BUSINESS WHITE PAPER

Best Practices in Cloud Computing for the Healthcare Industry
Best practices in Healthcare IT disaster Recovery planning

Today, healthcare organizations face an array of challenges: the need to comply with HIPAA, the HITECH Act for “meaningful use” of information, recovery audit tracker (RAC) audits, and IDC-10 disease classification mandates. They also must improve care outcomes while protecting patient health information (PHI).

The need to protect data is more urgent than ever, because risks are mounting. Criminal attacks on hospitals are on a huge upward trend, with a frightening 100 percent reported increase just from four years ago, according to a new Ponemon Institute study. HIPAA privacy and security breaches are also on the rise. The number of patient health records compromised in a HIPAA data breach since 2009 has risen to 29.3 million, a 138 percent jump just from 2012.

Adding to the challenges, healthcare organizations must serve an increasing number of patients due to an aging U.S. population, ensure consistent quality between rural and urban providers, be accountable for outcomes, provide accurate measures of success, and accomplish all of these outcomes at lower costs.

Because healthcare is so reliant on technology, one pressing need is to improve performance and reliability of information technology (IT) systems, because accurate and up-to-date information is essential to continuous quality improvement – particularly in an area as complex as healthcare. At the same time as cost reduction and IT improvements are a clear priority, many healthcare organizations possess information systems that are aging and lack integration, hampering rather than enhancing capabilities and efficiencies.
The need for integration is becoming more important than ever because several healthcare organizations are consolidating with other healthcare networks with differing IT systems. Disparate systems must be brought together to share information and work together in an orchestrated fashion to coordinate efforts. When merging with other organizations, institutions need to combine hospital practices with ease and quickly integrate and scale IT systems to accommodate growth and improve agility. These pressures are leading healthcare organizations to strategically review and revamp their IT strategies and infrastructures.

How can the cloud and a hosting provider assist your organization?

All of these factors are motivating healthcare providers to consider cloud computing as a solution to help them swiftly integrate with other practices, cut costs, maintain quality, meet regulations, safeguard patient information, and increase productivity. Healthcare has many unique requirements when it comes to technology, which is why adopting purpose-built, cloud-based solutions is becoming an ever-more attractive alternative to support a diversified infrastructure, access resources on-demand, speed provisioning, and ensure in-house data security.

Among the most common use cases for cloud computing are: electronic medical records (EMRs), radiology information systems (RISs) and picture archiving communication systems (PACs), backup and disaster recovery, virtualized desktops, and consumer and patient portals that streamline communications with external and internal parties. Also topping the list are integrated population health and clinical information, care collaboration tools, and “big data” environments used for analytics, data warehousing, and health information exchanges (HIEs) that help organizations share updated, electronic patient information with other providers across the continuum of care.

“Anywhere universal access” to documents and applications is another important factor in moving to cloud computing. This is particularly useful for healthcare providers for accessing electronic medical records, test results, and other important info — whether in the office, at the hospital, or at home.
The cloud: easier HIPAA/HITECH compliance

With stronger government enforcement of HIPAA rules and the ever-present risk of a data breach, providers must ensure that their systems and practices are secure and compliant. Many IT healthcare professionals worry that the cloud is not as secure as on-site IT resources, and want to avoid the risk of data loss or data breaches. However, cloud technology and security techniques have advanced to the point where the cloud is even more secure against data breaches and losses.

First off, in the cloud applications and data in the cloud do not reside on standalone, on-site servers or devices. This helps prevent data loss and safeguard patient information. The cloud service provider should disclose its data center infrastructures, technologies used, expertise, and locations, and jointly shoulder the responsibility for protecting against data loss and security breaches.

Second, security in the cloud is easier to enforce. Healthcare IT should be free to focus on the task at hand – providing information systems to improve patient care. On the other hand, the industry’s top cloud service providers that will stand out should 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.

