Navigating the World of Cloud Computing—What Counsel Need to Know

by Rachel V. Rose

Rachel V. Rose, J.D., MBA, is the chair of the FBA's Corporate and Association Counsel Division, a member of the executive board for the Health Law and Qui Tam Sections, and co-author of two books including, What Are International HIPAA Considerations? *She may be reached at* rvrose@rvrose.com.

The impetus for this article stemmed from one of my recent flights. As I looked out the window, I saw pillow-like masses floating in a blue sky. One may view data as the cloud and the network/infrastructure as the sky. But what, exactly, is cloud computing? According to the National Institute of Standards and Technology (NIST), cloud computing is "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."[1] In layman's terms, it is the ability of an individual to access information from a network from nearly any location.

Gone are the days when nearly every entity hosted its own data onsite. The trend is to have a third party host the data in a data center. Given the recent threats, breaches, and regulations in the world of cybersecurity, it is imperative that attorneys appreciate the various cloud models, as well as laws that may be implicated. Therefore, the purpose of this article is to provide a semblance of the "cloud" and an understanding of how cloud technology companies are regarded in relation to the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology Act (HITECH).

Cloud Computing

There is a plethora of reasons to use the cloud, including cost reduction. Because cloud providers have a larger pool of customers, they are able to spread the cost. Customers share in the capital costs, infrastructure, and maintenance and, in return, pay a lower rate than they would hosting their own internal network infrastructure. This is the general rule. Once an organization has decided to explore using the cloud or switching cloud providers, adequate due diligence needs to be done.

In order to conduct adequate due diligence, an organization should ask these fundamental questions:

1. Does the cloud company perform an annual risk assessment or analysis?
2. Are their employees and subcontractors trained on cybersecurity?
3. Does the cloud company execute Business Associate Agreements if protected health information (PHI) is being created, maintained, received or transmitted?
4. What variety of cloud is utilized (e.g., community, public, or private)?
5. What type of service model is used (e.g., SaaS, PaaS, or IaaS)?

Cloud Categories and Services

How are the cloud varieties and service model types defined? The four main categories of cloud computing deployment models are community, hybrid, public, and private. According to NIST, each type is defined as follows:[2]

- Community—The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination thereof, and it may exist on or off premises.
- Hybrid—The cloud infrastructure is a composition of two or more distinct cloud infrastructures (e.g., private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).
- Public—Multiple clients of a cloud service provide shared communal storage space, hopefully with metatags to provide segregation of the individual client's data.
- Private—Involves a single enterprise and its divisions and departments.

Private clouds offer the most protection and should be strongly considered. Although public

clouds should have adequate technical, administrative, and physical security measures in place, many do not, which makes it easier for one customers' information to "cross paths" with another's or for a hacker to find a "back door" into an organization's data. It is imperative that the cloud company provides adequate assurances that each entity's data has adequate "boundaries" in place. Assessing these aspects up front can save time and money later on.

After appreciating the types of clouds, the next step is to appreciate the service models. The three varieties of service models are defined as follows:[3]

- Software as a Service (SaaS)—The consumer uses the provider's applications, which run on the cloud's infrastructure.[4] The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- Platform as a Service (PaaS)—The consumer can deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure—including network, servers, operating systems, or storage—but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- Infrastructure as a Service (IaaS)—The consumer is able to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications and, possibly, limited control of select networking components (e.g., host firewalls).

Each type of service model carries varying levels of business risk and is utilized for different purposes. And, "with acknowledged cybercriminals seeking to penetrate enterprises' clouds for financial gain, enterprises need to assess the value of the data promoted to the cloud in terms of the potential value those data may hold for people with malicious intent."[5] These types of risks should be incorporated into audits and risk assessments, such as the requisite HIPAA risk assessment or SSAE-16 SOC Reports.[6]

HIPAA and the Cloud

The Final Omnibus Rule, which was published on Jan. 25, 2013, in the *Federal Register*, provides insight into how cloud computing providers are classified and what is required of them. It is important to note that cloud computing companies are considered to be either business associates or subcontractors (depending on the relationship between the parties) pursuant to 45 C.F.R. § 160.103.[7] Under § 160.103, the following types of entities are defined and referenced in relation to HIPAA and the HITECH Act:

- Covered Entity—includes providers, health care plans, or health care clearing houses.[8]
- Business Associate—creates, receives, maintains, or transmits PHI on behalf of a covered entity.
- Subcontractor—creates, receives, maintains, or transmits PHI on behalf of a business associate.

