Cloud Computing Privacy and Security 101

Introduction
Business and technology executives within healthcare organizations are under increasing pressure to reduce operating expenses, drive value to the business, and increase the quality of care. The current healthcare business climate requires leaders to balance business drivers with government mandates and policy considerations. Partnering with a cloud services provider can facilitate the ability to meet these challenges. When evaluating cloud services providers, careful consideration must be given to a number of issues, including that of data privacy and security and risk to the organization.

The following is intended to provide some general background on cloud computing privacy and security issues. It is not intended to focus specifically on healthcare-related issues, and so it should be read in conjunction with other documents in the HIMSS Cloud Computing Toolkit that have a specific healthcare focus, such as: (1) Top 10 Cloud Security Concerns; (2) Questions to Ask Potential Cloud Providers; and (3) Navigating HIPAA While Moving to the Cloud.

A Brief Treatment of Security Advantages and Disadvantages for Cloud Computing

Cloud computing services offer several advantages and disadvantages with respect to information privacy and security. These advantages and disadvantages will vary greatly by cloud services provider, with some offering potential customers significantly improved information privacy and security, while others may provide inferior privacy and security.

Some advantages that cloud services providers may offer in the areas of privacy and security include1:

- **Staff Specialization** - Cloud providers, as organizations with large-scale computing facilities, have an opportunity for staff to specialize in security, privacy, and other areas of high interest and concern to the healthcare organization. This cloud provider staff specialization can facilitate the healthcare organization’s ability to focus limited internal resources on core business initiatives, while entrusting the cloud provider to maintain infrastructure.

- **Platform Strength** - Greater uniformity and standardization facilitate platform hardening and enable better automation of security management activities like configuration control, vulnerability testing, security audits, and security patching of platform components.

---

• **Resource Availability** - Redundancy and disaster recovery capabilities can be built into cloud computing environments and on-demand resource capacity can be used for better resilience when facing increased service demands or distributed denial of service attacks, and for quicker recovery from serious incidents. The healthcare provider should ensure that the cloud computing environment’s disaster recovery capability will meet its requirements for restoration of data in the event of a disaster, whether manmade or natural. Standardized cloud service platform offerings can increase system availability by minimizing service interruptions that otherwise may be required for systems patching and maintenance.

• **Backup and Recovery** - The backup and recovery policies and procedures of a cloud service may be superior to those of the organization and, if copies are maintained in diverse geographic locations, may be more robust and contribute to the organization’s overall BCMP (Business Continuity Management Plan.)

• **Mobile Endpoints** - Since the main computational resources required are hosted by the cloud provider, clients are generally lightweight computationally and easily supported on portable devices.

• **Data Concentration** – Related to the previous point, data maintained and processed in the cloud can present less of a risk to an organization with a mobile workforce than having that data dispersed on portable computers or removable media out in the field, where theft and loss of devices routinely occur.

• **Improved Privacy Through Improved Security** – To the extent that the cloud services provider offers improved information security over the healthcare organization’s existing systems, the use of such cloud services may decrease impermissible uses and disclosures and related breach notifications.

Some basic concerns include:

• **System Complexity** - A public cloud computing environment adds new complexities as compared with that of a traditional data center, introducing a different set of risks that the cloud service provider and health care organization must address.

• **Increased Threat Level** – Because cloud computing services lead to centralization of information, resulting in a wealth of valuable information residing in a single location, such data centers may become more attractive targets for external attacks (although this risk may be partially mitigated by the presumption that such data centers have strong controls in place, causing many external actors to seek potentially easier targets).

• **Shared Multi-tenant Environment** - Public cloud services offered by cloud service providers have a serious underlying complication—subscribing organizations typically share components and resources with other subscribers that are unknown to them. Private cloud services do not raise this issue, but may have greater costs and require greater resources to manage.

