BUSINESS WHITE PAPER

7 Myths of Healthcare Cloud Security Debunked

Don’t let these common myths stall your healthcare cloud initiative

ClearDATA
HEALTHCARE · COMPLIANT · CLOUD

7 Myths of Cloud Security Debunked

Table of Contents

Cloud computing could be the next game-changer in healthcare – but not if healthcare IT professionals don't overcome their deep-rooted aversion to the cloud.

A conventionally risk-averse industry, healthcare has been relatively slow to adopt the cloud, citing security and privacy concerns. According to MarketsandMarkets, despite a slow start, healthcare providers are predicted to spend $5.4 billion on cloud services by 2017.

The Cloud is beginning to gain favor

As regulation pushes the industry toward storage, collaboration and accessibility, the cloud becomes even more attractive since it's often safer and more versatile than on-premises solutions. Health information exchanges also are contributing to the need for interconnected electronic medical record systems to ensure easy access to patient data. As a result, cloud-based software-as-a-service models are beginning to grow.

According to a June 2014 HIMSS Analytics Cloud Survey, 83 percent of 150 industry respondents said they currently use at least some cloud services. Another 9 percent plan to use the cloud, and just 6 percent don't plan to try cloud services. Despite the growth in cloud-based services, 61 percent of healthcare IT respondents indicated security is still a top concern.

Many of the concerns about cloud computing security are more myth than fact. Let us debunk seven of them.

Myth #1:
The cloud isn't secure enough for healthcare

A long-held perception exists in healthcare that cloud systems are inherently less secure than traditional on-premises systems. While both enterprise systems and cloud systems have an equal chance of being attacked, data shows that cloud-based systems are actually more secure than their on-premises counterparts. According to Alert Logic's 2012 Cloud Security Report, on-premises users experience an average of 61.4 attacks per year while service-provider/cloud customers experience an average of only 27.8 attacks annually.

The reason there are fewer attacks is because of better safeguards in the cloud, says Chris Bowen, chief privacy officer, ClearDATA. "With the cloud, the data centers have specialized safeguards such as perimeter controls, cameras, armed guards, biometrics, interconnected room locks, man traps, multiple pipes for bandwidth, massive UPSs and multiple power grids, which are things even large hospital systems have a hard time providing," he says.

Myth #2:
All cloud-based infrastructures are created equal

The cloud infrastructure can generally be boiled down to three components: network, storage, and computing. Each component must be purpose built for healthcare and with the use case in mind.

"In healthcare, networks must be secure, highly redundant, and designed to support 'burstability' and have communications ports designed for shared use," Bowen says. "But they must also be actively monitored and logged. Some cloud environments may be built with many of these features, but the logging requirements in healthcare often require other solutions to enable the logs to be kept, protected and archived according to specific data retention policies dictated by Health Information Trust Alliance (HITRUST), Omnibus and the Privacy and Security Rules."

Myth #3:
Data in the cloud is more vulnerable to hackers

In reality, data in the cloud is less susceptible when it is properly encrypted and secured. But it really depends on the cloud provider.

“Understanding how the provider approaches defense in depth from an administrative, technical and physical perspective is critical,” Bowen says. “Just as essential are the operating principles that the organization has developed to support a healthcare cloud. On-premises strategies are challenged to provide similar levels of service.”

Because IT security is not the core competency of most healthcare providers, turning to cloud providers can pay off since they focus on security extensively – particularly cloud providers that focus on healthcare clients. The investment of resources and staffing by cloud-based providers is difficult to match with in-house employees. Additionally, HITRUST-certified vendors are particularly attractive given the rigorous certification process vendors endure.

Myth #4:
Data in the cloud is accessible to other organizations using the same cloud

This myth is often unfounded since cloud providers take every precaution to secure the data. But since data in the cloud may be hosted on the same physical environment as others, it is important to choose a provider with the experience and know-how to ensure your data is segregated from other organizations’ data at all stages of the lifecycle.

It is important to focus on isolation tactics for added protection of data in the cloud.

“Isolation is really a core function of a lot of the virtual infrastructure that cloud providers are using,” says Rob Sadowski, of RSA, The Security Division of EMC. “Most providers are going to be segmenting customer networks into virtual LANs. They’re going to make sure that there is no cross-pollination over these virtual networks of customers. Another element to implement for isolation is the use of encryption.”

Myth #5:
Data that resides in the cloud can't be controlled or mined by providers

This myth might be the most important to debunk.

"What contributes to the perception that the cloud may not be as secure or may have some level of risk is the lack of visibility and the loss of control," Sadowski says. "The best way to ensure you have control is to extend the internal controls that you already trust into the cloud. For instance, make sure you have the same authentication, user management and access management capabilities in the cloud that you do with your on-premises solution."

Any cloud environment should allow you to maintain an auditable chain of custody for your data. "Any cloud provider that cannot guarantee this for you will put you at risk if you are ever audited by the ONC or investigated by the OCR," Bowen says. "Once data enters the cloud, it might traverse many different data centers and geographic regions, be hosted multiple places simultaneously or be dynamically relocated as needed."

Myth #6:
Identity and access management is a headache with cloud-based systems

In truth, it's not difficult to extend a provider's existing identification and authentication framework to a cloud environment. There are specific technologies (such as LDAP, SAML, Cloud Access Security Brokers, etc.) in the marketplace that can enable central identity management in the cloud. Network traffic settings also can help enable these technologies.

"Based on research we've seen, we know that healthcare providers have to increasingly adopt the cloud in order to meet the infrastructure requirements mandated by regulations and to cope with rising costs," Bowen says. "They can't necessarily meet infrastructure requirements with hardware-based solutions in their basement."

Myth #7:
I can't trust a cloud provider like I can trust my own people

This might be the most misguided myth of all since most data breaches to date are the result of employee negligence.

According to a California Data Breach Report, in 2012–13, the majority of breaches in the healthcare sector (70 percent) were caused by lost or stolen hardware or portable media containing unencrypted data, in contrast to just 19 percent of such breaches in other sectors.

Healthcare organizations are moving to secure cloud computing technologies such as virtual desktop infrastructure to allow practitioners easy access to patient data without ever storing protected health information on mobile or remote devices such as smartphones and laptops.

But there are ways to avoid this vulnerability by using the cloud. "Some of the biggest risks we see still go back to a person. But you can actually put controls in place so that even on a mobile device the data will never be stored locally," he says. "It can be viewed, but it can be completely controlled from a cloud-based environment."

To learn more about healthcare cloud security, please call (888) 899-2066 or visit www.ClearDATA.com