United Actuarial Services, Inc.
Actuaries and Consultants

2016-60

October 27, 2016

CLIENT BULLETIN

OCR Guidance on HIPAA & Cloud Computing

The Office of Civil Rights (OCR), the *HIPAA Privacy and Security Rule* enforcement arm of the Department of Health and Human Services (HHS), recently released guidance on *HIPAA* and "cloud computing." The guidance is available here and summarized below. In our discussion, the "covered entity" is the multiemployer group health plan and its "business associates" are plan service providers.

The OCR guidance was issued in response to questions from *HIPAA* covered entities and business associates about whether and how they can take advantage of cloud computing while complying with regulations protecting the privacy and security of electronic protected health information (ePHI).

The guidance explained that "cloud computing" takes many forms, but common cloud services provided by cloud services providers (CSPs) range from on-demand internet access to full-computing (e.g., networks, servers, storage, applications) services. For more information, see National Institute of Standards and Technology (NIST); SP 800-145, The NIST Definition of Cloud Computing - PDF.

The OCR guidance clarifies that if a covered entity engages the services of a CSP to create, receive, maintain or transmit ePHI (such as to process and/or store ePHI), on its behalf, *the CSP is a business associate* under *HIPAA*. Likewise, when a business associate subcontracts with a CSP to create, receive, maintain or transmit ePHI on its behalf, the *CSP subcontractor itself is a business associate*.

This is true even if the CSP processes or stores only encrypted ePHI and lacks an encryption key for the data. Lacking an encryption key does not exempt a CSP from business associate status and obligations under the *HIPAA* Rules.

Therefore, the covered entity (or business associate) and the CSP **must** enter into a *HIPAA*-compliant *business associate agreement (BAA),* and the CSP is both contractually liable for meeting the terms of the BAA and directly liable for compliance with the applicable requirements of the *HIPAA Rules.*

Prepared by Mike Ewing, J.D.
Director of Research
United Actuarial Services, Inc.
(317) 580-8659 • Fax (317) 580-8651
email: *mewing@unitedactuarial.com*

http://www.unitedactuarial.com

The guidance further consisted of 11 Questions and Answers. A short "yes" or "no" answer is listed below. For the full text of the Q&As, see the guidance. A specially prepared document with just the Q&As is available by "*clicking here*."

Questions and Answers - excerpts

1. *May a HIPAA covered entity or business associate use a cloud service to store or process ePHI?*
Yes

2. *If a CSP stores only encrypted ePHI and does not have a decryption key, is it a HIPAA business associate?*
Yes.

3. *Can a CSP be considered to be a "conduit" like the postal service, and, therefore, not a business associate that must comply with the HIPAA Rules?*
Generally, no.

4. *Which CSPs offer HIPAA-compliant cloud services?*
OCR does not endorse, certify, or recommend specific technology or products.

5. *What if a HIPAA covered entity (or business associate) uses a CSP to maintain ePHI without first executing a business associate agreement with that CSP?*
If a covered entity (or business associate) uses a CSP to maintain (e.g., to process or store) electronic protected health information (ePHI) without entering into a BAA with the CSP, the covered entity (or business associate) is in violation of the *HIPAA Rules*. 45 C.F.R §§164.308(b)(1) and §164.502(e).

6. *If a CSP experiences a security incident involving a HIPAA covered entity's or business associate's ePHI, must it report the incident to the covered entity or business associate?*
Yes.

7. *Do the HIPAA Rules allow health care providers to use mobile devices to access ePHI in a cloud?*
Yes.

8. *Do the HIPAA Rules require a CSP to maintain ePHI for some period of time beyond when it has finished providing services to a covered entity or business associate?*
No.

9. *Do the HIPAA Rules allow a covered entity or business associate to use a CSP that stores ePHI on servers outside of the United States?*
Yes.

10. *Do the HIPAA Rules require CSPs that are business associates to provide documentation, or allow auditing, of their security practices by their customers who are covered entities or business associates?*
No.

11. *If a CSP receives and maintains only information that has been de-identified in accordance with the HIPAA Privacy Rule, is it is a business associate?*
No.

Conclusion

Covered entities and business associates that use "cloud computing" should review the guidance carefully. The Guidance has detailed discussions of relevant provisions of the law and the allocation of duties of the *HIPAA Privacy and Security Rules* in this context.

* * *