Business White Paper

5 Risks Hospitals Face When Using The Public Cloud

(And How To Overcome Them)

ClearDATA
SECURE • HEALTHCARE • CLOUD

5 Risks Hospitals Face When Using The Public Cloud

(And How To Overcome Them)

Table of Contents

Hospitals and other healthcare organizations are in the midst of a major digital revolution that's forcing them to change their traditional ways of capturing, storing, and sharing information. To keep up with their needs for greater IT infrastructure agility, performance, security, and compliance, many savvy healthcare organizations are exploring the benefits of the cloud. The allure of on-demand cloud services combined with advances in cloud security have transformed the healthcare IT mindset from "Why move to the public cloud?" to "What should we move?" and "How do we do it?"

There are myriad studies that confirm healthcare IT workloads are moving to the cloud, and the majority of these implementations involve the public cloud with big name providers such as Amazon Web Services (AWS) and Microsoft Azure. A 2014 cloud survey from HIMSS (Healthcare Information and Management Systems Society) revealed that 83 percent of healthcare provider organizations are now using cloud services. A more recent study from MarketsandMarkets predicts the global adoption of cloud services in healthcare will grow from $3.73 billion in 2015 to nearly $9.5 billion in 2020, growing at a CAGR (compound annual growth rate) of 20.5 percent.

The list of healthcare IT workloads moving off premise is growing, too. According to the Cloud Standards Customer Council's (CSCC) Impact of Cloud Computing on Healthcare report, these workloads comprise six categories:

- **Clinical Research.** The explosion of data from DNA sequencing requires high-end compute power to process. Pharmacology vendors are tapping the cloud to improve research and drug development and to lower the cost of developing new drugs.

- **Electronic Medical Records (EMRs).** Moving medical records and medical image archiving services to the cloud allows hospital IT departments to focus on supporting other imperatives such as EMR adoption and improved clinical support systems.
- **Telemedicine.** Cloud technology is a key driver of telemedicine solutions that enable team-based care and collaboration via video conferencing and can be extended to rural environments for physician-to-physician or physicians-to-patient consultations and disaster response services.
- **Big Data.** EHRs, radiology images and DNA sequencing are just a few examples of sources generating big data in healthcare. Moving this data to the cloud enables hospitals and other healthcare organizations to more easily access information in a timely manner.
- **Analytics.** In addition to storing big data, the cloud is playing a key role in helping healthcare providers analyze data and quickly gain actionable insights.
- **Health Information Exchange.** Health information exchanges (HIEs) help healthcare organizations to share data contained in proprietary EHR systems. CIOs may accelerate the deployment of HIEs via a linkage to a strategic cloud implementation.

The Cloud Disconnect — Results Not Meeting Expectations

In 2014, industry analyst firm Enterprise Management Associates (EMA) conducted a survey of more than 400 IT professionals around the world. They were asked to share their experiences with public cloud IaaS (Infrastructure as a Service) providers, such as AWS, Azure, and Rackspace. The objective was to gather better insight into their successes and failures, achievements and challenges, wants and needs. Based on the title of their report that followed the research, "Casualties of Cloud Wars: Customers Are Paying the Price," you can imagine which side of the success vs. failure spectrum the responses landed on. The analyst group's conclusion was that companies using large IaaS vendors are experiencing failure rates nearly 60 percent of the time.

Cloud adoption studies conducted by other analyst groups reported similar or worse findings. Thomas Bittman, VP distinguished analyst at Gartner, for example, published "Problems Encountered by 95% of Private Clouds," which was based on feedback from 140 respondents who had private clouds in place. Only 5% of respondents reported having no major problems.

While there are a lot of different angles and categories by which these problems and failures can be categorized and evaluated, there are five major risks (and subsequent pitfalls) hospitals and other healthcare organizations should pay attention to before moving their IT workloads to a public cloud environment.

Risk 1: Overburdened IT Staff

Cloud providers have done a great job marketing their services as a way to make our lives simpler. Do you want an easy way to your personal photos and documents are protected from a hard drive crash or natural disaster? Back up your computer to the cloud. Do you want an easier way to organize and share photos, videos, and other digital resources with friends and colleagues? Use the cloud.

Consumers may be able to experience the benefits of the public cloud with little planning, education, and cost commitment, but for healthcare organizations there is much more involved than merely moving IT resources from A to B. For starters, the methods used for connecting, configuring, and testing resources is different. Unlike the on-premise practice of physically plugging in devices and connecting wires, cloud resources are managed through software. Even those familiar with concepts such as virtualization will find the methods for maneuvering in the cloud to be a big leap requiring training and/or coaching.

Security and compliance risks, which we will delve deeper into later, also contribute to the burden placed on the IT staff. The IT staff has to ensure the cloud provider's master agreement terms and conditions align with their Business Associate Agreement (BAA), which is a requirement of the HIPAA Omnibus Rule.

Additionally, common IT tasks such as change management, capacity planning, and availability planning don't go away after workloads move to the cloud; they just evolve in the way they are handled.

The burden placed on the IT staff is probably the most underestimated challenge of operating healthcare IT workloads in the cloud. The process can be especially daunting for healthcare organizations that lack enterprise cloud experience, and it can easily contribute to a number of additional risks and pitfalls.

