OPTIMIZING THE JOURNEY TO THE HEALTHCARE CLOUD

Cost, scalability, and flexibility are reasons for Healthcare organizations to move applications to the cloud

EMC PERSPECTIVE

EMC²

BACKGROUND

In general, cloud adoption has been embraced due to the compelling business benefits that can be achieved. Cloud technology has matured rapidly, public cloud offerings have proliferated, and private cloud has proven to be a robust and secure platform for all kinds of business applications. It's no longer a question of whether to use the cloud, but how to use the cloud to optimize the cost-effective business performance of information systems and technology.

However, is the Healthcare sector embracing cloud technology as readily as other industries? Cloud computing certainly has the potential for enormous benefits for Healthcare as well. These benefits may include improved patient care and new care delivery models that will make Healthcare more effective and efficient. Cloud can also be used to share information securely and seamlessly across devices inside the hospital in a cost-effective way. Specifically for Healthcare, clouds must provide high availability and high security, they must be scalable, and they also must ensure compliance with existing and emerging global compliance standards such as HIPAA, HITECH, and EU Data Directives. Clouds can enhance collaboration even for smaller providers who may not have the ability to build and maintain their own infrastructure or to thoroughly mine patient and claims data to improve clinical efficiencies. Clouds allow a shared pool of computing and storage resources that can also be available to participating hospitals, practices, clinics, and labs on a pay-as-you-go basis.

As a way to begin moving to the cloud, a Healthcare organization has to decide where each application, or set of related applications, belongs. The choices today are: in the public cloud, in a private cloud, in a hybrid cloud, or even in the Healthcare organization's legacy computing environment. Where can each of these "workloads" offer the best combination of performance, cost, and flexibility? This perspective will serve as a guide to making such decisions by assessing representative workloads through three filters: economic, trust, and functional, thus helping Healthcare organizations accelerate their journey to optimizing services in the cloud.

INTO THE CLOUD

A recent CIO Market Pulse survey by IDG found that nearly three-fourths of IT organizations are running business applications in cloud computing environments now or are planning to do so in the next 12 months.(i) In a McKinsey survey, nearly half of the responding companies are already running collaboration applications in the cloud, over a third are running customer relationship management, over a third are running finance or human resource systems, and a fifth are running supply chain or resource planning systems.(ii) In the Healthcare arena, Nearly one-third of decision makers said they are using cloud applications, and 73 percent said they are planning to move more applications to the cloud, according to a recent report by Accenture.(iii) "There are several key reasons why Healthcare IT leaders are moving applications into the cloud," says Dadong Wan, a senior research scientist at Accenture studying digital health trends and a co-author of the recent Accenture report examining cloud computing in Healthcare. "Some of those reasons are cost advantages and flexibility that cloud computing offers Healthcare organizations."

Business leaders, not just in Healthcare, appreciate the benefits of the cloud. In the McKinsey survey of both business and technology executives, 75 percent believe that cloud computing could drive value in their companies (another 16 percent aren't sure yet). Increased business flexibility, improved systems scalability to meet business needs, lower unit cost for IT, and better business continuity are all stated as compelling reasons to move to the cloud. (iv) As motivating as the direct economic benefits of the cloud seem, these executives recognize that cloud computing is very much a business performance proposition.

Some Healthcare organizations are still understandably hesitant to move their sensitive patient-centric information and mission-critical applications to the more open, more networked, and less familiar environment of cloud computing. Security, reliability, and regulatory compliance remain the most common concerns about the cloud; however, those concerns apply primarily to public cloud services, and many of the risks are overstated.

Currently Healthcare organizations are distinguishing between the public cloud, where the enterprise cannot maintain full control over its information assets, and a private cloud, where it can. A recent Gartner survey found that 76 percent of IT organizations will be pursuing a private cloud strategy by 2012 (and another 20 percent said maybe they will). When asked for a planned investment breakdown, 75 percent said they will spend more on private cloud than public, while only eight percent plan the reverse.(v)

CLOUD TYPES

Public Cloud

- Resources are owned and managed by the cloud provider and shared across customers. Scale economies can be high and costs low, but for the customer organization both transparency and control can be low. A variation is the community cloud, a multi-company, members-only version of a public cloud, usually centered on a common business process (e.g., for use by a purchasing consortium).

Private Cloud

- Resources are owned and managed by the Healthcare organization and shared across it. The organization has scale economies and cost advantages (though not on a par with the public cloud) together with more transparency and control. Private cloud resources are usually on premise; however, an external private cloud can be operated by an outside service and still offer high transparency and control, including control over asset location and segregation.

Hybrid Cloud

- Hybrid cloud is a combination of public and private clouds. Today, most applications run in one cloud or the other. In more complex configurations, selected data moves back and forth, for example, when a public cloud customer relationship management application shares data with financial applications in a private cloud. Sometimes a public cloud part of the hybrid serves as an on-demand extension of computing and storage infrastructure to handle peak loads or transaction volumes.

The most flexible and cost-effective computing environment today incorporates a federation of public and private clouds, with appropriate applications running in the public cloud, most mission-critical applications and those handling sensitive information running in a private cloud, and some applications crossing over and utilizing both public and private cloud services.

BUSINESS BENEFITS OF THE CLOUD

The potential economic benefits of cloud computing for Healthcare are as follows:

- With a private cloud platform, a Healthcare organization utilizes its technology more efficiently and reduces the footprint and cost (including energy cost) of its physical infrastructure. Traditional data center costs can decline significantly.
- Commodity services like email and collaborative workspaces can be provisioned at lower cost due to the scale economies of the public cloud. With Software-as-a-Service, the cost of using and maintaining business applications can be reduced. With pay-by-usage, the ongoing cost of applications and other services can decline and align with real business need.
- By optimizing the distribution and management of workloads across public, private, and hybrid clouds, a Healthcare organization can lower its total infrastructure and personnel IT spend by 25-30 percent.

As attractive as these direct cost and cost structure reductions may be to a Healthcare organization, the greatest payback of cloud computing may come from two other types of business benefits:

- Productivity—Clinicians have on-demand access to more information and the tools to use it. They can more readily collaborate and share information, expertise, and other resources. The IT staff spends much less effort on the operations and management of everyday information systems and can focus more on technology-enabled care improvement.
- Agility—With on-demand access to modular information assets, clinicians can fashion new care delivery capabilities and utilize them quickly. They can then scale those capabilities up and integrate them into operations with minimal disruption. They also can access, experiment with, and deploy new cloud-based applications and services in record time.

The cloud enables better patient care on multiple fronts simultaneously: cost, manageability, information access, new capability deployment, coordination and collaboration, business continuity and security, care innovation, and growth. It's the way for Healthcare organizations to get the best mix of capabilities, performance, and cost from their Health IT ecosystems.

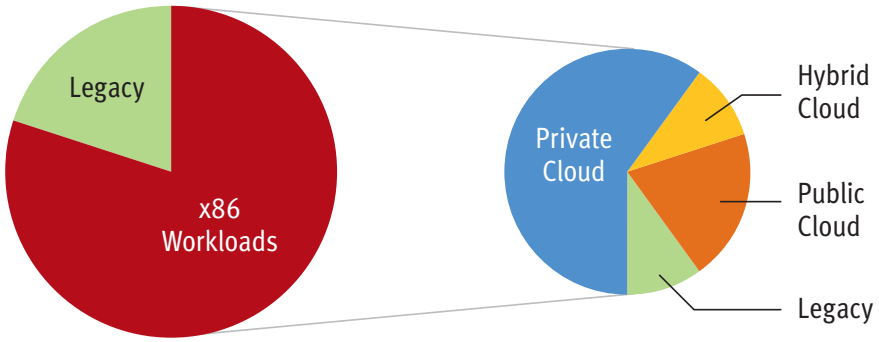

Figure 1. An optimized cloud environment yields 25-30 percent savings in total IT spend

WORKLOAD ANALYSIS USING THE THREE FILTERS

Healthcare organizations should specifically evaluate what applications and information are appropriate for cloud computing, and what type of cloud is the best destination for each. This involves looking at each asset and its potential migration to the cloud through three filters—economic, trust, and functional.

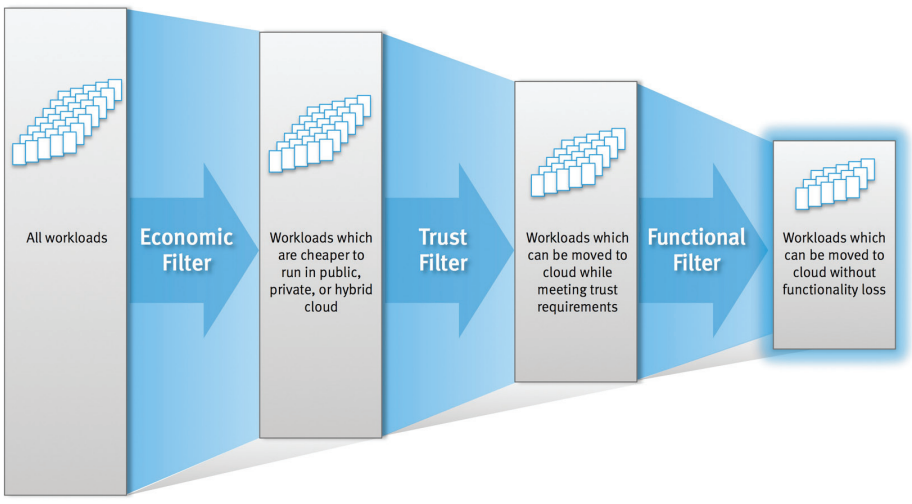

Figure 2. Application of the three filters to Healthcare organizations' workloads

INITIAL WORKLOAD AND INFORMATION FLOW ANALYSIS

A workload is a specific asset, often corresponding to a business or clinical application or set of related applications together with the information they use. A workload can also be a service like email or collaboration workspaces, or a shared resource like a data warehouse.

Start by identifying the workloads that are candidates for movement to the cloud. Well-defined and modular workloads with few interfaces may be good candidates; difficult-to-reconfigure legacy systems would not. Analyze the data and applications associated with the workload. What are their business importance and value? Who uses them and how? What workflows are used in making what business decisions? Very importantly, where does the information originate and flow, both inside and outside of the Healthcare organization? How important and/or sensitive is that information? The purpose of this initial analysis is to develop a working inventory of cloud-candidate workloads and understand them in sufficient detail to apply the three filters.

ECONOMIC FILTER

Assess the economic impact of moving each specific workload to the cloud. Look at its scale and transaction volume, including the number of users and the consumption of processing and storage resources. Determine if these are large enough to make a difference in terms of everyday operating cost. The key to this economic analysis is deriving a reasonably accurate "all in" cost that includes the costs of both moving to the cloud and operating there. How much effort will be needed to retrofit the workload and its interfaces? How will the consumption of bandwidth and network management resources increase, including for backup and recovery, if the destination cloud is remote? How much will be saved in each of the basic IT cost categories after the workload moves to the cloud? What's the bottom line for each individual workload?

TRUST FILTER

Before applying the trust filter, you should understand the characteristics and requirements of a trustworthy computing environment (see sidebar). You should understand the different trust profiles of the potential destinations for workloads—public, private, and hybrid clouds, and the in-house legacy environment. In particular, recognize how a private cloud presents the opportunity to improve the trustworthiness of the computing environment through greater transparency, more granular controls, improved reliability and business continuity, and more precise and complete protection of sensitive patient-centric information.

ANATOMY OF TRUST

A secure, compliant, and trustworthy computing environment, whether cloud-based or not, should meet six requirements:

These six requirements are not mutually exclusive. Protecting personally identifiable information, for example, is a privacy matter, a legal requirement, and a potential source of risk and exposure. However, you learn different things by looking through the lenses of each of these six requirements.

Compliance	The organization can meet specific legal requirements governing the management of information, and can comply with industry standards and rules (e.g., GAAP, ISO) and meet service-level agreements.
Governance	The organization can monitor the computing environment; enforce management policies, procedures, and controls; and establish the responsibilities, accountabilities, and decision rights of the people using and managing information technology resources.
Risk Management	The risks associated with a computing environment range from direct threats (e.g., intrusion and hacking) to business interruption (e.g., when systems are unavailable) to derived exposures (e.g., the financial, reputational, and legal repercussions of information loss or theft).
Availability	This includes both everyday access to computing resources and the quick and complete recovery of resources following any kind of interruption or failure.
Integrity	To maintain the integrity of information and other assets, access must be secure so only authorized people and systems can use specified information and applications. In addition, the transactions processed (think of a funds transfer) must be certifiably complete, even though there may be many potential points of network or system failure.
Confidentiality/ Privacy	This includes protecting the confidentiality of personal data as required by law; protecting commercial data such as financials, trade secrets, and other intellectual property; and meeting the expectations of customers, employees, and others regarding how information about them is obtained and used.

Start with any specific regulatory requirements (i.e. EU Data Directives), standards (i.e. DICOM), and any other rules governing the workload—the "compliance" category of trust. Then evaluate the workload's requirements in terms of the other five categories: governance, risk management, availability, integrity, and confidentiality/privacy. What conditions and standards must be met? How well does the current computing environment meet them? Which among the cloud deployment options can meet them adequately, or perhaps better than the current environment can? Take note of needed improvements independent of planned migration to the cloud.

Workloads with lower trust requirements naturally have more flexible cloud deployment options. Some workloads will be quickly disqualified from the public cloud on compliance and governance, if not other grounds. With a private cloud, it's much less of an all-or-nothing proposition. You need to ask: what exposures are reduced by migration to the cloud? What exposures are increased? What risk mitigation tactics might enable the workload to run trustfully in a private cloud? How can we leverage migration to a private cloud to improve the trust profile of the workload?

FUNCTIONAL FILTER

Can the workload operate in the cloud at least as well as it does today? Will it lose functionality because of restrictions on interfaces with other less cloud-compatible applications or because of restrictions on information availability and movement? Can its basic performance characteristics, such as response time, be maintained? Will access by authorized users outside the company, especially customers, be complicated (or facilitated) by movement to the cloud?

Basic content and applications code should be unaffected by movement of a workload to the cloud, but other things can change, especially around access and interfaces. So anticipate the workload's entire performance context. Will functionality be reduced or lost? Also remember to consider ways in which functionality, performance, and flexibility can be enhanced by movement to the cloud.

MAPPING WORKLOADS TO CLOUD OPTIONS

As the three filters are applied, the field of candidates (especially for short-term cloud migration) narrows, and the preferred cloud deployment destination of each workload emerges. Combine the results from the three filters, and then make adjustments based on their interplay. For example, "all in" cost may change if there is added expense to maintain the workload's functionality or to adjust its trust profile through security enhancements. Keep in mind that marginal economic payback may not be a disqualifier for a workload that belongs in the cloud for business performance and agility reasons.

In general, you'll find that widely used but non-differentiated workloads, where less than 100 percent availability is acceptable, fit the public cloud (for example, email and collaboration spaces). Most core clinical applications belong in a private cloud, especially those that are tailored and are closely integrated with other applications or must perform to mission-critical service-level agreements. Market-facing workloads such as e-commerce applications may need a hybrid cloud for rapid scaling to meet peak demand. Highly specialized and fine-tuned workloads such as operational control systems typically belong in the legacy environment. However, this is all painting with a very broad brush. There are many variations, and a Healthcare organization must evaluate its workloads in detail.

After assessing workloads individually, assemble the composite picture. What will the new distribution of workloads across platforms look like? How will key information have to flow across workloads and platforms? How will the interfaces work? What will be the overall impacts be in terms of economics, trust, and functionality?

ROADMAP TO THE CLOUD

This process culminates in a readiness assessment and roadmap for putting the new pieces in place—from technology and automation, to process changes and staff training, to the migration of specific workloads to their cloud destinations—all under the guidance of a clear governance structure. A roadmap establishes scope, objectives, and measures. It details implementation actions, sequences, dependencies, milestones, alternatives, and triggers for alternative action. It also details the means of tracking progress and performance, as well as capturing what's learned along the way.

Cloud adoption is a journey, not a one-time implementation. The consolidation and virtualization of technology, and the re-automation of its management, will happen early in the journey and yield immediate financial benefits. However, workloads will migrate to private, public, and hybrid clouds over time as both the workloads and their cloud destinations are ready. People will learn to work, collaborate, and use information and applications in new ways. Business performance and agility benefits, as well as economic gains, will accumulate and amplify.

IMPLICATIONS FOR IT MANAGEMENT

Cloud computing represents a different and more productive way for Healthcare technology services to be provided, consumed, and managed. Technology assets are defined and packaged differently—modular, inter-connectable, and virtualized. IT's work is structured and provisioned differently—as a catalog of business services. Clinicians access and consume services differently—frequently through a self-service portal, and they often pay by actual usage. IT and the business together can manage the technology environment and its services differently with greater transparency into business performance and value.

For IT, cloud computing also offers the opportunity to reduce complexity, raise efficiency, and finally break the pattern of devoting 70 percent or more of its budget and energy to maintaining resources and "keeping the lights on."

To realize these benefits—to really enter the cloud—requires specific changes in how IT works. These changes may include virtualizing assets, automating operations, organizing around services, and enabling self-service. Recent Forrester research found that most IT organizations' ambitions around private cloud exceed their readiness and operational capa-

bility. Most are not investing enough effort in automating their virtual environments, deploying self-service portals, or implementing the resource tracking and cost allocation systems needed to support self-service and pay-by-use. For companies short on these necessary capabilities, an externally hosted private cloud may be the fastest and most effective way to get started.(vi)

Research by IDG for the Leadership Council for Information Advantage explored perhaps the biggest gap in IT capability—lack of information governance policies for cloud computing. Existing policies can be leveraged for a private cloud environment, where information and applications remain under the direct control of the enterprise. However, public and hybrid clouds need new approaches. Only one-third of companies surveyed have specific governance policies for cloud-based information (though another 38 percent said they are planning to develop them).(vii)

Without such policies, a Healthcare organization may find itself with a proliferation of incompatible public cloud platforms and services, new forms of fragmentation and isolation of information assets, and lack of control over the chains of custody for information and its security. Without policies that span cloud platforms and the computing environment as a whole, complexity grows and benefits are diluted.(viii)

Wherever the capability gaps may be—technology architecture, infrastructure automation, information management, service orientation, cloud platform federation, or IT governance, policy, and management—IT can accelerate the journey to the cloud and its business benefits by partnering with experts.

CONCLUSION

The Healthcare industry and technology providers are working to ensure that cloud computing offerings are secure and meet the regulations of the HITECH Act in the way data is stored and accessed in the cloud. As those assurances emerge, we expect that over the next three to five years, we'll see more providers embracing the benefits of cloud computing. We also expect to see increased adoption and a mixture of private and public cloud deployments in Healthcare facilities, with some larger Healthcare organizations even experimenting with the cloud to create and sell custom applications. The possibilities for the cloud are many for Healthcare organizations.

The steps outlined in this perspective are a cloud-focused extension of what Healthcare organizations should already be doing. Review important information and technology assets, determine whether they are doing the best job they can for patient care, and evaluate how the Health IT ecosystem amplifies or inhibits evidence-based medicine. Then plan the next-generation computing environment, move steadily toward it, and realize benefits along the way.

If your organization hasn't made this assessment lately, then let the business and patient care opportunities of cloud computing be your reason to do it now. Use the economic and performance benefits of the cloud as the driver to take a fresh look at your IT assets, raise their value, and enhance the economics, performance, and trustworthiness of your Healthcare organization's computing environment. Optimize your use of the cloud.

CONTACT US

To learn about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at www.EMC.com.

i "In the Race to the Cloud, Do Your Organization's Governance Policies Stack Up?" 2010, page 1

ii "McKinsey Global Survey Results: How IT is managing new demands," 2010, page 8

iii "Healthcare Taking Computing to the Cloud" Marianne Kolbasuk McGee, Information Week, June 21, 2010

iv "McKinsey Global Survey Results: How IT is managing new demands," page 7

v "Private Cloud Computing Plans From Conference Polls," Thomas J. Bittman, 30 April 2010, pages 3-4

vi "Companies Building Private Clouds Focus On Infrastructure But Not Operations," James Staten, November 23, 2010, pages 7-8

vii "In the Race to the Cloud, Do Your Organization's Governance Policies Stack Up?" 2010, page 1

viii "Creating Information Advantage in a Cloudy World," October 2010, pages 4, 8-9

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.EMC.com

EMC²