules. The conduit exception applies where the only services provided are for transmission of ePHI; where a CSP provides transmission services, in addition to maintaining ePHI for purposes of processing and/or storing the information, the CSP is still a Business Associate with respect to such transmission of ePHI.
- Health care providers may use mobile devices to access ePHI in a cloud as long as appropriate physical, administrative and technical safeguards are in place to protect the confidentiality, integrity and availability of the ePHI on the mobile device and in the cloud, and appropriate BAAs are in place with any third party service providers for the device and/or the cloud that will have access to the ePHI.
- The HIPAA rules do not prevent using a CSP that stores ePHI on services outside the U.S. However, OCR notes that the risks to such ePHI may vary greatly depending on its geographic location and, "[i]n particular, outsourcing storage or other services for ePHI overseas may increase the risks and vulnerabilities to the information or present special considerations with respect to enforceability of privacy and security protections over the data." Those risks should be taken into account when conducting the risk analysis and risk management required by the Security Rule.
- Clarification that a CSP is not a Business Associate if it receives and maintains only information de-identified through a process meeting the requirements of the Privacy Rule.

Authors