Data in motion is another vital consideration when considering moving to the cloud. An important piece of valid encryption processes for data in motion is Transport Layer Security (TLS), a protocol meant to ensure there are mechanisms in place to protect and provide authentication, confidentiality, and integrity of sensitive data during electronic communication. The Department of Health and Human Services (HHS) defers to NIST Special Publication 800-52 Revision 1, released in September 2013, for data in motion encryption best practices.

---

5 http://healthitsecurity.com/2014/03/06/healthcare-cloud-security-resources-advice-for-providers/
Cloud service providers can also add value by establishing multi-tier authentication. This best practice adds an extra layer of protection on top of the traditional username and password to help save healthcare entities from data breaches.

**Considering the costs: the advantages of OPEX vs. CAPEX**

Shifting cost structures are an additional benefit of moving to the cloud. Many healthcare institutions prefer to move their IT infrastructures from being a capital expenditure (CAPEX) toward an operating expenditure (OPEX) model. Building an internal data center requires initial capital expenditure and ongoing equipment refreshing, while using an external cloud service that offers pay-as-you-go service falls into the category of an ongoing operating expenditure.

If healthcare organizations decide to maintain an internal data center and go the CAPEX route, there are the direct costs that accompany running a server: power, floor space, storage, and IT operations to manage those resources. These fixed capital expenditures, from an accounting standpoint, must be amortized over time. There are also indirect costs of running a server, including the network and storage infrastructure and IT operations to manage the general infrastructure.

Other factors include the overhead costs of owning a server: procurement and accounting personnel, not to mention a critical resource in short supply: IT management and its attention. Oftentimes, cost comparisons ignore the utilization of the internal server: if it’s running at 20% utilization, the effective cost of a given level of computing is actually five times higher than typically assumed in cost comparisons.

OPEX, on the other hand, offers several benefits. Because the IT infrastructure is “rented” through the cloud, resources can be scaled up or down as needed. As growth or acquisitions occur, a service provider can scale resources – servers, storage, networking, and hosted software – on an as-needed basis through an OPEX model. Or, if budgets change, a cloud service provider can deliver tremendous flexibility in terms of the technical environment. They can juggle technical resources in their infrastructure to mesh with business requirements for increased performance, security, storage space, cost requirements, and so on.
By contrast, payment on a capital good such as a server is one of a series—each of which the enterprise is committed to, no matter if the server is being used or not. With a cloud-based, OPEX model, organizations are committed to using the IT resources only as long as they are needed. Once the use is paid for, there is no further financial obligation.

**Moving to the cloud: how, what, when?**

Migrating to the cloud can feel daunting and risky, but many healthcare organizations are reaping the benefits of making the shift and realizing positive effects, both from business, security, cost, and technology standpoints. The first best step is to conduct a health-check on the existing environment. Determine where the IT organization is today, prioritize the most important areas for improvement; and then identify any existing and near-term issues.

A service provider should provide a comprehensive analysis and report that provides insights and recommendations on infrastructure, data, and financial considerations. This process should include a review of all business applications (EMR, 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 can not be currently migrated due to technology or business constraints

Next, expect a migration road map for all near-term and long-term applications than can be moved into the cloud, as well as list of recommended technology and/or applications that the organization is not currently using but could deploy into the cloud and the reasoning and business benefits of adoption.

Also required is a review of existing technology deficiencies and recommendations for implementing improvements. (e.g. leveraging a virtual desktop infrastructure as an easy, cost-effective solution for hospitals still using Windows XP versus upgrading to a new operating system). Finally evaluate resources, including staffing and budget to provide recommendations for improving efficiencies within current constraints.

---

A recent report by CDW of 1,242 IT professionals found that more than half of organizations are moving a variety of capabilities to the cloud. And a majority of them are recognizing cost savings and increased profits, according to another study by a leading hosting company.  

---

Once the IT “reality check” is accomplished regarding the IT infrastructure, the next step is to identify and prioritize areas for improvement. Set goals and create a list of what needs to occur first. Find out where your organization needs to be in the next few months and establish a solid foundation for future next steps.

