Cloud Security Toolkit

Navigating HIPAA While Moving to the Cloud

By Adam H. Greene, JD, MPH

Updated September 2013

Introduction

The potential benefits of cloud computing have been well established.[1] The National Institute of Standards and Technology defines "cloud computing" as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[2] In many circumstances, cloud computing services offer health care providers and health plans significant information technology savings opportunities and increased flexibility. Of course, such opportunities also come with potential risks and challenges.[3]

One such challenge is how to move information technology resources to a cloud computing platform while still complying with the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (collectively, "HIPAA"). A $100,000 settlement between the U.S. Department of Health and Human Services ("HHS") and a small physician practice regarding the use of cloud services in potential violation of HIPAA highlights the importance of this issue. The following discusses some steps that a HIPAA covered entity, such as a health care provider[4] or health plan, may consider in order to comply with HIPAA with respect to cloud computing services.

Be Cautious of Claims of "Certified HIPAA Compliance"

If you are considering storing protected health information ("PHI") with a cloud provider, the cloud provider should be knowledgeable about HIPAA (ideally, they should even spell the term correctly). Some cloud providers will market their HIPAA compliance, such as by asserting that their solution has been certified as HIPAA compliant. Without question, it is a good thing that the vendor is considering and prioritizing HIPAA compliance. When you see claims of "certified HIPAA compliant" solutions, however, you may want to dig a little deeper.

---

[1] *See* NIST Special Publication No. 800-145, *available at* <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> (Sections 5.3, 6.3, and 7.4).
[2] *See* NIST Special Publication No. 800-145, *available at* <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.
[3] *See* NIST Special Publication No. 800-145, *available at* <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> (Sections 5.3, 6.3, and 7.4).
[4] For purposes of this paper, the health care provider is presumed to conduct certain transactions electronically and, therefore, is assumed to be subject to HIPAA. *See* <http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf>, pages 7-8).

There are third parties that will assess compliance with the HIPAA Standards for the Security of Electronic Protected Health Information (the "Security Rule"),[5] but such HIPAA certification is not recognized by HHS or any other government body. If the cloud provider has had a third party review its security program against the obligations of the Security Rule, this could be a step in the right direction. However, the quality of such third party reviews may differ greatly (including the degree to which the third party understands the Security Rule). Additionally, is the cloud provider willing to share the results of any third party review?

Second, the Security Rule involves some level of subjectivity of what constitutes "reasonable and appropriate" safeguards. Accordingly, just because a cloud provider or its third-party assessor considers a control, such as an addressable implementation specification, to be reasonable and appropriate does not necessarily mean that you – or HHS – would reach the same conclusion.

Third, and most importantly, the cloud provider's HIPAA compliance does not equate to your HIPAA compliance. As discussed below, no matter how robust a cloud computing provider's security is, there are still steps that you, as the covered entity, must take to comply with HIPAA. Unfortunately, there is no "plug-and-play" HIPAA compliance, meaning that you cannot hand your protected health information over to a cloud provider and rely entirely on them for your HIPAA compliance.

If you should be cautious of general claims of HIPAA compliance, what can you do to address HIPAA compliance with the cloud provider? You can consider a number of steps, such as: (1) seeking documentation of a quality third-party assessment; (2) questioning whether and how often the cloud provider conducts a risk analysis, and whether there is any information about their most recent risk analysis that they can share; and/or (3) seeking details about what specific controls they have in place (for example, what information is encrypted, what form of encryption is used, and who has the keys?).

Do We Need a Business Associate Contract?

One of the most fundamental questions under HIPAA is whether the cloud provider will be your business associate under the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule") and the Security Rule. HIPAA previously defined a business associate as including "with respect to a covered entity, a person who … on behalf of such covered entity … but other than in the capacity of a member of the workforce of such covered entity … performs, or assists in the performance of … a function or activity involving the use or disclosure of individually identifiable health information …."[6] "Use" is defined as "with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information."[7] "Disclosure" is defined as "the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information."[8]

Under the previous definition of business associate, there was sometimes confusion as to whether a cloud provider was necessarily a business associate. First, there was some question as to whether a cloud provider, such as an infrastructure-as-a-service ("IaaS") or platform-as-a-service ("PaaS") provider, was using or disclosing protected health information when it only passively stored information but did not access it. Second, HHS has issued guidance indicating that an entity that is merely a "conduit" of PHI, but does not

[5] *See generally* 45 CFR Part 160 and Subparts A and C of Part 164.
[6] 45 C.F.R. § 160.103 (definition of "business associate").
[7] 45 C.F.R. § 160.103 (definition of "use").
[8] 45 C.F.R. § 160.103 (definition of "disclosure").

access the information other than on a random or infrequent basis to support the transport or as required by law, is not a business associate. [9] There was some question as to whether certain cloud providers were only acting as conduits. Third, HHS has issued a response to a public storage company indicating that such a company was not a business associate where it did not access the PHI that it stored for covered entities.[10] Some cloud providers considered themselves similarly situated to such storage companies.

