Guidance on HIPAA & Cloud Computing

Introduction

With the proliferation and widespread adoption of cloud computing solutions, HIPAA covered entities and business associates are questioning 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). This guidance assists such entities, including cloud services providers (CSPs), in understanding their HIPAA obligations.

Cloud computing takes many forms. This guidance focuses on cloud resources offered by a CSP that is an entity legally separate from the covered entity or business associate considering the use of its services. CSPs generally offer online access to shared computing resources with varying levels of functionality depending on the users' requirements, ranging from mere data storage to complete software solutions (e.g., an electronic medical record system), platforms to simplify the ability of application developers to create new products, and entire computing infrastructure for software programmers to deploy and test programs. Common cloud services are on-demand internet access to computing (e.g., networks, servers, storage, applications) services. We encourage covered entities and business associates seeking information about types of cloud computing services and technical arrangement options to consult a resource offered by the National Institute of Standards and Technology; SP 800-145, The NIST Definition of Cloud Computing - PDF.[1]

The HIPAA Privacy, Security, and Breach Notification Rules (the *HIPAA Rules*) establish important protections for individually identifiable health information (called *protected health information* or *PHI* when created, received, maintained, or transmitted by a HIPAA covered entity or business associate), including limitations on uses and disclosures of such information, safeguards against inappropriate uses and disclosures, and individuals' rights with respect to their health information. Covered entities and business associates must comply with the applicable provisions of the HIPAA Rules. A *covered entity* is a health plan, a health care clearinghouse, or a health care provider who conducts certain billing and payment related transactions electronically. A *business associate* is an entity or person, other than a member of the workforce of a covered entity, that performs functions or activities on behalf of, or provides certain

services to, a covered entity that involve creating, receiving, maintaining, or transmitting PHI. A business associate also is any subcontractor that creates, receives, maintains, or transmits PHI on behalf of another business associate.

When 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. Further, 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. As a result, 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.

This guidance presents key questions and answers to assist HIPAA regulated CSPs and their customers in understanding their responsibilities under the HIPAA Rules when they create, receive, maintain or transmit ePHI using cloud products and services.

Questions

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

Yes, provided the covered entity or business associate enters into a HIPAA-compliant business associate contract or agreement (BAA) with the CSP that will be creating, receiving, maintaining, or transmitting electronic protected health information (ePHI) on its behalf, and otherwise complies with the HIPAA Rules. Among other things, the BAA establishes the permitted and required uses and disclosures of ePHI by the business associate performing activities or services for the covered entity or business associate, based on the relationship between the parties and the activities or services being performed by the business associate. The BAA also contractually requires the business associate to appropriately safeguard the ePHI, including implementing the requirements of the Security Rule. OCR has created guidance on the elements of BAAs[2]

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, as well as enter into appropriate BAAs. See 45 CFR §§ 164.308(a)(1)(ii)(A); 164.308(a)(1)(ii)(B); and 164.502. Both covered entities and business associates must conduct risk analyses to identify and assess potential threats and

vulnerabilities to the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit. For example, while a covered entity or business associate may use cloud-based services of any configuration (public, hybrid, private, etc.),[3] provided it enters into a BAA with the CSP, the type of cloud configuration to be used may affect the risk analysis and risk management plans of all parties and the resultant provisions of the BAA.

In addition, a *Service Level Agreement (SLA)*[4] is commonly used to address more specific business expectations between the CSP and its customer, which also may be relevant to HIPAA compliance. For example, SLAs can include provisions that address such HIPAA concerns as:

- System availability and reliability;
- Back-up and data recovery (e.g., as necessary to be able to respond to a ransomware attack or other emergency situation);
- Manner in which data will be returned to the customer after service use termination;
- Security responsibility; and
- Use, retention and disclosure limitations.[5]

If a covered entity or business associate enters into a SLA with a CSP, it should ensure that the terms of the SLA are consistent with the BAA and the HIPAA Rules. For example, the covered entity or business associate should ensure that the terms of the SLA and BAA with the CSP do not prevent the entity from accessing its ePHI in violation of 45 CFR §§ 164.308(b)(3), 164.502(e)(2), and 164.504(e)(1).[6]

In addition to its contractual obligations, the CSP, as a business associate, has regulatory obligations and is directly liable under the HIPAA Rules if it makes uses and disclosures of PHI that are not authorized by its contract, required by law, or permitted by the Privacy Rule. A CSP, as a business associate, also is directly liable if it fails to safeguard ePHI in accordance with the Security Rule, or fails to notify the covered entity or business associate of the discovery of a breach of unsecured PHI in compliance with the Breach Notification Rule.

