NOW + NEXT

HEALTH CARE ALERT | NIXON PEABODY LLP

OCTOBER 12, 2016

OCR issues new guidance on HIPAA and cloud computing

By Laurie T. Cohen

The Office for Civil Rights (OCR) continues to issue guidance to covered entities and business associates on discrete arrangements that implicate the HIPAA Privacy and Security Rules (HIPAA Rules). Most recently, OCR released guidance on "HIPAA and Cloud Computing" accompanied by a series of frequently asked questions (FAQs).

The guidance affirms that a covered entity (or business associate) may engage a cloud service provider (CSP) to store electronic protected health information (ePHI) or to create, receive or transmit ePHI on the covered entity's (or business associate's) behalf provided that the parties enter into a HIPAA-compliant business associate agreement. OCR cautions, however, that "a covered entity (or business associate) that engages a CSP should understand the cloud computing environment or solution offered by a particular CSP so that the covered entity (or business associate) can appropriately conduct its own risk analysis and establish risk management policies . . .."

OCR also clarifies that a CSP storing or maintaining encrypted ePHI on behalf of a covered entity or on behalf of a business associate is itself a business associate. This is the case, even when the CSP does not have access to the decryption key and cannot actually view the ePHI. OCR asserts that, although encryption may protect ePHI from being viewed in an unauthorized manner, such protections do not adequately safeguard the integrity and availability of ePHI as required by the Security Rule. Most notably, encryption does not ensure that the information cannot be corrupted by malware, nor does it ensure that the ePHI remains available to authorized persons.

Also of note, OCR recognizes that "a CSP may not have actual or constructive knowledge that a covered entity or another business associate is using its services to create, receive, maintain[] or transmit ePHI." OCR explains that "if a CSP becomes aware that it is maintaining ePHI, it must come into compliance with the HIPAA Rules, or securely return the ePHI to the customer or, if agreed to by the customer, securely destroy the ePHI." A CSP is at risk of violating the HIPAA Rules if it fails to take steps to become compliant once it learns that its service is being used to create, receive, maintain or transmit ePHI. Although the HIPAA Rules provide an affirmative defense in cases where a CSP is unaware that a covered entity or business associate customer is

maintaining ePHI in its cloud, such defense is not available if the CSP's lack of awareness is the result of its own willful neglect.

The guidance and the full text of the FAQs can be found here.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

— Laurie T. Cohen at **lauriecohen@nixonpeabody.com** or 518-427-2708

— Valerie Breslin Montague at **vbmontague@nixonpeabody.com** or 312-977-4485

— Jill H. Gordon at **jgordon@nixonpeabody.com** or 213-629-6175

— Carolyn Jacoby Gabbay at **cgabbay@nixonpeabody.com** or 617-345-6112

— Lindsay R. Maleson at **lmaleson@nixonpeabody.com** or 516-832-7627