Business White Paper

Best Practices in Cloud Computing for Healthcare

A pragmatic roadmap for the adoption of cloud technology in a highly regulated healthcare environment

ClearDATA
SECURE • HEALTHCARE • CLOUD

Best Practices in Cloud Computing for Healthcare

Table of Contents

Healthcare providers face a variety of resource, compliance, security, cost, reimbursement, and integration challenges that have not only strained hospital IT departments, but also have affected they way clinicians provide care.

Spurred by generous incentives to adopt electronic medical record (EMR) solutions and increase documentation, healthcare providers are now faced with collecting, managing, storing and securing vast amounts of sensitive protected health information (PHI). Reliance on EMRs and other types of clinical solutions has made providers more vulnerable to cyber-attacks and system outages. The proliferation of new software solutions and space-hungry electronic image and data storage requirement has put additional pressure on the IT staff and budget as the number of servers in the data center increases.

The number of patients each hospital or physician practice serves is also increasing rapidly. The passage of the Affordable Care Act and accompanying expansion of Medicaid in many states has increased patient counts in many states, along with the aging of the overall population. Evolving outcome-based reimbursement systems have simultaneously increased the need for more accurate data collection and analysis.

New collaborative care models require better data integration and communication among healthcare providers so that patient information can be aggregated, shared, and evaluated by every stakeholder in the care continuum (including patients). This integration allows providers to measure and improve outcomes, but has proven difficult to accomplish because of incompatibilities among different provider software systems.

What's more, all of these solutions (and the data centers that house them) must meet stringent HIPAA and HITECH Act security requirements, while providing the ability to access, analyze, and audit data quickly. As providers move more data online, the risks of keeping that data secure increase.

Clinical staff across all departments want to adopt new technology that can streamline this communication and their workflows. However, traditional IT security and compliance reviews are often too slow and inflexible, and can discourage innovation. In many organizations, this has to led to so-called "shadow IT" projects targeted at specific applications, along with data silos and and potentially damaging HIPAA violations.

As a result, an increasing number of healthcare organizations are turning to cloud-based services. According to the 2014 HIMSS Analytics Cloud Survey, more than 80 percent of healthcare respondents currently use such services, and the majority of those users plan to expand their cloud activities. Markets and Markets has forecast that the healthcare cloud computing market will experience a CAGR of 20.5 percent through 2020, while Transparency Market Research estimates the market was set to expand 21.3 percent annually from 2012 to 2018.

This mirrors the uptake of cloud services across industries. Verizon's "State of the Market: Enterprise Cloud 2014," 65 percent of enterprises are using cloud computing, and 71 percent of enterprises expect to use the cloud for external-facing production applications by 2017. The cloud is clearly mainstream.

Cloud computing offers a viable, secure alternative to premise-based healthcare solutions. Purpose-built cloud platforms can address the integration, security, and time-to-market challenges faced by healthcare organizations, while eliminating many of the headaches associated with maintaining on-site data center hardware and applications. The cloud also gives IT departments a way to centrally pilot, manage and monitor new applications without the risk associated with an accompanying investment in new infrastructure, but while also ensuring compliance, security, and good governance.

Cloud Benefits

According to the HIMSS Survey, more than half of current healthcare cloud users are leveraging the technology for hosting clinical applications. Other common uses include health information exchange (HIE), hosting human resources applications and data, and back-up/disaster recover.

In all of these scenarios, the value of the cloud lies in the technology's ability to ease the burden of managing integration, security, and other issues by shifting responsibility from the IT department to the cloud provider.

Doing so can provide improvements in agility, security, compliance, and IT costs.

Agility

For healthcare providers tasked with collaborating with other organizations, and moving quickly to accommodate value-based reimbursement models, cloud platforms provide a much faster method of developing and deploying the collaborative and analytical tools necessary to make that transition. Building and deploying these workflows or applications in the cloud eliminates the long lead times associated with capital procurement and internal architecting, while also accelerating security and compliance reviews because the cloud infrastructure has already been vetted and certified.

Staff are no longer constrained by existing infrastructure limitations, and internal IT resources can focus on these clinical initiatives rather than on managing or maintaining data center hardware.

The cloud also reduces the risk associated with these new applications. The new reimbursement and care delivery models are still immature, and providers do not want to make large investments in on-premise systems knowing that requirements are likely to change. Efforts are underway by private payers, managed care organizations, and the Centers for Medicare and Medicaid Services (CMS) to implement pay-for-performance models, but these programs are in various stages of development and exactly what the industry will look like in a few years is not clear. IT systems used to managed care or collect compliance data may face vastly different sets of requirements in just a few years.

