Health Information Compliance Alert

Enforcement News: Share Data But Be Wise to the Possibility of A Breach, OCR Says

A recent survey about cloud computing and data sharing reveals risks.

Cloud technology removes the necessity for clunky in-house hardware and puts the onus on your vendor to store and compute your practice data. But a new report from the HHS-OCR maintains that file-sharing collaboration has its drawbacks.

Last October, the HHS-OCR offered provider guidance, focusing on the privacy and security concerns that arise when ePHI is shared through the cloud. In spite of the advice, which spoke to both the HIPAA Privacy and Security Rules pertaining to disclosures, Business Associate Agreements (BAAs), Service Level Agreements (SLAs), encryption and system requirements, a recent survey of a myriad of organizations across business spectrums suggested that many had already experienced breaches due to issues with the cloud computing technologies, suggested the latest edition of the HHS-OCR Cybersecurity Newsletter.

The June issue showed that the biggest problems arose from temporary staff, "contractors, or third parties accessing data they should not see; employees accidentally exposing data; and broken security management processes." Interestingly, "only 28 percent of respondents listed external hackers as one of their top three concerns," the survey indicated.

Poorly configured file-sharing systems "as well as cloudcomputing services, are common issues that can result in the disclosure of sensitive data, including ePHI," the Cybersecurity Newsletter noted. "Too often, access, authentication, encryption, and other security controls are either disabled or left with default settings, which can lead to unauthorized access to or disclosure of that data."

Resource: To read the June 2017 HHS-OCR Cybersecurity Newsletter, visit https://www.hhs.gov/sites/default/files/june-2017-ocr-cyber-newsletter.pdf.