In two actions, HHS clarified that cloud providers are generally considered business associates. In April 2012, HHS settled with a small physician practice called Phoenix Cardiac Surgery for $100,000 over potential HIPAA noncompliance.[11] The conduct at issue included the posting of electronic PHI on "a publicly accessible, Internet-based calendar" and transmission of electronic PHI to employees' personal, Internet-based e-mail accounts.[12] HHS took issue with, among other things, the physician practice's alleged lack of security safeguards, the lack of a business associate agreement with cloud providers that were handling electronic PHI on the practice's behalf, and the lack of controls that led to such electronic PHI, in the case of the online calendar, becoming accessible to the general public.[13] Accordingly, the settlement suggests that, with respect to software-as-a-service ("SaaS") cloud computing services, such as online calendars or Internet-based e-mail, a covered entity should have a business associate contract with the cloud provider if the SaaS cloud services involve electronic PHI.

In January 2013, HHS provided further clarification in a set of final regulations commonly known as the HIPAA Omnibus Rule. HHS revised the definition of "business associate" to, in short, a person who on behalf of a covered entity (or its business associate) creates, receives, *maintains*, or transmits PHI for a function or activity regulated by the HIPAA rules.[14] In the preamble to the Omnibus Rule, HHS clarified that "the conduit exception is limited to transmission services (whether digital or hard copy), including any temporary storage of transmitted data incident to such transmission" and does not include "an entity that maintains protected health information on behalf of a covered entity … even if the entity does not actually view the protected health information."[15] While the preamble does not use the phrase "cloud computing," it clarifies that "a data storage company that has access to protected health information (whether digital or hard copy) qualifies as a business associate, even if the entity does not view the information or only does so on a random or infrequent basis."[16]

Accordingly, HHS has mostly settled the question of whether a cloud computing provider is a business associate. There remains one open question, however. The above-referenced preamble to the Omnibus Rule makes reference to when a data storage company has access to PHI. The question has arisen whether a cloud provider is a business associate if it maintains only encrypted PHI but does not have the key (i.e., the key used to decrypt the encrypted PHI). HHS has longstanding guidance indicating that encrypted PHI remains PHI – the fact that it is encrypted does not necessarily mean that it may be treated as de-identified health information (which would no longer be subject to HIPAA).[17] However, in presentations subsequent to publication of the Omnibus Rule, HHS officials have informally responded to

---

[9] HHS Office for Civil Rights Frequently Asked Question No. 245, http://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/245.html.
[10] Letter from Richard Campanelli, Director, HHS Office for Civil Rights, to Elizabeth Tindall (May 12, 2003), available at http://www.regulations.gov (Document ID: HHS-OCR-2010-0016-0071)
[11] *See* <http://www.hhs.gov/news/press/2012pres/04/20120417a.html>.
[12] *See* <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/pcsurgery_agreement.pdf>.
[13] *See* <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/pcsurgery_agreement.pdf>.
[14] 78 Fed. Reg. 5688 (Jan. 25, 2013) (to be codified at 45 C.F.R. § 160.103) (emphasis added).
[15] *Id.* at 5572.
[16] *Id.*
[17] Health Services Research and the HIPAA Privacy Rule, U.S. Department of Health and Human Services National Institutes of Health (May 20, 2005), http://privacyruleandresearch.nih.gov/healthservicesprivacy.asp ("For example, an encrypted individual identifier (e.g., an encrypted Social Security number) would make otherwise de-identified health information identifiable.").

questions by indicating that a cloud provider is not a business associate if it only has access to encrypted PHI and does not have the key. In subsequent presentations where the same question was posed, the same HHS officials indicated that the matter is under consideration. Accordingly, the matter remains open. In the absence of formal guidance, however, there is some legal risk to covered entities or business associates storing encrypted PHI with a cloud provider in the absence of a business associate contract, even if the cloud provider does not have the key.

What Should Be in a Business Associate Contract with a Cloud Provider?