The end result should be a migration plan to help your organization move forward. The plan should include an extensive review of existing systems, identification of which IT functions can, could, or should be moved into the cloud. Integral to the migration plan should be an identification of the benefits, and prioritization and sequencing of moving to the cloud.

**Careful analysis and planning is essential**

At this point, it is also important to conduct an impact analysis. This process will enable organizations to discover how a new cloud-based solution would affect both the business and IT. For healthcare, consideration includes both standard cloud-based computing benefits such as reduced costs and pay-as-you-go capabilities, but also the need to meet patient information security, HIPAA, and other regulatory requirements.

After careful analysis and planning, your organization should know the drivers for change, which assets are functioning well, and where the gaps are. The next step is to determine solution requirements. Oftentimes, healthcare providers simply respond based on vendor features and functions, but this can lead to mismatched goals and capabilities. After identifying drivers and existing conditions, it is crucial to identify specific requirements and use them to evaluate solutions.

First start by considering your most vital business requirements. What problems are you trying to solve? You may have just acquired another health network with very different IT systems and need to integrate it so that everyone can securely collaborate, communicate, and share information. Or, cost reduction may be a primary concern, and investing hundreds of thousands in a new data center that must be amortized over time may not make sense.

Technology requirements are another vital consideration. What are the required specifications? Perhaps you have a shortage of storage capacity
that is inhibiting you from implementing an HIE or business intelligence solution. Or, maybe you are unable to meet backup windows to ensure security and safety of patient information.

These business and technology requirements should then drive creation of an in-depth list of requirements to help guide your transition or partial transition into the cloud. In addition to the business and technical requirements, it goes without saying that it is crucial to look at the financial viability, references, and stability of each vendor.

Here are some of the most important criteria to consider when selecting a hosting provider:

• **Locations:**
  Where will data need to be hosted, and how far away should it be? Should data be replicated to another data center facility? Will they be located in different disaster zones? How far away should it be from the primary site?

• **Virtualization needs:**
  Ensure that physical servers and a Storage Area Network (SAN) will be provided for any virtual server environment. Verify that data is not accessible to any other organization and that security measures are taken to protect this environment from vulnerabilities. Data must be protected in accordance with HIPAA regulations.

  Inquire about the availability of a “single pane of glass” management console to connect and manage virtual servers. Be sure that the virtual environment offers high availability features so that no business disruption occurs so that virtual servers will continue to operate in the event of a physical server hardware failure. Be sure of the ability to procure a new virtual server on demand, and ask for load balancing across physical servers to maximize performance.

• **Make a checklist of facility requirements. Among them, be certain:**
  Find a Tier III data center that is SOC II and III and SAEE 16-certified, as well as HIPAA and PCI compliant. These certifications provide proof that the service provider has documented security processes that are followed strictly and completely auditable. Ask about service-level agreements (SLAs) and uptime records for platform,
network, and storage availability. Find SLAs that speak to the main components of availability: security, network, cloud platform, and storage. An SLA needs to be a guarantee, as well as something that can be reported on.

- **Dive deeply into service capabilities:**
  Healthcare organizations have to work around the clock, and so does the hosting provider. Ask for 24/7/365 service capabilities and ensure that your service provider can meet your response times.

- **Storage needs:**
  The SAN should be available 100% of the time, excluding scheduled maintenance. In the event of any hardware failure, the hosting provider should have a technician with appropriate parts available on site within six hours, or the service provider should credit your organization for a portion of the cost of your downtime.

- **Data backup and restore:**
  Understand the backup process, frequency, and retention periods. Do they work with your controls? How flexible are they? Understand how backups are validated. Instead of relying solely on test restores, request continual reports of successes and/or failures and gain to a log of success versus failed backup jobs to drive best practices.

- **Pay attention to monitoring and response:**
  All servers should be monitored by at least six ports, and gaged on key performance metrics.

