5 things to know about HIPAA and cloud computing

OCT 14, 2016

Troy Parks
News Writer

Protecting patients’ health information is critical to the future of data collection that informs population health. But how can physicians make sure they are in compliance with Health Insurance Portability and Accountability Act (HIPAA) regulations when using cloud computing?

The Department of Health and Human Services Office of Civil Rights (OCR) recently issued guidance on HIPAA and cloud computing that confirms cloud services providers (CSP) are business associates under HIPAA.

If you are currently using a CSP or are planning to soon, the guidance offers detailed direction on the nature of cloud computing, business associate agreements (BAA) and how it all relates to HIPAA, including:

- **Physicians and health care professionals can use mobile devices to access ePHI in a cloud.** Accessing information in a cloud is appropriate as long as physical, administrative and technical safeguards are in place to protect the confidentiality, integrity and availability of the ePHI on the device and the cloud. Read the OCR and Office of the National Coordinator for Health IT guidance on the use of mobile devices and tips for securing ePHI on those devices.

- **A HIPAA-covered entity or business associate can use a cloud service to store or process ePHI.** The covered entity or business associate must first enter into a HIPAA-compliant BAA with the CSP that will be creating, receiving, maintaining or transmitting ePHI on its behalf. The BAA establishes how ePHI can be disclosed and used. OCR offers guidance on the elements of BAAs. To address more specific business expectations with your CSP, you can enter into a Service Level Agreement (SLA). SLAs can include provisions that address HIPAA concerns such as system availability and reliability, back-up and data recovery, how data will be returned to the customer after service use termination, security responsibility and use, retention and disclosure limitations. The AMA offers a sample BAA for your reference.
Using a CSP to maintain ePHI without a BAA is a violation of HIPAA rules. Entering into a BAA with your CSP is the key first step. However, if a CSP meets the definition of a business associate—in other words, the CSP creates, receives, maintains or transmits ePHI on behalf of a covered entity or another business associate—remember that it is a business associate and must comply with all applicable HIPAA rules, regardless of whether it has executed a BAA. The key takeaway is that if you use or are thinking of using a CSP to create, receive, maintain or transmit ePHI on your behalf, you must have a BAA with the CSP or both you and the CSP will be in violation of HIPAA.

A CSP that stores encrypted ePHI and does not have a decryption key is still considered a HIPAA business associate. Because the CSP receives and maintains ePHI for a covered entity or other business associate, lacking an decryption key for the data does not exempt a CSP from business associate status.

If a CSP experiences a security incident it must report the incident to the covered entity or business associate. HIPAA requires business associates to identify and respond to suspected or known security incidents, mitigate harmful effects that are known and document security incidents and their outcomes.

The Breach Notification Rule specifies the content, timing and other requirements to report for incidents that rise to the level of a breach of unsecured patient information. For more on security incidents, see the FAQ about reporting security incidents.

For more on cloud use and health IT:

- Why medicine needs a cloud
- Finding tech passion in an unlikely place
- Patient-first technology: Improving care for the chronically ill
- 4 ways HHS hopes to simplify and support patient care
- 3 barriers keeping data from improving health outcomes