Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Highlights Of HHS Privacy Guidance For Cloud Providers

Law360, New York (October 17, 2016, 12:29 PM EDT) --


Jodi Daniel

The U.S. Department of Health and Human Services' Office for Civil Rights recently released its long-awaited "Guidance on HIPAA & Cloud Computing." Using 11 questions and comprehensive responses, the guidance details the OCR's position on the obligations of covered entities and business associates who use cloud services providers (CSPs) to manage their electronic protected health information (ePHI). There are three important takeaways from the guidance: (1) CSPs are presumably business associates with very limited exceptions even if they only handle encrypted data, (2) the OCR continues to emphasize the importance of tailored security risk assessments in its enforcement efforts, and (3) the OCR is increasing its scrutiny of contractual agreements involving ePHI in its enforcement efforts.

The Guidance Confirms the General Presumption That CSPs Are Business Associates


Elliot Golding

Unsurprisingly, the guidance confirms that the OCR views the obligations of CSPs who create, receive, maintain or transmit ePHI very broadly. There is no doubt that CSPs who engage in such activities for covered entities or business associates are themselves business associates under the Health Insurance Portability and Accountability Act. Even where a CSP receives or maintains only encrypted ePHI and does not have the decryption key to view the information, the OCR asserts that the CSP is a business associate, albeit one that is providing "no-view services." Furthermore, the OCR asserts that CSPs that create receive, maintain or transmit ePHI are business associates when they are a subcontractor to a business associate.


Stephanie Willis

Conversely, the guidance also describes two narrow circumstances under which CSPs are not business associates: (1) where they serve only as conduits to covered entities or business associates, or (2) where they only receive and maintain information that has been de-identified in accordance with the HIPAA Privacy Rule. The OCR further clarified that CSPs that provide "no view services" cannot rely on the conduit exception unless they only provide ePHI transmission services to a covered entity or business associate and there is only incidental and temporary, not persistent, storage of any ePHI during transmission. If the CSP's access to a covered entity's or business associate's ePHI is more than incident to the transmission of such ePHI, then the CSP is required to enter into a business associate agreement (BAA) with the covered entity or business associate. In addition, the guidance confirms that a CSP cannot assert that it is not a business associate when it is performing transmission-related services for a covered entity or business associate if the CSP also provides storage or other services for that same customer.

The guidance implicitly acknowledges that many CSPs may currently have arrangements with covered entities and business associates without a BAA in place. The OCR reminds readers of its July 2016 resolution agreement and corrective action planimposed on a covered entity that impermissibly used a CSP to store over 3,000 individuals' ePHI without entering into a BAA. Where a CSP lacks a BAA with a covered entity or business associate, and is not aware that it is maintaining ePHI, the guidance advises the CSP to take action to correct any noncompliance within 30 days of when it knew or should have known of the noncompliance. The OCR notes that a CSP that discovers a customer's use of the CSP's resources to create, receive, maintain, or transmit ePHI without a BAA may have an affirmative defense against a HIPAA violation if: (1) the CSP takes quick action to get in compliance with HIPAA, or (2) the CSP returns the ePHI to the customer within 30 days (or destroys the ePHI with the customer's consent). The defense, however, does not protect CSPs who willfully neglect their obligations under HIPAA. Thus, other than where the defense would apply, the guidance reinforces the CSP's obligation to proactively evaluate whether ePHI is being stored or maintained in its cloud programs and platforms.

The Guidance Reiterates OCR's Emphasis on Comprehensive Security Risk Assessments and Risk Mitigation

Based on the above, the OCR would deem most CSPs to be business associates that must have BAAs with a covered entity or a business associate customer for which the CSP creates, receives maintains, or transmits ePHI. Furthermore, the BAA, and any contracts such as service-level agreements (SLA), must be tailored to address the security risks unique to the relationship between the customer and the CSP. This security risk analysis must "identify and assess potential threats and vulnerabilities to the confidentiality, integrity, and availability of all ePHI they create, receive maintain or transmit." Thus, for example, if a CSP stores a covered entity's ePHI on servers outside of the United States, the CSP and the covered entity customer may need to take any increased risks associated with that remote storage into account in their respective security risk analyses. The guidance also briefly addresses the administrative, physical and technical safeguards that parties using mobile devices to access or store ePHI, including third-party service providers, must consider in their risk analyses.