- **Select a service provider that can support multiple models:**
  Most cloud service providers should be able to provide several options:
  - A private cloud, the most expensive option, is one in which the services and infrastructure are maintained on a private network. These clouds offer a high level of security and control, but they require the company to purchase and maintain all the software and infrastructure, which leads to somewhat higher expenses.
  - A public cloud shares space with other organizations. Note that this is the most cost-effective alternative, but public clouds are often not the most appropriate option for healthcare organizations due to security concerns.
  - A hybrid cloud includes a variety of public and private options with multiple providers. By spreading things out over a hybrid cloud,
each aspect of the business can be kept in the most efficient environment possible. The downside is that IT managers have to keep track of multiple different security platforms and ensure that all aspects of the business can communicate. Hybrid clouds are often good choices when healthcare organizations want to set up a virtual private network (VPN) behind their firewall. Or, perhaps a medical institution wants to use a public cloud to interact with patients but keep their data secured within a private cloud.

- A multi-tenant private cloud is a good option for healthcare institutions because it balances reasonable costs with high security. A multi-tenancy architecture can take advantage of virtualization and remote access. A software as-a-service (SaaS) provider, for example, can run one instance of its application on one instance of a database and provide web access to multiple customers. In such a scenario, each tenant’s data is isolated and remains invisible to and secure from other tenants.

**Be sure to choose a provider that will:**

- Sign a HIPAA Business Associate Agreement and be HIPAA compliance experts
- Support a SOC2, SSAE16 and HIPAA-compliant
- Provide set response times, depending on the risk to your organization (emergency, urgent, standard, and so on)
- Provide extensive healthcare cloud computing managed services
- Deliver 24x7x365 live healthcare-level support
- Offer industry-leading healthcare-specific products
- Exhibit exceptional data center, cloud hosting, and cloud managed services
- Be flexible and provision additional services as necessary, such as initial cloud services setup and provisioning and additional Internet bandwidth
- Be exclusively focused on the healthcare industry. Healthcare IT is a complex and regulated environment with its own language and high criticality uptime, redundancy, and security requirements.
Rely on solid implementation processes

Once your organization has established its business and technology requirements and singled out a cloud service provider, the final step is to make a smooth transition.

Fundamental requirements include:

- Strong project management
- A firm schedule
- Ongoing testing and reporting
- Performance monitoring
- Change management and training
- A roll-back plan if key processes need to revert temporarily to the old infrastructure
- A solid schedule of deliverables and assigned responsibilities
- An easy way to track progress and issues

Select a service provider that follows Information Technology Infrastructure Library (ITIL) best practices for change management to ensure that the move to the cloud is accomplished at a low risk and is executed with minimal impact. Service providers need to develop and deliver IT-based services under the umbrella of solid process implementation, with operational rigor and control. Every process should be both auditable and repeatable, and the service provider should meet stringent service-level agreements (SLAs) around implementation, support, and maintenance processes.

This includes establishing metrics around mean time to failure and mean time to repair, and insisting on transparent communications around the root causes and reasons for any outage. Ensure that everything is documented. All of this sounds very rigorous, and it is, but it is also important to find a service provider that is a true partner that goes above and beyond mere paper contracts and documented processes. The key is to find a provider that genuinely has your organization’s best interests at heart.
Conclusion

As healthcare organizations of all sizes adapt to new security, reporting, compliance, and technology requirements, many are finding great value in the cloud. While healthcare, understandably, is somewhat wary of adopting new technologies, they are a burgeoning part of the growing cloud movement. The industry overall is poised for strong growth through 2014, when worldwide cloud services revenue is projected to reach $148.8 billion.

Especially in the healthcare industry, cloud computing has become more important than ever, because the challenges inherent in managing technology based on the principles of previous eras – complex, custom, expensive solutions managed by large in-house IT teams – have become greater, and the benefits of cloud computing in addressing these challenges have matured to become more appropriate and business-critical to healthcare enterprises of all types and sizes.

Ready to identify ways that cloud computing can help your healthcare organization improve HIPAA compliance, reduce costs, and drive greater performance and reliability?

Call (888) 899-2066
Visit www.ClearDATA.com