• **Internet-facing Services** - Public cloud services are delivered over the Internet, exposing both the administrative interfaces (used to self-service and support an account) and the end user interfaces (used for end user applications access) to the Internet, which can be a potential vulnerability. Alternative solutions can be evaluated, where the customer could potentially connect to the hosting provider over a dedicated private communications link.
• **Additional Administrators** – The use of cloud services generally may mean that additional administrative users (employees and contractors of the cloud services provider) have access to the healthcare organization’s information, potentially increasing the risk of unauthorized access through the abuse of such access. Depending on the cloud configuration, the cloud customer may be able to encrypt its data in a manner that eliminates access to unencrypted data by cloud service providers’ administrators.

• **Loss of Transparency** – Cloud customers may have limited transparency with respect to the cloud service provider’s policies, procedures, and actions, such as to what extent the cloud provider discloses information to law enforcement officials.

• **Potential for Secondary Use of Data** – The cloud service provider could potentially use and disclose the customer’s data for secondary purposes, such as marketing, data mining, or other uses that primarily serve the cloud service provider.

• **Loss of Control** - While security and privacy concerns in cloud computing services are similar to those of traditional non-cloud services, they are amplified by external control over organizational assets and the potential for mismanagement of those assets. Consideration must be given to the cloud provider’s policy, process, and procedures around data security compared with those of the customer.

• **Introduction of Additional Subcontractors** – Cloud service providers may rely upon one or more subcontractors to provide services or collocate their equipment. The healthcare organization may not have control over the use of such subcontractors or transparency into their infrastructure or privacy and security practices.

---

**Key Considerations for Healthcare Organizations Considering Cloud Computing**

“Cloud computing” represents a growing form of information technology outsourcing and can be associated with many different vendor offerings. Healthcare organizations must be mindful that they bear ultimate responsibility for management of their data and compliance with legal and regulatory requirements.

When considering the use of cloud computing services, the customer must carefully consider what types of data will be hosted in the cloud environments, the associated regulatory requirements, and how this will impact their compliance planning. Will electronic protected health information (ePHI) be hosted by the cloud service provider? Will data be subject to the Payment Card Industry Data Security Standards (PCI DSS)? Where will this data be physically stored (what country) and who will have administrative and end user access to it?

Once a healthcare provider makes the decision to use a cloud service, though, it may want to look to whether it needs to upgrade its network infrastructure, bandwidth, etc., since the information and/or applications will be pulled on demand from the cloud service. The healthcare provider should also ensure that strong authentication is used (i.e. ensuring no unauthorized users are accessing the cloud services). NIST provides the following considerations as the responsibility of the organization itself:

• **Governance** - control and oversight over policies, procedures, and standards for application development, as well as the design, implementation, testing, and monitoring of deployed services.

---

Compliance - conformance with an established specification, standard, regulation, or law. Various types of security and privacy laws and regulations exist within different countries at the national, state, and local levels, making compliance a potentially complicated issue for cloud computing. HIPAA/HITECH must be considered when evaluating the migration of ePHI to a cloud based solution.

Trust - Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and, in doing so, confers an unprecedented level of trust onto the cloud provider. A clear understanding of the cloud provider’s policies and processes around security are key.

Architecture - The architecture of the software systems used to deliver cloud services comprises hardware and software residing in the cloud. Many of the “simplified” interfaces and service abstractions belie the inherent complexity that affects security. For instance, how will cloud architecture from one provider integrate with an organization’s other third party solutions? If a company leverages cloud services from multiple providers how will this impact system integration and overall architecture?

Identity and Access Management - One recurring issue is that the organizational identification and authentication framework may not easily integrate into the cloud. Extending or changing the existing identity management framework to support cloud services may be difficult and may result in additional expense.

Software Isolation - The security of a computer system depends on the quality of the underlying software kernel that controls the confinement and execution of processes. Understanding the use of virtualization by a cloud provider is a prerequisite to understanding the security risk involved.

