Business White Paper

Healthcare IT in the Public Cloud

Do-It-Yourself vs. Managed Services, Choosing the Best Approach

ClearDATA
SECURE • HEALTHCARE • CLOUD

Healthcare IT in the Public Cloud

Do-It-Yourself vs. Managed Services, Choosing the Best Approach

Table of Contents

Healthcare Cloud Migration

Health IT infrastructure is under constant pressure. Meaningful Use, advanced imaging, electronic health records, patient portals, and other applications have increased the massive growth in data volume. There is also increasing need for advanced analytics solutions to turn that data into useful, meaningful information that can be leveraged to improve patient care, develop new treatments, and improve hospital operations.

Supporting all of this activity requires tremendous investment in new servers and other infrastructure equipment, along with security and performance monitoring.

At the same time, healthcare organizations, insurers, and pharmaceutical companies are creating and absorbing unprecedented amounts of data that internal stakeholders hope to analyze and manipulate. This requires access to compute resources that would be prohibitively expensive for all but the most well-heeled research institutions to support.

The cloud solves many of these problems by providing access to nearly unlimited storage that can be expanded on demand; to hosted applications that can be centrally supported and maintained by a third party; and to compute power that can be ramped up and down based on need. This keeps costs low while maximizing scalability and flexibility.

All of this activity has to be maintained in a secure and fully compliant environment. Healthcare companies may be tempted to assume responsibility for managing that environment in an effort to either reduce costs or to maintain more control of their data.

But there are real challenges and costs associated with a DIY approach that may not be readily apparent, and that can increase the total cost of ownership (TCO) of the cloud initiative if they aren't considered. While a DIY strategy can save some upfront costs, by and large a cloud managed services provider can ultimately help the organization better utilize their IT resources, save long-term support costs, and reduce compliance and security risks.

Public Cloud: Advantages & Challenges

Public clouds such as AWS, Azure and others are becoming more attractive because of scalability, agility, features, speed to market, etc. But the key challenge becomes how to best maintain security and compliance in a public cloud.

According to Markets and Markets, global adoption of cloud services in healthcare will grow from $3.73 billion in 2015 to nearly $9.5 billion in 2020. The 2014 HIMSS Analytics Cloud Survey found that 83% of healthcare provider organizations were using cloud services.

The majority of these implementations involve the public cloud. A study from HyTrust found that 77 percent of healthcare executives planned on moving additional systems to the public cloud within the next year.

With a cloud strategy in place, organizations then have to make a tactical decision about how to manage public cloud operations. There are two broad approaches available – using internal staff to manage the cloud (a DIY approach), or working with cloud managed service provider.

For healthcare organizations this is no small decision. There are security and compliance requirements unique to healthcare, under HIPAA and the HITECH Act, that must be taken into consideration, or the company risks serious penalties and fines, potentially legal action, and severe brand damage if there is a data breach.

You may have the internal staff to manage a public cloud, but do you have the expertise? What are the business associate agreement (BAA) considerations? How much is your responsibility? What does the cloud vendor cover?

While the internal IT staff may be highly competent, managing the cloud is just one of their responsibilities. The tasks associated with remaining in compliance in a remote computing environment can quickly vacuum up scarce and expensive resources and employees. This erodes the labor and cost savings promised by the cloud infrastructure, and negates the benefits of shifting to that type of model in the first place.

Companies have to accurately compare the total cost of ownership (TCO) of using a DIY versus a managed services approach to the public cloud. Performing a thorough TCO analysis and carefully weighing the risks and benefits of each approach will ensure a successful cloud deployment. That analysis will also quickly highlight the deficiencies inherent in the DIY approach.

Security and compliance are at the heart of any health IT (HIT) initiative. Managed services by healthcare experts may be the best approach to compliance and security in a public cloud. Features and services can be deployed with the confidence that the latest security and compliance requirements are being met. HIT resources can be refocused on clinical initiatives.

DIY vs. Managed Services

There are instances where DIY can have an advantage. An internally-focused cloud development environment, for example, could be managed using internal resources, provided care is taken to manage security and compliance issues.

However, in most cases a managed service provider provides the best route to ensuring the cloud deployment is compliant, secure, and cost-effective, factors that will determine whether the project ultimately fails or succeeds. Partnering with a managed service provider that has both deep experience and understanding of the healthcare market and a strong business association agreement (BAA) in place can ensure a successful, secure deployment, while freeing internal HIT resources to focus on application-level management and clinical projects.

An MSP can also provide guidance and consulting services that can aid in performing a business review, developing a migration roadmap for applications, and suggestions for improving technology utilization or creating new efficiencies within the IT department.

To further illustrate the advantages of a cloud managed service approach cut across multiple aspects of the deployment, including:

Security: This is by far one area where a managed service partner can provide real value and expertise. Data breaches are common and are increasing, and healthcare is a common industry target. According to "Data Breaches by the Numbers" from security firm CyberSponse, in the first six months of 2015 34% of the records lost or stolen via data breach were from the healthcare industry, more than any other category.

Effectively monitoring and managing security in the public cloud requires expertise, manpower, and 24/7 visibility. Very few healthcare organizations can provide that type of monitoring for application vulnerabilities and outside threats.

In a managed services model, the service provider offers just this type of monitoring from a central dashboard across all applications and users, a more cost effective approach. Customers don't have to staff for security. They can receive alerts and respond to them in a much more scalable manner.