For more information about the Security Rule, see OCR and ONC tools for small entities[7] and OCR guidance on SR compliance.[8]

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

Yes, because the CSP receives and maintains (e.g., to process and/or store) electronic protected health information (ePHI) for a covered entity or another business associate. Lacking an encryption key for the encrypted data it receives and maintains does not exempt a CSP from business associate status and associated obligations under the HIPAA Rules. An entity that maintains ePHI on behalf of a covered entity (or another business associate) is a business associate, even if the entity cannot actually view the ePHI. [9] Thus, a CSP that maintains encrypted ePHI on behalf a covered entity (or another business associate) is a business associate, even if it does not hold a decryption key [10] and therefore cannot view the information. For convenience purposes this guidance uses the term *no-viewservices* to describe the situation in which the CSP maintains encrypted ePHI on behalf of a covered entity (or another business associate) without having access to the decryption key.

While encryption protects ePHI by significantly reducing the risk of the information being viewed by unauthorized persons, such protections alone cannot adequately safeguard the confidentiality, integrity, and availability of ePHI as required by the Security Rule. Encryption does not maintain the integrity and availability of the ePHI, such as ensuring that the information is not corrupted by malware, or ensuring through contingency planning that the data remains available to authorized persons even during emergency or disaster situations. Further, encryption does not address other safeguards that are also important to maintaining confidentiality, such as administrative safeguards to analyze risks to the ePHI or physical safeguards for systems and servers that may house the ePHI.

As a business associate, a CSP providing no-view services is not exempt from any otherwise applicable requirements of the HIPAA Rules. However, the requirements of the Rules are flexible and scalable to take into account the no-view nature of the services provided by the CSP.

Security Rule Considerations

All CSPs that are business associates must comply with the applicable standards and implementation specifications of the Security Rule with respect to ePHI. However, in cases where a CSP is providing only no-view services to a covered entity (or business associate) customer, certain Security Rule requirements that apply to the ePHI maintained by the CSP may be satisfied for both parties through the actions of one of the parties. In particular, where only the customer controls who is able to view the ePHI maintained by the CSP, certain access controls, such as authentication or unique user identification, may be the responsibility of the customer, while others, such as encryption, may be the responsibility of the CSP business associate. Which access controls are to be implemented by the customer and which are to be implemented by the CSP may depend on the respective security risk management plans of the parties as well as the terms of the BAA. For example, if a customer implements its own reasonable and appropriate

user authentication controls and agrees that the CSP providing no-view services need not implement additional procedures to authenticate (verify the identity of) a person or entity seeking access to ePHI, these Security Rule access control responsibilities would be met for both parties by the action of the customer.

However, as a business associate, the CSP is still responsible under the Security Rule for implementing other reasonable and appropriate controls to limit access to information systems that maintain customer ePHI. For example, even when the parties have agreed that the customer is responsible for authenticating access to ePHI, the CSP may still be required to implement appropriate internal controls to assure only authorized access to the administrative tools that manage the resources (e.g., storage, memory, network interfaces, CPUs) critical to the operation of its information systems. For example, a CSP that is a business associate needs to consider and address, as part of its risk analysis and risk management process, the risks of a malicious actor having unauthorized access to its system's administrative tools, which could impact system operations and impact the confidentiality, integrity and availability of the customer's ePHI. CSPs should also consider the risks of using unpatched or obsolete administrative tools. The CSP and the customer should each confirm in writing, in either the BAA or other documents, how each party will address the Security Rule requirements.

Note that where the contractual agreements between a CSP and customer provide that the customer will control and implement certain security features of the cloud service consistent with the Security Rule, and the customer fails to do so, OCR will consider this factor as important and relevant during any investigation into compliance of either the customer or the CSP. A CSP is not responsible for the compliance failures that are attributable solely to the actions or inactions of the customer, as determined by the facts and circumstances of the particular case.