Cloud-based solutions can be rapidly scaled up, altered, or even shut down quickly without large capital investments or write offs. IT teams can experiment with new solutions economically, and respond to user needs much more quickly.

Security

Cyber attacks in all industries are on the upswing, and healthcare providers are hardly immune. As providers increase their reliance on electronic resources, their risk of a breach, data loss, and HIPAA/ HITECH violations also increases. Advances in technology and the sophistication of cyber criminals make it nearly impossible for a healthcare provider to devote enough resources to keep their PHI secure.

Credible cloud hosting providers offer 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 vulnerabilities that lead to breaches. In fact, the technology has advanced to the point that cloud solutions are often more secure against data breaches and losses than on-premise data centers.

Cloud providers can leverage highly specialized security expertise that may not be available within the healthcare provider's IT department, provide continuous monitoring of potential threats, and establish global visibility into security compliance of all applications and workflows that, in an on-premise environment, may be housed in disconnected or siloed hardware assets.

While there is still some reluctance to put patient records into a cloud-based system because of security concerns, an evaluation of actual HIPAA violations can easily put that to rest. The vast majority of breaches are due to theft or loss of paper documents, hard drives, or mobile devices and laptops. (Of the 1,413 incidents listed on the HHS website as of December 2015, 58 percent of those were due theft or loss.)

Hacking and other IT incidents accounted for just over 10 percent of breaches. While HHS does not specifically track cloud-related incidents, the majority of hacking breaches did not involve a business associate. Anecdotal information and the descriptions in the HHS database indicate the majority of those incidents involved misuse of data by internal employees of the healthcare provider. For example, a breach at Oregon Health & Science University involved unauthorized storage of unencrypted patient data in the cloud by two residents. Likewise, St. Elizabeth's Medical Center in Brighton, Mass., received a $218,000 fine for HIPAA violations after staff improperly used a public file sharing service.

The problem in these cases was not the cloud; it was improper use of the cloud by uninformed or careless employees.

In fact, use of cloud-based data could significantly reduce all types of HIPAA violations. By providing online, secure and encrypted access to data in the cloud from any computer (provided the user has the right credentials), hospitals can reduce the need to store or transport patient information on laptops or other devices. A lost laptop would no longer compromise the PHI of thousands of patients. By not storing patient information on portable devices, providers can protect themselves from the majority of potential violations and breaches.

Compliance

One of the biggest reservations healthcare providers have about shifting from an on-premise to a cloud-based IT strategy centers on compliance with HIPAA, HITECH, Meaningful Use requirements, and other industry-specific regulations.

However, managing compliance internally can be costly and challenging. When you work with a cloud provider, you aren't just investing in their technical infrastructure, you are also investing in their expertise and staffing. Healthcare providers pay a premium for IT staff that are versed in healthcare security requirements and cloud technology. Cloud platform providers offer economies of scale so that they can provide those resources in a scope that no single hospital, for example, could afford to keep on staff.

Selecting a cloud provider with deep healthcare knowledge and expertise is the first step. They should also be willing to sign a strong business associate agreement (BAA) that transfers compliance risk from the internal IT department to the cloud vendor.

Consider basic functions like file sharing. As is evident in the number of data breaches and HIPAA violations caused by unauthorized use of public, cloud-based solutions by individual employees or whole departments, providers want an easy way to store, access, and share files. By using a single secure and compliant cloud services provider, and making it easy for all employees to correctly utilize those services, hospitals can ensure a single, compliant point of service with an established BAA. The alternative would involve attempting to build a compliant solution, establishing multiple business associate agreements with different vendors, and/or chasing down ad hoc “rogue” file sharing solutions.

Putting patient data and clinical applications in the cloud creates a central point of compliance monitoring. Data can be restricted such that users are forbidden from downloading or storing it on another device with out the proper credentials, and when the data is moved or altered, a cloud-based solution can create an auditable record of those transactions.

Cost Efficiencies

Cloud solutions are not necessarily always less expensive than on-premise solutions, but they do provide other economic benefits that can provide long-term benefits to the healthcare organization.

First, moving to the cloud shifts technology from a capital expense (CapEx) model to an operating expense (OpEx) model. CapEx IT investments are an ongoing concern because they must be maintained, updated, and expanded to meet changing service and storage needs. Shifting these IT costs from capital expenses to OpEx can be an advantage from a budgeting standpoint. In addition, operating expenses are 100% reimbursable by the federal government for hospitals attesting to Meaningful Use; capital expenditures are only partly reimbursed.

The cloud also eliminates ongoing data center, server, and OS maintenance and support. This can allow you to shift IT resources to activities that serve clinical outcomes, rather than hardware upkeep.