If a covered entity determines that a business associate contract is necessary, the next question is what should be in it. Of course, all required elements of both the HIPAA Privacy and Security Rules should be included. These include provisions related to:

- Uses and disclosures of PHI;
- Facilitation of patient rights to access or amend their own PHI in a designated record set (if the cloud provider will have designated record set information, e.g., information used in whole or in part to make decisions about patients);
- Patients' right to receive an accounting of certain disclosures (including such disclosures by business associates);
- Safeguarding of PHI;
- Access of HHS to records during an HHS investigation of HIPAA compliance;
- Restrictions for agents or subcontractors who receive PHI;
- Notification requirements for impermissible uses or disclosures or security incidents at the cloud provider involving the PHI;
- Termination provisions, including how PHI will be handled at contract termination (e.g., returned, destroyed, or maintained by the cloud provider subject to continuing restrictions); and
- Whether the cloud provider may use or disclose PHI for its own administration and management or perform certain data aggregation services (optional – the covered entity need not permit the cloud provider to do so).[18]

While the above items are standard elements of business associate contracts with which health care providers and health plans should already be familiar, the devil is in the details. For example, how quickly must the cloud provider notify the covered entity of an impermissible use or disclosure – does the cloud provider have as much time as afforded under the HIPAA Breach Notification Rule (without unreasonable delay and in no case greater than 60 calendar days from discovery), or does the contract require notification sooner? State law may affect this issue, which may be especially complicated if a covered entity operates in multiple states with differing breach notification deadlines. HIPAA provides that the contract require the business associate to notify the covered entity of security incidents, which is defined as including unsuccessful attempts to access information systems. How will the cloud provider notify the covered entity of "security incidents" that are unsuccessful? The contract must require such notification, but unsuccessful security attempts may be routine and HIPAA does not specify a particular reporting timeframe or frequency. In some cases, the cloud provider may not be willing to deviate from its own standardized language (since the cloud provider may not be able to comply with different standards for different customers). In other cases, the covered entity may have more room to negotiate, and it may be in everyone's interest to clarify each party's obligations.

[18] 45 C.F.R. § 164.504(e)(2)(ii).

In addition to these details regarding HIPAA requirements, covered entities may wish to consider additional requirements. Will the covered entity receive notification or even the right to approve whether PHI is disclosed to subcontractors? Will all PHI reside in the United States?[19] Must the cloud provider indemnify the covered entity for any liability or costs under HIPAA or otherwise attributable to the cloud provider's acts or omissions (including breach notification costs)? May the cloud provider de-identify the PHI that it receives (with such de-identified health information no longer subject to HIPAA)? There are no right and wrong answers – these issues are subjects of negotiation.

Another area to consider is what detail should be established with respect to the cloud provider's administrative, physical, and technical safeguards. For example, the agreement may go beyond general terms and require particular controls (such as level of encryption, limits on access by the cloud provider's employees, etc.).

To assist health care organizations in evaluation of cloud providers, the HIMSS Cloud Security Toolkit includes *Questions to Ask Potential Cloud Providers.*[20]

Plugging Cloud Computing Into Your Risk Analysis and Risk Management Plan

Another important area is considering the risks of cloud computing services in your risk analysis and appropriately mitigating such risks in your risk management process. It is important to note that when using a cloud provider, there are two distinct risk analyses that have to occur (if the cloud provider is a business associate) – the cloud provider must conduct its own risk analysis, and the covered entity must conduct its own risk analysis.

A covered entity should include risks associated with the use of cloud services in its risk analysis, at least with respect to the risks on the covered entity's side (in contrast to risks to the cloud provider's servers). Although there are myriad approaches to a risk analysis, one possible approach is to divide the risks based on confidentiality, integrity, and availability, such as:

- The risk that PHI may be intercepted in transit to or from the cloud provider (such risk may vary based on whether encryption or other access control is employed);
- The risk that PHI can be inappropriately accessed by unauthorized members of the workforce;
- The risk that PHI can be inappropriately accessed by authorized members of the workforce or third parties (insider threat);[21]
- The risk that PHI can be inappropriately accessed by third parties due to weak or non-existent access controls (such as the covered entity using weak passwords or default vendor passwords. misconfigured firewalls, or the failure to appropriately patch systems);
- The risk that PHI can be downloaded from the cloud provider in a manner that exposes it to potential loss or theft (e.g., saved to an unencrypted mobile device);
- The risk that PHI will become corrupted in transit to and from the cloud provider (or, if applicable, its third party data center partner and/or Internet service provider);