Privacy Rule Considerations

A business associate may only use and disclose PHI as permitted by its BAA and the Privacy Rule, or as otherwise required by law. While a CSP that provides only no-view services to a covered entity or business associate customer may not control who views the ePHI, the CSP still must ensure that it itself only uses and discloses the encrypted information as permitted by its BAA and the Privacy Rule, or as otherwise required by law. This includes, for example, ensuring the CSP does not impermissibly use the ePHI by blocking or terminating access by the customer to the ePHI.[11]

Further, a BAA must include provisions that require the business associate to, among other things, make available PHI as necessary for the covered entity to meet its obligations to provide individuals with their rights to access, amend, and receive an accounting of certain disclosures of PHI in compliance with 45 CFR § 164.504(e)(2)(ii)(E)-(G). The BAA between a no-view CSP and a covered entity or business associate customer should describe in what manner the no-view CSP will meet these obligations – for example, a CSP may agree in the BAA that it will make the ePHI available to the customer for the purpose of incorporating amendments to ePHI requested by the individual, but only the customer will make those amendments.

Breach Notification Rule Considerations

As a business associate, a CSP that offers only no-view services to a covered entity or business associate still must comply with the HIPAA breach notification requirements that apply to business associates. In particular, a business associate is responsible for notifying the covered entity (or the business associate with which it has contracted) of breaches of unsecured PHI. See 45 CFR § 164.410. *Unsecured PHI* is PHI that has not been destroyed or is not encrypted at the levels specified in HHS' *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* [12] If the ePHI that has been breached is encrypted consistent with the HIPAA standards set forth in 45 CFR § 164.402(2) and HHS' *Guidance* [13] the incident falls within the breach "safe harbor" and the CSP business associate is not required to report the incident to its customer. However, if the ePHI is encrypted, but not at a level that meets the HIPAA standards or the decryption key was also breached, then the incident must be reported to its customer as a breach, unless one of the exceptions to the definition of "breach" applies. See 45 CFR § 164.402. See also 45 CFR § 164.410 for more information about breach notification obligations for business associates.

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. CSPs that provide cloud services to a covered entity or business associate that involve creating, receiving, or maintaining (e.g., to process and/or store) electronic protected health information (ePHI) meet the definition of a business associate, even if the CSP cannot view the ePHI because it is encrypted and the CSP does not have the decryption key.

As explained in previous guidance,[14] the conduit exception is limited to *transmission-only* services for PHI (whether in electronic or paper form), including any temporary storage of PHI incident to such transmission. Any access to PHI by a conduit is only *transient* in nature. In contrast, a CSP that

maintains ePHI for the purpose of storing it will qualify as a business associate, and not a conduit, even if the CSP does not actually view the information, because the entity has more *persistent access* to the ePHI.

Further, where a CSP provides transmission services for a covered entity or business associate customer, in addition to maintaining ePHI for purposes of processing and/or storing the information, the CSP is still a business associate with respect to such transmission of ePHI. The conduit exception applies where the *only* services provided to a covered entity or business associate customer are for transmission of ePHI that do not involve any storage of the information other than on a temporary basis incident to the transmission service.

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). OCR has entered into a resolution agreement and corrective action plan with a covered entity that OCR determined stored ePHI of over 3,000 individuals on a cloud-based server without entering into a BAA with the CSP.[15]

Further, a CSP that meets the definition of a business associate – that is a CSP that creates, receives, maintains, or transmits PHI on behalf of a covered entity or another business associate – must comply with all applicable provisions of the HIPAA Rules, regardless of whether it has executed a BAA with the entity using its services. See 78 Fed. Reg. 5565, 5598 (January 25, 2013). OCR recognizes that there may, however, be circumstances where 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. The HIPAA Rules provide an affirmative defense in cases where a CSP takes action to correct any non-compliance within 30 days (or such additional period as OCR may determine appropriate based on the nature and extent of the non-compliance) of the time that it knew or should have known of the violation (e.g., at the point the CSP knows or should have known that a covered entity or business associate customer is maintaining ePHI in its cloud). 45 CFR 160.410. This affirmative defense does not, however, apply in cases where the CSP was not aware of the violation due to its own willful neglect.