Once the parties have been identified, it is necessary to discern the relationship between all parties involved. For example, is it a linear relationship (e.g., covered entity contracts with a business associate, who, in turn, contracts with a subcontractor) or is it a triangular relationship (e.g., covered entity contracts with two separate business associates who need to share information, or a business associate contracts with two subcontractors who need to share information). Other types of structures may exist between different parties; however, a linear and a triangular structure are the most common.

Now that the relationship has been established between the parties, it is important to ascertain whether one of the parties is exempt from executing a Business Associate Agreement and substantiating compliance with HIPAA and the HITECH Act. As espoused in the HIPAA Omnibus Rule, these entities are considered to fall under the "conduit exception." According to the *Federal Register,* "[t]he conduit exception is a narrow one and is intended to exclude only those entities providing mere courier services, such as the U.S. Postal Service or United Parcel Service and their electronic equivalents, such as internet service providers providing mere data transmission services."[9] In the *Federal Register,* the U.S. Department of Health and Human Services expressly stated that, "an entity that maintains protected health information on behalf of a covered entity is a business associate and not a conduit, even if the entity does not actually view the protected health information."[10] Hence, it is important to recognize that cloud providers and data centers do not fall under the conduit exception.

It is also important to consider state and international laws, which may have different or broader definitions of a covered entity, business associate, or subcontractor.[11] Furthermore, the Federal Trade Commission "issued the Health Breach Notification Rule to require certain businesses not covered by HIPAA to notify their customers and others if there's a breach of unsecured, individually identifiable electronic health information."[12] In sum, the conduit exception is very narrowly curtailed and liability extends beyond the federal HIPAA and HITECH acts.

Conclusion

In sum, cloud computing and HIPAA/HITECH are areas that counsel, compliance officers, and auditors need to appreciate. Even if an entity is not a covered entity (e.g., provider, clearing house, or health insurance company) numerous businesses in a variety of sectors fall under the designation of either a business associate or subcontractor—cloud providers/technology companies are one of them. Performing adequate due diligence and annual risk assessments is crucial for an organization to limit its own liability from a financial, legal, and reputational standpoint. Failing to appreciate the various models and related vulnerabilities and threats can turn those white, pillow-like clouds into threatening dark gray ones. As you log in to your email on your next flight, look out the window and look at your screen to see if your data is encrypted, at rest, and in transit! ⊙

continued on page 13

In-House Insight *continued from page 11*

Endnotes

[1]National Institute of Standards and Technology, Special Publication 800-146, *Cloud Computing Synopsis and Recommendations* 2.1 (May 2012), *available at* csrc.nist.gov/publications/nistpubs/800146/sp800146.pdf.

[2]National Institute of Standards and Technology, Special Publication 800-145, *The NIST Definition of Cloud Computing* 3 (2011), *available at* nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[3]*IT Control Objectives for Cloud Computing: Controls and Assurances in the Cloud* (2011), *available at*, www.isaca.org/chapters2/kampala/newsandannouncements/Documents/IT%20contro%20objectives%20for%20Cloud%20computing.pdf.

[4]NIST Special Publication 800-145 at 2, fn. 2 (setting forth that, "[a] cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.").

[5]*Id*. at 8.

[6]*SOC 1 Report*, SSAE-16, https://www.ssae-16.com/soc-1 (last visited June 12, 2016).

[7]*See* 78 Fed. Reg. 5566, 5572 (Jan. 25, 2013), (indicating that, "[t]he term 'person' as defined at § 160.103 includes entities as well as natural persons.").

[8]It is important to note that a covered entity may be the business associate of another covered entity. Some covered entities have both a covered entity and business associate line of business and are classified as a "hybrid entity" under 45 C.F.R. § 160.103.

[9]78 Fed. Reg. 5566, 5572 (Jan. 25, 2013).

[10]*Id*. (emphasis added).

[11]*See* Texas Health and Safety Code, § 181.001 *et seq.*, *available at* www.statutes.legis.state.tx.us/Docs/HS/htm/HS.181.htm.

[12]U.S. Federal Trade Commission, *Complying with the FTC's Health Breach Notification Rule*, www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule (last visited June 12, 2016).