Data Protection - Data stored in the cloud can reside in a shared environment collocated with data from other customers. Organizations moving sensitive and regulated data into the cloud, therefore, must account for the means by which access to the data is controlled and the data is kept secure. What cloud provider options are available for dedicated versus shared cloud services?

Availability - Availability is the extent to which an organization’s full set of computational resources is accessible and usable. Denial of service attacks, equipment outages, and natural disasters are all threats to availability in the cloud. Business continuity and disaster recovery are important considerations when evaluating a potential cloud solution.

Incident Response - The cloud provider’s role is vital in performing incident response activities, including incident verification, attack analysis, containment, data collection and preservation, problem remediation, and service restoration. Revising an organization’s incident response plan to address differences between the organizational computing environment and a cloud computing environment is an important, prerequisite when transitioning applications and data. The HITECH Act has increased responsibility for breach notification when ePHI is potentially compromised. Careful evaluation of the cloud provider’s role must be taken into consideration.

The use of cloud services also requires a shared security model. For example, the cloud provider can offer a high level of security, but it may fall on the healthcare organization to properly configure such security (such as through enabling encryption). Additionally, the healthcare organization retains responsibilities related to provisioning access to the service and password management. Under this model, the parties
must understand their respective responsibilities. For example, the healthcare organization must understand whether it is relying on the cloud provider to encrypt data where appropriate or whether this responsibility falls to the healthcare organization.

Conclusion
It is important to weigh the security advantages and concerns of using cloud computing services against the security posture of maintaining IT infrastructure within the healthcare organization. If a healthcare organization does not currently have strong controls in place for its data, and does not have the resources to implement adequate controls, then the information security advantages of using cloud computing services through a sophisticated and experienced cloud provider may outweigh the security concerns. By contrast, if a healthcare organization has robust controls in place, then the loss of control over security may be a greater consideration when evaluating cloud services. A healthcare organization’s current downtime (both planned downtime for system maintenance as well as unscheduled services interruptions) for its technology systems should be used as a benchmark and compared against cloud computing services provider guaranteed service levels.

The healthcare organization also should consider how it will address potential security concerns of cloud computing services. For example, a benefit of cloud computing services may be that it allows access to data and services on a variety and multitude of end user client devices, including laptops, tablets, and smart phones. The healthcare organization should consider whether data that is stored in the cloud may be copied onto such portable devices and, if so, what controls must be placed on the devices to safeguard data (e.g., encryption and authentication).

Additionally, when considering different deployment options of cloud computing services, such as a public versus a private cloud, the health care organization should recognize that there are significant security advantages and disadvantages to the different deployment models. For example, public cloud services may be offered at less cost or may include additional offerings, but these benefits must be weighed against added complexities that may adversely affect confidentiality, integrity, and availability of data.

The healthcare organization should also consider the privacy implications. If the cloud provider offers improved security, this may translate to improved privacy through reduction of risk to inappropriate uses and disclosures. On the other hand, there could be significant privacy concerns if the cloud provider uses the data for secondary purposes (such as data mining or marketing). The healthcare organization also may need to understand under what circumstances the cloud provider will provide data to law enforcement, and whether the healthcare organization will have an opportunity to learn of such disclosures.

Finally, when contracting for cloud services, the healthcare organization should carefully review, evaluate, and negotiate contract documents and service schedules to ensure a clear understanding and mutually acceptable terms for the services being provided, including the services provided related to security. The HITECH Act and subsequent regulations (such as the HIPAA Omnibus Rule) have created increased responsibilities for contracted business associates when ePHI is involved. Healthcare payers and providers must ensure that their contracted cloud services providers are able to meet these requirements, including the HIPAA Privacy and Security Rules when ePHI is to be hosted in a cloud solution. The NIST “Guidelines on Security and Privacy in Public Cloud Computing” provide a fine summary of concerns, detailed examples and a step-by-step section on considering and procuring cloud computing resources.