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. Once the CSP securely returns or destroys the ePHI (subject to arrangement with the customer), it is no longer a business associate. We recommend CSPs document these actions.

While a CSP maintains ePHI, the HIPAA Rules prohibit the CSP from using or disclosing the data in a manner that is inconsistent with the Rules.

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. The Security Rule at 45 CFR § 164.308(a)(6)(ii) requires business associates to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the business associate; and document security incidents and their outcomes. In addition, the Security Rule at 45 CFR § 164.314(a)(2)(i)(C) provides that a business associate agreement must require the business associate to report, to the covered entity or business associate whose electronic protected health information (ePHI) it maintains, any security incidents of which it becomes aware. A security incident under 45 CFR § 164.304 means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. Thus, a business associate CSP must implement policies and procedures to address and document security incidents, and must report security incidents to its covered entity or business associate customer.

The Security Rule, however, is flexible and does not prescribe the level of detail, frequency, or format of reports of security incidents, which may be worked out between the parties to the business associate agreement (BAA). For example, the BAA may prescribe differing levels of detail, frequency, and formatting of reports based on the nature of the security incidents – e.g., based on the level of threat or exploitation of vulnerabilities, and the risk to the ePHI they pose. The BAA could also specify appropriate responses to certain incidents and whether identifying patterns of attempted security incidents is reasonable and appropriate.

Note, though, that the Breach Notification Rule specifies the content, timing, and other requirements for a business associate to report incidents that rise to the level of a breach of unsecured PHI to the covered entity (or business associate) on whose behalf the business associate is maintaining the PHI. See 45 CFR § 164.410. The BAA may specify more stringent (e.g., more timely) requirements for reporting than those required by the Breach Notification Rule (so long as they still also meet the Rule's requirements) but may not otherwise override the Rule's requirements for notification of breaches of unsecured PHI.

For more information on this topic, see the FAQ about reporting security incidents (although directed to plan sponsors and group health plans, the guidance is also relevant to business associates); [16] as well as OCR breach notification guidance [17]

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

Yes. Health care providers, other covered entities, and business associates may use mobile devices to access electronic protected health information (ePHI) in a cloud as long as appropriate physical, administrative, and technical safeguards are in place to protect the confidentiality, integrity, and availability of the ePHI on the mobile device and in the cloud, and appropriate BAAs are in place with any third party service providers for the device and/or the cloud that will have access to the e-PHI. The HIPAA Rules do not endorse or require specific types of technology, but rather establish the standards for how covered entities and business associates may use or disclose ePHI through certain technology while protecting the security of the ePHI by requiring analysis of the risks to the ePHI posed by such technology and implementation of reasonable and appropriate administrative, technical, and physical safeguards to address such risks. OCR and ONC have issued guidance on the use of mobile devices and tips for securing ePHI on mobile devices. [18]

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, the HIPAA Rules generally do not require a business associate to maintain electronic protected health information (ePHI) beyond the time it provides services to a covered entity or business associate. The Privacy Rule provides that a business associate agreement (BAA) must require a business associate to return or destroy all PHI at the termination of the BAA where feasible. 45 CFR § 164.504(e)(2)(J).

If such return or destruction is not feasible, the BAA must extend the privacy and security protections of the BAA to the ePHI and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible. For example, return or destruction would be considered "infeasible" if other law requires the business associate CSP to retain ePHI for a period of time beyond the termination of the business associate contract.[19]

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, provided the covered entity (or business associate) enters into a business associate agreement (BAA) with the CSP and otherwise complies with the applicable requirements of the HIPAA Rules. However, while the HIPAA Rules do not include requirements specific to protection of electronic protected health information (ePHI) processed or stored by a CSP or any other business associate outside of the

United States, OCR notes that the risks to such ePHI may vary greatly depending on its geographic location. In particular, outsourcing storage or other services for ePHI overseas may increase the risks and vulnerabilities to the information or present special considerations with respect to enforceability of privacy and security protections over the data. Covered entities (and business associates, including the CSP) should take these risks into account when conducting the risk analysis and risk management required by the Security Rule. See 45 CFR §§ 164.308(a)(1)(ii)(A) and (a)(1)(ii)(B). For example, if ePHI is maintained in a country where there are documented increased attempts at hacking or other malware attacks, such risks should be considered, and entities must implement reasonable and appropriate technical safeguards to address such threats.