Cloud solutions also provide a more flexible expense model. You only pay for what you use, so there is no need to invest in massive amounts of capacity for future growth or to run workloads that require short bursts of high compute resources and storage. With the cloud, you can start small and scale up (or down) as demand and storage needs change.

However, organizations looking for the cloud to produce large cost savings may not find them. In the HIMSS survey, less than half of respondents reported getting the data they needed from their cloud services provider to measure the value of the services.

Common Cloud Workloads

Hospitals and other providers are already using cloud solutions for a wide variety of workflows and applications, but they can all be classified into four general buckets:

Managed Infrastructure: Many organizations use the cloud as a way to reduce their data center management requirements. In these cases, they access cloud-based storage, networking, or computing resources, which gives them the flexibility to shrink or expand capacity quickly and cost-effectively.

Application Hosting: This was the most common scenario in the HIMSS survey, with 52.4 percent of respondents using the cloud for hosting clinical applications and data, and between 25 percent and 41 percent hosting a variety of human resources, financial, operational, and back-office applications. Hosted applications can come in a number of flavors. The application provider may offer a hosted version of the software that multiple customers access. Hospitals also may move their own proprietary applications to the cloud to make it easier to update, manage and provision the software from a central point. The majority of cloud users in the HIMSS survey (66.9 percent) were using a software as a service (SaaS) hosting model of some sort.

The types of applications used in the cloud vary by organization. Many hospitals leverage the cloud for capacity-hungry imaging applications, or data intensive population health management. E-mail, electronic medical records, and labor tracking are also frequently access via this model.

Analytics is another important area of cloud development and a critical part of the evolving care delivery model. Organizations need to be able to measure the cost and quality of care, along with the effectiveness of care delivery, and then share those measurements with other constituents (patients, insurers, federal agencies, etc.). The cloud is particularly well suited for this because stakeholders who are not part of the same organization can easily share data and collaborate in the cloud, even if they use different application platforms.

Additionally, providers can leverage the cloud for new, innovative applications and initiatives that would otherwise be too costly or time-consuming to launch through traditional channel. Using a cloud platform, providers can develop new workloads and applications that require speed and flexibility that wouldn’t be possible if they were developed in house. Under on-premise models, these types of shadow IT/skunkworks projects wouldn’t be able to quickly get through security, privacy or compliance reviews. Solutions developed in specific departments to enable data sharing or apps used to gather data for population health studies could be quickly built and deployed in the cloud, relying on already established and hardened security certifications and BAA of the cloud platform provider.

Disaster Recovery and Off-Site Back-Up: Similar to cloud-based storage scenarios, healthcare providers can access pay-as-you back-up infrastructure. There's an added appeal for healthcare users, as well. Meaningful Use Stage 2 requires providers to protect electronic health information, and that includes off-site HIPAA-compliant storage, back-up, and disaster recovery measures. Cloud-based resources eliminate the need to make ongoing investments in security and infrastructure, while making it easier to expand off-site storage.

Consumer and Provider Engagement: For new collaborative care models to work, all stakeholders need to be able to access and interact with healthcare data, including patients, physicians, and other providers. A cloud-based infrastructure can provide universal access to key data via patient and physician portals that don't require direct integration with other providers' infrastructures, and without requiring direct access to sensitive clinical systems.

Cloud solutions also provide "neutral" territory where data can reside when competing health systems need to collaborate on care. Getting patient data to follow the patient to different provider locations can be challenging, especially if those providers use different types of clinical software systems. If that data resides in the cloud, authorized providers can access it no matter what type of internal platform they utilize. As previously mentioned, analytics tools and other applications can also be built and hosted in the cloud to enable this type of cross-provider collaboration and population health management.

Key Considerations for Selecting a Cloud Provider

Identifying the right cloud platform provider for your organization is critical if you want the transition to be successful. Vendor evaluation should be largely informed by your most important business requirements and technology requirements. Those requirements will guide development of an in-depth checklist that will help you match vendor capabilities to your own business needs.

While deployment models vary, there are several key areas that you should evaluate during the selection process:

Security: How does the provider keep your data safe? Evaluate their certifications and their specific knowledge of healthcare security and privacy regulations. What types of encryption and authentication do they use? Is there a chief privacy officer? According to HIMSS, top factors that healthcare organizations evaluated before selecting a cloud provider included willingness to enter into a BAA, as well as physical and technical security. Make sure the cloud services provider has deployed the necessary firewall, intrusion detection, and denial of service protection solutions required to keep you information secure, and that they thoroughly vet, restrict and monitor staff.

Compliance: Make sure they offer, or are willing to sign, a strong HIPAA business associate agreement (BAA). That agreement should have real “teeth”, establishing the level of risk the vendor is willing to assume and what the consequences are of a violation of the terms.