Risk 2: Security

Hospitals and other healthcare organizations are well aware of the concerns associated with securing PHI (protected health information) within their facilities. Enterprise cloud providers offer superior security than what most companies have available. So, how is security one of the major risks of moving workloads to a public cloud environment? The primary public cloud security risk is a disconnect between the healthcare organization and cloud provider as to who is responsible for applying and managing each aspect of security. This communication breakdown most often occurs after the implementation — when everything appears to be working and both parties turn their focus on other projects. For example, is reviewing server logs the cloud provider's responsibility or the healthcare organization's responsibility? Without checking this security detail upfront, it's possible neither party claims responsibility for this important task.

To mitigate security vulnerabilities, healthcare organizations should use an ITIL (Information Technology Infrastructure Library) best practice known as RACI to determine who is responsible, accountable, consulted, and informed about each cloud security tenant. Additionally, healthcare IT personnel should view moving to the cloud as gaining an IT person, perhaps, but not an entire IT security team. There will continue to be several security tasks the health IT team will be required to manage.

Risk 3: 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.

Many compliance-related responsibilities are outlined in the BAA, which all too often healthcare organizations, cloud providers, or both parties don't fully understand before signing. One example is when a healthcare company publishes PHI inside a public cloud provider's environment. Over time, the healthcare company may make firewall rule changes to the cloud environment, but fails to notify the cloud provider of the changes. A closer look at the BAA requires that the environment be recertified to ensure compliance is being maintained. By failing to take these steps a healthcare organization can inadvertently nullify its BAA with the cloud provider.

It's important to note, too, that while public cloud providers may sign BAAs, it doesn't guarantee that the cloud provider understands what it's signing. It's imperative for the health IT team to discuss and validate key points of the agreement to ensure both parties are on the same page.

Lastly, one of the most overlooked compliance-related risks has to do with the audit process. In 2016, the HHS Office for Civil Rights began Phase 2 of the HIPAA Audit Program. Phase 2 entails reviewing 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. Cloud providers vary widely in how well they will assist healthcare organizations during an audit. It's highly recommended that healthcare organizations find out how familiar the cloud provider is with the audit process and how accommodating they will be if the healthcare organization is audited.

Risk 4: Manual Processes

This risk/pitfall is probably the most surprising on the list, especially for those who have never gone through the planning, migration, and management phases of a cloud project. Sometimes organizations think they can save money by relying solely on their internal staff to manage the entire process. This "learn as you go" approach brings with it the requirement to create new business processes and procedures from scratch and continuously revise and improve the procedures after repeated trials and errors. Inevitably, manual processes lead to oversights, which can range from problematic (e.g. hours of downtime caused by missed steps during a mission-critical application switchover) to very serious (e.g. accidentally exposing PHI in the cloud due to not confirming security responsibilities with the cloud provider ahead of time).

Even if no major occurrences happen during the planning and migration phases, manual processes can come back to haunt an organization later. Post-implementation problems are most likely to occur when new workloads are added or changes in security policies are made. Managing manual processes over the long-term is almost always a recipe for disaster, especially as the number and complexity of workloads moving to the cloud increases.

Risk 5: Unexpected Costs

Ironically, the fifth major risk/pitfall, unexpected costs, occurs most often when cost savings are the sole focus for moving to the cloud. The reason this happens is that companies tend to look at the cloud in terms of only compute and storage. Perhaps the healthcare organization has legacy servers reaching end of life, or it needs to upgrade appliances to accommodate increasing demands. The health IT staff compares the cost of buying new equipment and installing it on premise to the cost of self-provisioning these same resources in AWS, Azure, or another public cloud environment. This tunnel vision causes the organization to overlook the security-, compliance-, planning-, and migration-related manual processes and labor expenses we covered earlier. And, the end result is the same disillusionment and disappointment highlighted in the analyst reports earlier.

Partner With A HITRUST-Certified Expert

For internal, private cloud deployments, a DIY (do it yourself) approach may be a viable strategy, provided care is taken to manage security and compliance issues. When it comes to moving healthcare IT workloads to the public cloud, however, partnering with a managed service provider (MSP) is more often the better route to success.

A HITRUST (Health Information Trust Alliance)-certified MSP that has deep experience and understanding of the healthcare market and a strong BAA is the best bet. The MSP can provide guidance and consulting services for business reviews, migration roadmaps, and make suggestions for improving technology utilization or creating new efficiencies within the IT department.

An MSP can provide additional value after the cloud project has been implemented, too. For example, some MSPs offer HIPAA compliance dashboards that provide healthcare IT professionals with a singular view of their data, communications, and applications, which simplifies security and compliance management requirements. An MSP also can help healthcare organizations reduce their staffing and training costs, which ultimately contributes to a higher TCO (total cost of ownership) on the project.

Conclusion

The evidence is clear that hospitals and other healthcare organizations are seeing the potential of moving data, apps, and other IT workloads to the cloud. Many have already taken some steps in that direction and over the next few years many more will follow suit. Staying mindful of the five major risks that accompany the move to the cloud will help ensure hospitals and other healthcare organizations avoid becoming “cloud casualties” and can experience the promise and full potential that the public cloud has to offer.

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

Sponsored By

Health IT OUTCOMES

ClearDATA
SECURE • HEALTHCARE • CLOUD