Segal Consulting

update

Compliance News for Multiemployer Plans

November 10, 2016

New Guidance on Cloud Computing and the HIPAA Privacy and Security Rules

Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage and process data, rather than on a local server or a personal computer. Many plan sponsors are turning to cloud-based systems offered by third parties to manage plan information and store data. However, questions have been raised as to how a cloud-based platform complies with the Privacy and Security Rules issued under the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH).[1] The Office for Civil Rights (OCR) of the Department of Health and Human Services (HHS) has now released guidance on cloud computing and how to address it in a HIPAA-compliant manner.

Background

In previous guidance, the OCR addressed how the HIPAA Privacy and Security Rules affect entities that store protected health information (PHI), either electronically (ePHI) or in hardcopy.[2] These entities are considered "business associates" and are therefore required to protect the security of that PHI, even if they do not access, use or disclose the information. Storage providers may include companies that host ePHI, such as hosted email, websites or servers, as well as those that store ePHI for backup, disaster recovery or archival purposes.

The new guidance focuses on cloud resources offered by cloud service providers that are legally separate from the covered entity or business associate that uses these cloud-based services.

Cloud Service Providers Are Business Associates Under HIPAA

When a covered entity hires a cloud service provider to create, receive, maintain or transmit ePHI on its behalf, the cloud service provider is a business associate under HIPAA. Further, when a business associate subcontracts with a cloud service provider to create, receive, maintain or transmit ePHI on its behalf, the cloud service provider subcontractor is a HIPAA business associate of the business associate. The cloud service provider is still a business associate even if the cloud service provider processes or stores only encrypted ePHI and lacks an encryption key for the data.

Health Compliance News Highlights:

- A cloud service provider is a business associate under HIPAA even if the cloud service provider processes or stores only encrypted ePHI and lacks an encryption key for the data.
- Even "no-view" cloud-based systems are business associates and require monitoring to ensure compliance with HIPAA.
- Plan sponsors should review their benefits systems to determine which are cloud-based and ensure that HIPAA protections are in place.

[1] The guidance is available on the HHS website.

[2] The guidance was published in the January 25, 2013 *Federal Register*.

Thus, the covered entity (or business associate) and the cloud service provider must enter into a HIPAA-compliant business associate agreement, and the cloud service provider is both contractually liable for meeting the terms of the business associate agreement and directly liable for compliance with the applicable requirements of the HIPAA rules, most notably the HIPAA Security Rule's administrative, physical and technical safeguards.

Cloud Service Providers that Provide Only "No-View" Services

A cloud service provider that stores encrypted ePHI which it cannot view or "decrypt" is providing "no-view" services. Such a cloud service provider is still a business associate and subject to the requirements set out above. However, where the cloud service provider is providing only no-view services to a covered entity or business associate, certain Security Rule requirements that apply to the ePHI maintained by the cloud service provider may be satisfied for *both parties* through the action of *one of the parties*. For example, if the plan sponsor controls who is able to view the ePHI maintained by the cloud service provider, certain access controls (such as authentication or unique user identification) may remain the responsibility of the plan sponsor.

However, because the cloud service provider is a business associate, even in the case where both parties have agreed that the customer is responsible for authenticating access to ePHI, the cloud service provider may still be required to implement appropriate *internal controls* to ensure only authorized access to the administrative tools that manage the resources critical to the operation of its information system. This recent guidance suggests that the cloud service provider and the plan sponsor should confirm in writing how each party will address the various Security Rule requirements.

Implications for Plan Sponsors

Plan sponsors should review with their benefits administration systems whether PHI is used or stored using a cloud-based service. Those that have such services should ensure that they have reviewed the use of PHI in light of HIPAA/HITECH, and that they have entered into HIPAA-compliant business associate agreements with their cloud service providers.

If existing providers use cloud subcontractors, the providers should be asked to confirm that they have business associate agreements with their cloud subcontractors.

When selecting a new cloud service provider, plan sponsors should exercise due diligence to ensure that the cloud service provider understands its obligations as a HIPAA business associate and will comply with these obligations. Hiring a cloud service provider is likely considered a change to an electronic system housing ePHI. A risk assessment should be conducted with any such change. The risk assessment should cover whether the cloud service provider is a HIPAA business associate and allocate responsibilities under HIPAA.

How Segal Can Help

Segal's Compliance Practice can help identify which service providers are HIPAA business associates to the plan and conduct a privacy assessment related to how PHI is used and stored by the plan. Additionally, Segal's Administration and Technology Consulting Practice can help select cloud service providers, as well as provide security assessments for the group health plan.

"Plan sponsors should review … whether PHI is used or stored using a cloud-based service. Those that have such services should ensure that they have reviewed the use of PHI in light of HIPAA/HITECH, and that they have entered into HIPAA-compliant business associate agreements with their cloud service providers."

Questions?

For more information about how these new rules may affect your plan, please contact your Segal consultant or the Segal office nearest you.

Segal Consulting

Segal Consulting is a member of The Segal Group.

To receive *Update* and other Segal publications, join our email list.

Follow us: