Business White Paper

Moving to the Cloud: Key Considerations for Healthcare Technology

ClearDATA
SECURE • HEALTHCARE • CLOUD

Moving to the Cloud: Key Considerations for Healthcare Technology

Table of Contents

For healthcare institutions, cloud-based solutions are becoming an increasingly attractive IT option to cut costs, support on-demand provisioning and more diversified infrastructures, and obtain higher levels of flexibility and security.[1] However, many healthcare IT leaders are uncertain about whether or not migrating portions of their IT to the cloud makes sense, which steps to take, and in what order.

Several concerns have held healthcare organizations back from moving ahead toward full-scale cloud migrations. Healthcare IT leaders may have security concerns due to the alarming growth of HIPAA privacy and security breaches.[2] IT healthcare leaders also are often uncertain of the business, clinical, and IT reasons for pursuing a cloud strategy. Will it pay off? What are the risks and rewards? The biggest difficulties lie in understanding where to start, which data and systems can be migrated and when, and determining resource requirements.

Many moves to the cloud fail to meet expectations due to improper planning. Before making any changes or moves, develop and stick to stringent planning documents, processes, and procedures to govern any cloud-based projects.[3]

A Pragmatic, Well-Planned Approach

Although it may seem obvious, the best way for healthcare organizations to determine the variables and sensible options involved in moving to the cloud is through a comprehensive migration assessment and plan. In order to reduce risks and move forward with confidence, the first step in moving to the cloud is to conduct a comprehensive review of the existing IT infrastructure, and then develop a cloud technology strategy that

1 http://www.thewhir.com/web-hosting-news/hybrid-cloud-growth-driven-enterprise-deployment-marketsandmarkets-report

2 http://www.healthcareitnews.com/news/hipaa-data-breaches-climb-138-percent

3 http://www.phoenixhealth.com/info-security-privacy/cloud-computing/

includes pragmatic recommendations and a migration roadmap for intelligently moving to the cloud step-by-step, starting with what makes the most sense to tackle first.

Although most healthcare organizations possess highly skilled IT staff, they are almost always consumed by maintaining day-to-day operations: ensuring that electronic medical records (EMRs), picture archiving and communications systems (PACs), billing and other systems are operating properly. Of necessity, their jobs often revolve around day-to-day, reactive requests and issues.

Healthcare IT professionals have little time to spare to invest toward longer-term initiatives and considerations in moving to the cloud. Migrating to the cloud is best accomplish through reliance on a trusted, outsourced team of consultants dedicated solely to the healthcare industry who can develop a comprehensive analysis and corresponding report with insights and recommendations on infrastructure, data, and financial considerations.

What to Expect When Moving to the Cloud

The consultants should be able to walk through a comprehensive, proven, and systematic approach that includes:

Deliverables

- A comprehensive review of all business and clinical applications (EMR, PACS, billing, etc,) and assignment of each into one of three categories:
  - Applications that can be immediately migrated
  - Applications that can be migrated in the future
  - Applications that cannot be currently migrated due to technology or business constraints.
- A migration roadmap for all near-term and long-term applications than can be moved into the cloud.
- A list of recommended technology and/or applications that the organization is not currently using that could move the business

forward. These value-added applications could be deployed from the start in the cloud. The consulting team should be able to provide the reasoning and business benefits of adopting cloud-based solutions.

- A review of existing technology deficiencies and recommendations for implementing improvements. Examples include leveraging virtual desktops as an easy, cost effective solution for hospitals still using Microsoft Windows XP versus upgrading to a new operating system.
- An in-depth evaluation of resources, including staffing resources and budgets, to provide recommendations for improving efficiencies within current constraints.

Next Steps: Setting Goals and Identifying Limitations and Opportunities

Once the third-party provider has a clear picture of your entire environment, they should learn about your primary goals and limitations. These may include limited bandwidth and latency issues, or the need to execute a more comprehensive backup and disaster recovery (DR) plan. Key service providers should be informed, and ask the right questions to facilitate a move – or partial move – into the cloud.

Performance and latency

Be sure the consultants test your bandwidth, if your organization has not already done so. Conduct a poll of physicians and others in the organization to determine whether or not latency is an issue.

Back up, DR, and Emergency Preparedness

Work with consultants to determine the status of backup, DR, and Emergency Preparedness. Have your plans and strategies been updated since moving to electronic medical records? Also consider your imaging (PACS) strategy and data growth, and determine if it makes sense to update it or move image storage into the cloud.

Compliance and security issues

Evaluate the organization's compliance with the appropriate Stage Meaningful Use initiatives. If you attest to compliance, then who completed your Core-15 requirement, the Security Risk Analysis (SRA), and does the SRA need to be improved or updated? Investigate and review any findings related to data encryption. Be sure your service provider will review your SRA and provide any recommendations.