Business associates (and their subcontractors) must adhere to the HIPAA Breach Notification Rule. Covered entities are liable for acts of their business associate agents, so carefully vetting a cloud services provider and establishing a BAA is even more important.

Healthcare Expertise: Does the cloud service provider understand the healthcare industry? Supporting healthcare applications in the cloud requires an intimate understanding of complex security and compliance issues, as well as providing reliable service. In the HIMSS survey, 60.5 percent of respondents reported that compliance with regulations and laws was a factor in their cloud services provider selection, while 51.6 percent cited the number of healthcare entities the provider has as customers. Cloud-based data and applications must meet the same stringent HIPAA privacy requirements as those held on your own premises.

Cloud providers, even if they never view the protected health information they hold, are still considered business associates under HIPAA rules. If they won't sign a HIPAA BAA, you shouldn't use them. If they claim to be HIPAA compliant or audited, make sure they have actually undergone an independent audit measured against the current OCR HIPAA Audit Protocol.

Workload Suitability: This requires both a review of the vendor and of your internal capabilities. Determine whether your applications can run in a multi-tenant cloud environment, and if moving to that model has any performance implications. Evaluate your own network bandwidth; if you are moving large amounts of files or data, you could overwhelm your own network and cause latency issues. In the HIMNSS survey, roughly half of respondents reported upgrading their network infrastructure and/or monitoring capabilities to prepare for a cloud implementation, while 37 percent reported creating or modifying existing business processes for cloud services.

Some applications may also be easier to move to the cloud than others. Older, legacy systems (particularly proprietary solutions) can require substantial re-coding in order to transition to the cloud. In that case, it may not make financial sense to make the change. Prioritize applications based on their technical and financial viability.

Service Level Agreement (SLA): There should be clear expectations about security, uptime, and responsiveness. Make sure the vendor understands and can support he rigors and urgency required for managing mission-critical healthcare applications.

According to the HIMSS survey, half of respondents experience problems with their cloud service provider's ability to meet their service requirements, and two-thirds reported challenges such as lack of visibility into ongoing operations, costs/fees, and customer service. Make sure the SLA clearly spells out your expectations, and the consequences for the service provider if there is a failure.

Support: Just as with on-premise solutions, vendor support is crucial to keeping your systems reliable and available. Support expectations should be spelled out in the SLA. Outage alerts should be prompt, and you should have adequate access to technical support 24/7.

Data Migration: Depending on the state of your legacy infrastructure, transferring existing data to a new cloud solution may pose a challenge. Determine up front which party will oversee that migration, and whether the process might disrupt clinical operations. Mapping old data to a new system can lead to system failures or errors so identify potential challenges up front so that you can give them adequate attention during deployment.

Management Capabilities: The cloud service provider should provide a customer portal that allows you to monitor performance and availability, history, and other information. Is there a central console that allows you to manage virtual servers? Can the provider offer load balancing features, or on-demand procurement of new servers?

Getting Started

A cloud transition is much more complex than simply transferring some data and flipping a switch. Organizations should develop a thorough cloud roadmap with a holistic view of all operations that may make that migration. Determine which workloads or applications can be transferred to the cloud now, and which may have to be transitioned at a later date. There may be some applications that can't be migrated because of technical or operational limitations.

You'll also need to identify and assign internal resources from both the IT and clinical staff to oversee and guide the transition, and arm them with the time and budget necessary to make the project a success. The team can use the selection criteria above to evaluate and select a cloud service provider.

The team will also need to gather the data necessary to calculate the return on investment in moving to the cloud. That savings calculation should include not just the direct cost of purchasing on-premise hardware and software, but also ongoing support and maintenance costs. The ROI discussion should also take into account the value of improved compliance and security, as well as the speed and flexibility provided by the cloud infrastructure.

Finally, commit to making a decision. The evaluation process should not be open-ended; establish a deadline and set specific goals. Healthcare providers can no longer delay taking a serious look at cloud-based IT solutions. If they haven't already, non-IT executives and board members are going to start asking the IT department about its plans for the cloud, vendor evaluations, potential pilots, and a long-term strategy. Now is the time to begin that evaluation and launch some initial pilot projects so that your team can gain some experience working in the cloud environment.

Pressure is mounting to more quickly develop and deploy innovative workflows and applications that can help healthcare providers transition to new models of care and reimbursement. They must do so under security requirements that are increasingly difficult to meet without a significant investment in infrastructure and manpower. The cloud offers a way to more quickly adopt new applications while refocusing IT resources on clinical improvements and reducing the security and compliance burden on healthcare providers.

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