In fact, many data breaches in the healthcare space typically stem from on-premise issues or lost or stolen mobile devices. The majority of breaches listed as HIPAA violations by the Department of Health and Human Services were due to theft or loss of paper documents, hard drives, or mobile computing devices. While no one can prevent all security breaches, a cloud managed service provider is better positioned to notice the problem faster ad promptly respond to the situation.

The use of ad hoc public cloud deployments by uniformed or careless employees can also result in potential HIPAA or data breaches. With a managed services provider, organizations can avoid these rogue implementations by providing an existing cloud infrastructure that provides the scalability and burstability employees are looking for, while ensuring compliance.

A HITRUST-certified provider can offer compliant and secure client-side data encryption, service-side encryption, network traffic protection, as well as platform, OS, network and firewall configurations. In addition, the managed service provider can fully oversee anti-virus protection for each customer instance, update them and respond to alerts. They can also monitor and identify suspicious activity via anti-intrusion detection services.

A managed service provider offers security essentials such as data encryption (in rest and motion), multi-factor authentication, network monitoring, intrusion detection/prevention, log monitoring, hardware and OS patching, and much more which eliminate the common data vulnerabilities. Those capabilities and expertise may not be available within the HIT department.

Compliance: Similar to security, maintaining compliance with HIPAA, HITECH and other regulations requires both expertise and regular monitoring. Organizations also have to be prepared to provide an auditable information trail relative to changes or disruptions in the infrastructure.

The HHS Office for Civil Rights began Phase 2 of the HIPAA Audit Program in 2016 to review policies and procedures adopted and employed by covered entities and their business associates relative to adherence to HIPAA's privacy, security, and breach notification rules.

Managed service providers can relieve much of the compliance burden for the IT and other departments, are able to aggregate and provide the information required for an audit quickly and accurately.

MSPs can also provide HIPAA compliance dashboards so that CIOs, for example, can have a singular view of how well their data, communications, and applications measure up against the regulations relative to encryption, security, back-up schedules, and other requirements. Such a dashboard can provide a per-asset scorecard for compliance mapped against the HIPAA CFR, allowing companies to have a real-time view of compliance while also providing a compliance audit trail.

Training: Even for organizations that have large in-house IT staffs, cloud expertise may be in short supply. Managing cloud-based solutions requires the team to provide scalability and high availability at unprecedented levels. While many of these individuals may be familiar with virtualization or other technologies, most of them will likely have not utilized public cloud services. The cost to train the team is significant; for some roles, years of experience are necessary for staff to truly be effective.

Optimizing IT Resources: The other advantage of using managed services is that you can focus your HIT resources on important clinical technology initiatives. Ask yourself – does your HIT staff have the skills to do an excellent job managing the cloud infrastructure and ensuring HIPAA compliance,24/7? In addition, any customizations required in a public cloud scenario may mean that support and maintenance responsibilities fall back on your internal IT department. Staying current with the complexity of the cloud environment is also a challenge for staff with other duties. Is that the best use of your IT resources?

With an MSP, staff can stay focused on internal clients and clinical initiatives, rather than using precious hours ensuring that the public cloud remains in compliance with changing security and compliance requirements.

Data Migration: Many large providers, insurance carriers, pharmaceutical companies, and other healthcare companies rely on legacy solutions that may be years or even decades old. Transferring that data to a cloud solution can pose a significant challenge. The data migration process can potentially disrupt clinical operations and lead to system failures or errors.

A cloud MSP can help organize the migration and oversee the data transfer process to minimize those disruptions and ensure a smooth transition.

An MSP can also provide the ability to normalize and analyze data within the same location where it is managed and stored. The ability to analyze these large data sets is critical for healthcare innovation.

Compliance and Security Monitoring: Maintaining and monitoring compliance is another potential pitfall of a DIY approach, particularly when it comes to the BAA of the covered entity.

While there are public cloud providers that can offer a HIPAA-compliant environment, in many cases they expect the end user organization to monitor and maintain that environment from an availability, capacity, and scalability perspective. For IT organizations, this means they are responsible for monitoring the capacity of an infrastructure they don’t have direct control of.

If there are changes to the network or environment, such as a new practice opening new VPN tunnels, or changes to the network firewall rules, the organization must notify the public cloud provider to rectify the environment and ensure continued compliance. If the provider isn't notified, the BAA can become null and void.

In a managed environment, the cloud provider is executing the network changes directly on behalf of the customer, or at least logging those changes for HIPAA compliance on behalf of the customer. The managed service provider also provides monitoring of capacity, TCP ports, instance availability,

Conclusion

A managed service approach also helps ensure continuity and reliability of the cloud resources. This approach can also save money, reduce IT maintenance and support requirements, and provide a more secure and reliably compliant environment for your applications and data.

Using a cloud MSP also reduces the staffing and training costs for the HIT department, and makes it easier to monitor, manage, and migrate data and applications to the cloud. While DIY cloud management may save some initial costs, it ultimately produces a higher TCO (and lower return on investment) through higher operating expenses and increased risk.

About Us

ClearDATA is the nation's fastest growing healthcare cloud computing company. More than 310,000 healthcare professionals rely on ClearDATA's HIPAA compliant cloud computing HealthDATA platform and infrastructure to store, manage, protect and share their patient data and critical applications.

For more information

1600 W. Broadway Road, Tempe AZ 🏠
(800) 804-6052 ☎
www.cleardata.com 🌐

ClearDATA
SECURE • HEALTHCARE • CLOUD