Infrastructure refresh

Migrating what makes sense to the cloud requires conducting full reviews of the status of the overall infrastructure, including how many total servers are being operated on-premise, and which servers or other hardware are slated for sun-setting in the near term. Determine which legacy software and hardware are being managed today, and what challenges they represent. What other hardware or other capital expenditure (CAPEX) costs, such as security cameras, are planned for the near term, and what budgets are allocated for these purposes?

A desktop overview should be conducted alongside the server assessment. Determine the number of desktops and their operating systems by percentage. The service provider should also evaluate your bringing your own device (BYOD) initiatives and policies.

Virtualization

It is also helpful to level-set when it comes to virtualization. If portions of the infrastructure (desktops or servers) are virtualized, how are they virtualized, and using which technologies?

Data center overview

At the heart of most healthcare IT operations is the data center and its capacity and uptime. A consultant and IT partner should provide a comprehensive overview, including a capacity plan. Outline key concerns such as outages, as well as plans for expansion, re-building, or creating an off-site backup and DR facility to reduce the risk of compromising patient data.

A service provider should be able to assess capabilities and risks in current primary and secondary data centers, and determine whether or not upgrades are needed for location, power, AC, networking, generators, and so on. If pending improvements are required, then determine estimated costs.

Data security and growth

Select a partner that will provide a comprehensive report that will cover the state of existing data storage, back-up, and DR efforts, including how the data is stored, how is it moved, how is it used and most importantly, how secure it is. The partner should deliver recommendations and a migration roadmap for moving data to a secure, HIPAA-compliant infrastructure. Service providers also should provide recommendations for improving security of existing and future personal health information (PHI).

The service provider should inquire how much storage you currently manage, who are your primary storage architectures and vendors, and whether or not any plans exist for having a Vendor Neutral Archive (VNA). They also should determine whether or not you are growing your imaging service lines or modalities.

Many times, the answers to these questions will involve moving at least some data to the cloud. Although many IT leaders in healthcare believe that the cloud is less secure, it actually offers security advantages due to advanced encryption services and sophisticated network monitoring. Additionally, since the data is securely replicated across multiple data centers there is significant protection from loss due to hardware failure, power loss, natural disasters or other events.

Many healthcare organizations do not possess high levels of data encryption or protection expertise, which is understandable because it is not their core competency. On the other hand, the industry's top cloud service providers specialize in security and risk management. Service providers for healthcare should encrypt any data stored within the cloud with the most recent technologies. Data at rest should be protected through techniques such as full disk encryption, volume and virtual disk encryption, or file/folder encryption. The Department of Health and Human Services

(HHS) requires that HIPAA covered entities use storage encryption technologies as part of their storage security controls for data at rest.4 Because service providers specialize in encryption, they are well versed in data protection strategies
and technologies.

Moving data to the cloud is becoming a crucial necessity for several reasons, not the least of which is growth due to EMR and PACS systems. Boston-based Beth Israel Deaconess Medical Center recently moved to cloud data storage, due in large part to their volume of medical records, according to CIO of the Beth Israel Deaconess Care Organization
Bill Gillis.5

Determining Financial and Economic Impact

No phased migration to the cloud would be complete without a complete financial checklist, including detailed recommendations on ways to reduce IT costs, including but not limited to CAPEX, staffing, hardware, and data center space and power requirements.

Skilled service providers specializing in the medical vertical can also help pinpoint opportunities to improve government reimbursements, including but not limited to:

- Meaningful Use
- Cost Report Optimization
- Grants
- Local Foundations
- ICD-10 Readiness Assessment
- Gap analysis of current state versus completion
- Roadmap and recommendations for completing the ICD-10 transition in the most cost efficient way.

To complete this assessment, the partner should uncover key strategic business and IT goals for the next three years to reduce

costs, accelerate business and clinical strategies, and more. Obtaining executive involvement and supporting their top initiatives is vital.

Equally important is to obtain an idea of the balance sheet – where is money coming from? What is the facility's gross revenue, and is it profitable? Determine average daily bed census, how many clinics feed into the hospital, competition, staffing and affiliated physicians, donations, and other variables. Consider what changes may be anticipated under the Affordable Care Act. Also determine the impact of Meaningful Use dollars – did they affect profits or losses last year? What is anticipated for this year? Will your institution be attesting to Stage 1 or Stage 2 Meaningful use this year? If so, what costs will this involve?

Conclusion

Few industries face more challenges today than healthcare. So much rapid-fire change is occurring as healthcare organizations of all sizes acclimate to new security, reporting, compliance, and technology requirements. The first step is to enlist a trusted partner with several key differentiators. They should have an exclusive healthcare focus, be HIPAA compliance experts and best-in-class cloud and hosting experts, and provide 24/7/365 live support. Only with this level of healthcare-specific experience and expertise can healthcare

organizations be guided wisely and move forward with confidence. Through sufficient planning and experienced processes and procedures, healthcare organizations can attain their desired outcomes and advance their IT infrastructures with confidence to cut costs, support on-demand provisioning and more diversified infrastructures, and obtain higher levels of flexibility and data security.

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