[19] HIPAA does not explicitly prohibit disclosing PHI to a business associate or subcontractor outside of the United States. The Privacy and Security Rules do, however, require the use of reasonable and appropriate safeguards. There is some risk that OCR or a state attorney general, in enforcing HIPAA, would deem the maintenance of PHI in a country with little legal protection to be a lack of reasonable safeguards. This risk may be lessened with strong contractual safeguards to compensate for the lack of applicable legal requirements.
[20] http://www.himss.org/ResourceLibrary/ResourceDetail.aspx?ItemNumber=10542.
[21] *See Common Sense Guide to Mitigating Insider Threats, 4th ed.*<http://www.sei.cmu.edu/reports/12tr012.pdf>.

- The risk that PHI will be unavailable due to an outage at the cloud provider (e.g., power, network, machine, storage, or other computing resources); or
- The risk that PHI will be unavailable due to a loss of network access through the covered entity's Internet service provider.

The covered entity's risk management process can then try to mitigate the identified risks pertaining to the use of cloud computing services to a reasonable level, which may include developing policies and procedures, training, on-going review, encryption, and other appropriate access controls. These may include such areas as the following:

- Appropriate use of cloud computing services within the organization;
- Automated threat mitigation;
- Automated analysis of logs;
- Password management;
- Patch management;
- When information may be downloaded from the cloud and stored locally;
- What information may be stored in the cloud;
- Addressing disruption of cloud services;
- Contingency operations and disaster recovery;
- Training on the cloud-related policies;
- Review of system activity related to cloud computing; and
- Encryption of information transmitted to and from the cloud.

To assist health care organizations in including cloud computing in their risk analysis, the HIMSS Risk Assessment Toolkit includes *Sample Risk Assessment for Cloud Computing.*[22]

The Privacy Rule and Cloud Computing

While the Security Rule includes a number of obligations for a covered entity to consider with respect to cloud computing, the Privacy Rule has fewer issues. There is no requirement to address cloud computing in a notice of privacy practices, or to agree to a patient request that information not be disclosed to a cloud provider.

A covered entity is required to document the designated record sets that are subject to the right of access by individuals.[23] Designated record sets will include medical and billing records and other records used, in whole or in part, to make decisions about patients. Accordingly, to the extent that designated record sets are maintained with a cloud provider, the covered entity may want to document this.

Additionally, a covered entity must provide a patient with timely access to PHI in a designated record set.[24] Cloud computing services theoretically should not stand as an obstacle to such access, since the purpose of cloud computing is to provide ubiquitous access to data. However, things do not always go as planned, so the covered entity should consider whether there may be circumstances where it cannot provide timely access to a patient's PHI that is maintained in the cloud (i.e., contingency operations). Ideally, the covered

[22] http://himss.files.cms-plus.com/HIMSSorg/Content/files/RA05_RA_Cloud_Computing.xlsx.
[23] 45 C.F.R. § 164.524(e)(1).
[24] 45 C.F.R. § 164.524(a).

entity should have a written plan of action which specifies what resources and workforce members need to be engaged, in such an event.

A covered entity currently must account for disclosures of PHI, other than certain excepted disclosures (such as disclosures for treatment, payment, and health care operations).[25] The accounting must include disclosures by business associates.[26] Most disclosures to and by the cloud provider presumably will be for treatment, payment, or health care operations and, therefore, excepted from the accounting requirements. The cloud provider may make some disclosures, however, that are subject to an accounting of disclosures, such as if a disclosure is made to law enforcement or is required by law. Accordingly, in the event that a covered entity receives an accounting of disclosures request from a patient, the covered entity may need to contact the cloud provider to receive an accounting of disclosures from the cloud provider (which may be the time when you discover whether your cloud provider actually follows its business associate contract obligations).

Conclusion

HIPAA does not prohibit a HIPAA covered entity, such as a health care provider or plan, from using cloud computing services, but the covered entity should not rely solely on a cloud provider's glossy marketing materials for HIPAA compliance. Rather, the covered entity should take proactive steps, such as putting into place an appropriate business associate contract where necessary and addressing cloud computing risks in a risk analysis and risk management plan. By considering the application of HIPAA, covered entities can realize the benefits of cloud computing services without foregoing patient privacy and security or exposing themselves to substantial penalties.

[25] 45 C.F.R. § 164.528(a).
[26] 45 C.F.R. § 164.528(b)(1).