Publications

Health Care Alert: OCR Releases Guidance on HIPAA Compliance and Cloud Computing

Related Services

Data Strategy, Privacy and Security

Related Industries

Health Care

CLIENT ALERT | 12.14.2016

In October, the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) released new guidance for covered entities and business associates that utilize cloud computing for data storage, software, or online access to shared resources and contract with cloud service providers (CSPs) for the service. The guidance provides information about best practices to achieve compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as well as highlights some HIPAA compliance risks associated with the use of cloud computing services.

Significantly, OCR stated that CSPs that process or store electronic protected health information (ePHI) on behalf of a covered entity are receiving, maintaining, or transmitting ePHI as it is defined by HIPAA and are considered business associates under HIPAA regardless of whether the CSP processes or stores encrypted or unencrypted ePHI. A CSP does not qualify for the mere conduit exception under HIPAA even if the ePHI is encrypted, the CSP does not have the encryption key, and the ePHI is processed on a "no-view" basis. The mere conduit exception applies only to those entities such as the U.S. Postal Service which have transient access to PHI. To perform all of its functions, a CSP has persistent access to ePHI even if the CSP does not actually view the information.

Because the CSP, or any entity that the CSP might subcontract with to provide cloud services, would be considered a business associate it is essential that any covered entity that uses cloud computing to store ePHI enter into an appropriate business associate agreement (BAA) with its CSP. Furthermore, the covered entity and the CSP must each understand its privacy and security obligations under HIPAA. While some HIPAA Security and Privacy Rule requirements will likely be satisfied by the covered entity's actions by, for example, providing only encrypted ePHI to the CSP, the CSP will still need to separately comply with other responsibilities such as data availability, physical security, or risk analysis and risk management. A CSP will also be responsible for complying with any breach notification requirements that may arise in the event of a breach of unsecured ePHI.

OCR suggests that covered entities and CSPs consider entering into a service level agreement (SLA) that defines exactly which party will be accountable for which elements of compliance with the HIPAA Privacy and Security rules. The SLA may address provisions such as data retention, system availability, back-up and data recovery, use and disclosure limitations, and security responsibilities. Regardless of whether the individual compliance responsibilities of the covered entity and the CSP are outlined in a SLA, the underlying service agreement, or in the BAA, OCR notes that a written designation of how compliance activities have been delineated between the two will be "important and relevant" in the event of a compliance investigation.