Of note, the guidance confirms that CSPs cannot rely solely on encryption to fulfill their responsibilities under the Security Rule. Though encryption to the level specified in the HIPAA Breach Notification Rule may provide a safe harbor from breach notification obligations, OCR maintains that encryption does not address many of the other Security Rule requirements that apply regardless of whether the data is encrypted. For example, encrypting data does not address how the CSP will maintain the integrity of ePHI, such as how to manage the risks from malware, or how to ensure the availability of ePHI through contingency planning for emergency or disaster situations. Encryption also does not address "administrative safeguards to analyze potential risks to the ePHI or physical safeguards for systems and services that may house the ePHI."

Despite these strong statements regarding the limited protection that encryption provides with respect to Security Rule obligations, the guidance does allow for the parties themselves to define the scope of their respective Security Rule-related responsibilities in a manner consistent with how ePHI is accessed and exchanged. For instance, if a CSP provides solely "no view services" to a covered entity or business associate customer, "certain Security Rule requirements that apply ... may be satisfied for both parties through the actions of one of the parties." Thus, although the CSP in a "no view services" arrangement may be responsible for using "reasonable and appropriate controls" to ensure that its cloud platform is encrypted, the responsibility of implementing an individual or group's access controls to the ePHI may fall solely on the customer. Thus, the OCR recognizes that "a CSP is not responsible for the compliance

failures that are attributable solely to the actions or inactions of the customer."

To address the foregoing issues, the OCR strongly recommends that written contractual terms detail how all parties will address Security Rule obligations so that OCR may rely on those provisions if it subsequently investigates the parties' compliance under HIPAA. These written provisions, however, do not need to expressly document the CSP's actual security practices or permit a customer to audit those practices.

OCR Expects Contracts to Clearly Address the Responsibilities of CSPs, Covered Entities and Business Associates

In line with the foregoing, the guidance indicates more generally that the OCR could review BAAs and SLAs for provisions that address the parties' responsibilities as they relate to HIPAA concerns, such as:

- system availability and reliability;
- backup and data recovery;
- responsibility for specific security controls (e.g., for accessing or authenticating ePHI);
- limitations on use, disclosure, and retention of the ePHI (particularly in accordance with the Privacy Rule); and
- how the ePHI will be returned or destroyed after ending the SLA.

CSPs should refer to the HHS Office of the National Coordinator for Health IT EHR Contracts Untangled guidance,[1] for sample contract terms with technology vendors that address these matters. In addition, the OCR recently published an FAQ response that specifically states its view that provisions within agreements that block a covered entity or business associate's access to its ePHI would cause all parties involved to be in violation of both the HIPAA Privacy and Security Rules.

These HHS publications, combined with the guidance, signal the OCR's focus on enforcing not only the protections necessary to secure PHI under HIPAA, but also on ensuring that parties to a BAA fulfill their obligations to make PHI available as necessary to provide individuals with their rights to access, amend, and receive an accounting of permissible uses and disclosures of PHI.

Conclusions

The guidance provides further warning to covered entities, business associates and CSPs about their obligations under the HIPAA Privacy and Security Rules. But more importantly, the guidance indicates that the OCR expects the CSP contracting and negotiation process to define and delineate each party's roles and responsibilities with respect to ePHI.

—By Jodi Daniel, Elliot Golding and Stephanie Willis, Crowell & Moring LLP

Jodi Daniel is a partner in Crowell & Moring's Washington, D.C., office. She was the founding director of the Office of Policy in the Office of the National Coordinator for Health Information Technology at the U.S. Department of Health and Human Services for a decade after serving in the Office of the General Counsel at HHS for five years. She was also one of the key drafters of the original HIPAA Privacy Rules and Enforcement Rules.

Elliot Golding is a counsel in the firm's Washington office.

Stephanie Willis is an associate in the firm's Washington office and a former associate counsel in the Office of the Inspector General for the Department of Health and Human Services.

[1] Discussed in an alert here.