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. The HIPAA Rules require covered entity and business associate customers to obtain satisfactory assurances in the form of a business associate agreement (BAA) with the CSP that the CSP will, among other things, appropriately safeguard the protected health information (PHI) that it creates, receives, maintains or transmits for the covered entity or business associate in accordance with the HIPAA Rules. The CSP is also directly liable for failing to safeguard electronic PHI in accordance with the Security Rule [20] and for impermissible uses or disclosures of the PHI. [21]. The HIPAA Rules do not expressly require that a CSP provide documentation of its security practices to or otherwise allow a customer to audit its security practices. However, customers may require from a CSP (through the BAA, service level agreement, or other documentation) additional assurances of protections for the PHI, such as documentation of safeguards or audits, based on their own risk analysis and risk management or other compliance activities.

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. A CSP is not a business associate if it receives and maintains (e.g., to process and/or store) only information de-identified following the processes required by the Privacy Rule. The Privacy Rule does not restrict the use or disclosure of de-identified information, nor does the Security Rule require that safeguards be applied to de-identified information, as the information is not considered protected health information. See the OCR guidance on de-identificationfor more information.[22]

---

[1] See http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[2] See http://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.

[3] As adapted from NIST Special Publication 800-144, vi:

A Public cloud is open for use by the general public and may be owned, managed, and operated by any organization. Examples are the message storage services offered by major email providers, photo-sharing sites, and certain EMR providers. Many large organizations use Private clouds that exclusively serve their business functions. A Community cloud serves exclusively a specific community of users from organizations that have shared concerns. A Hybrid cloud is a combination of any of the above, bound together by standardized or proprietary technology that enables data and application portability.

[4] See NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing (December 2011). Available at http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909494

[5] For more information see NIST SP 800-146, Cloud Computing Synopsis and Recommendations (May 2012). Available at http://www.nist.gov/manuscript-publication-search.cfm?pub_id=911075

[6] See OCR FAQ http://www.hhs.gov/hipaa/for-professionals/faq/2074/may-a-business-associate-of-a-hipaa-covered-entity-block-or-terminate-access/index.html

[7] See http://www.healthit.gov/providers-professionals/ehr-privacy-security.

[8] See http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html.

[9] 78 Fed. Reg. 5,566, 5,572 (January 25, 2013).

[10] A key used to encrypt and decrypt data, also called a cryptographic key, is “[a] parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the key can reproduce or reverse the operation, while an entity without knowledge of the key cannot.” See NIST SP 800-47 Part 1 Revision 4, Recommendation for Key Management Part 1: General (January 2016). Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf - PDF

[11] See OCR FAQ regarding impermissible blocking of covered entity access to ePHI by a business associate http://www.hhs.gov/hipaa/for-professionals/faq/2074/may-a-business-associate-of-a-hipaa-covered-entity-block-or-terminate-access/index.html.

[12] See OCR guidance regarding unsecured PHI that is subject to the Breach Notification Rule requirements http://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html.

[13] Ibid.

[14] See 78 Fed. Reg. 5,566, 5,572 (January 25, 2013). Also see http://www.hhs.gov/hipaa/for-professionals/faq/245/are-entities-business-associates/

[15] See http://www.hhs.gov/about/news/2016/07/18/widespread-hipaa-vulnerabilities-result-in-settlement-with-oregon-health-science-university.html.

[16]See http://www.hhs.gov/hipaa/for-professionals/faq/2016/under-the-security-rule-must-plan-sponsors-report-security-incidents-to-the-group-plan/.

[17] See http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html; http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

[18] See http://www.healthit.gov/providers-professionals/how-can-you-protect-and-secure-health-information-when-using-mobile-device.

[19] 67 Fed. Reg. 53181, 53254 (August 14, 2002).

[20] See Section 13401 of the HITECH Act.

[21] See 45 CFR § 164.502(a)(3).

[22] See http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/.