Impact of Cloud Computing on Healthcare
Introduction
The aim of this guide is to provide a practical reference to help enterprise information technology (IT) and business decision makers of the healthcare industry as they analyze and consider the implications of cloud computing on their business. The paper includes guidance and strategies, designed to help these decision makers evaluate and compare cloud computing offerings in key areas from different cloud providers, taking into account different requirements from various actors including medical practices, hospitals, research facilities, insurance companies and governments.

When considering a move to use cloud computing, healthcare consumers must have a clear understanding of unique benefits and risks associated with cloud computing, and set realistic expectations with their cloud provider. Consideration must be given to the different models of service delivery: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) as each model brings different requirements and responsibilities. Cloud deployment models (private, public, and hybrid) will also weigh heavily in strategic decisions.

The “Current Market Dynamics” section highlights the current state of the cloud computing market for healthcare and how it is expected to evolve over the next several years. This section introduces the key factors expected to accelerate adoption of cloud computing in the healthcare industry along with an overview of the key barriers that must be addressed. This section also highlights the key considerations for service and deployment models.

The “Challenges to Leveraging Cloud Computing for Healthcare” section explains the critical barriers to cloud computing adoption for the healthcare industry with specific focus on the stringent security and privacy requirements that must be addressed including the impact of government and industry regulations.

The “Benefits of Cloud Computing for Healthcare” section discusses specific IT trends in the healthcare industry that are addressed most effectively, both technically and economically, by cloud computing as opposed to traditional IT environments.

The paper closes with a “Strategic Recommendations” section that provides healthcare consumers with specific guidance on how best to achieve the benefits of cloud computing while maintaining an acceptable level of risk. Although guidance is provided, each organization must perform its own analysis of its needs, and assess, select, engage, and oversee the cloud services that can best fulfill those needs.

Throughout the paper, the role that standards play to improve the flexibility, interoperability and portability of cloud computing environments is highlighted. The paper also identifies areas where future standardization could be effective.

Current Market Dynamics
Compared to other industries, the healthcare industry has significantly underutilized technology to improve operational efficiency. Most healthcare systems still rely on paper medical records. Information
that is digitized is typically not portable, inhibiting information sharing amongst the different healthcare actors. Use of technology to facilitate collaboration and to coordinate care between patients and physicians, and amongst the medical community is limited.

Around the globe, healthcare reform has mandated that it is time for healthcare information technology (HIT) to be modernized and cloud computing is at the center of this transformation. The healthcare industry is shifting toward an information-centric care delivery model, enabled in part by open standards that support cooperation, collaborative workflows and information sharing. Cloud computing provides an infrastructure that allows hospitals, medical practices, insurance companies, and research facilities to tap improved computing resources at lower initial capital outlays. Additionally, cloud environments will lower the barriers for innovation and modernization of HIT systems and applications. Cloud computing caters to the key technology requirements of the healthcare industry:

- Enables on-demand access to computing and large storage facilities which are not provided in traditional IT environments.
- Supports big data sets for electronic health records (EHR), radiology images and genomic data offloading, a burdensome task, from hospital IT departments.
- Facilitates the sharing of EHRs among authorized physicians and hospitals in various geographic areas, providing more timely access to life-saving information and reducing the need for duplicate testing.
- Improves the ability to analyze and track information (with the proper information governance) so that data on treatments, costs, performance, and effectiveness studies can be analyzed and acted upon.

Healthcare data has stringent requirements for security, confidentiality, availability to authorized users, traceability of access, reversibility of data, and long-term preservation. Hence, cloud vendors need to account for all these while conforming to government and industry regulations. Problems in making IT systems interoperable have delayed cloud computing growth in the health care industry.1

When considering a move to cloud computing, healthcare actors (medical practices, hospitals, research facilities, etc.) need to carefully consider the type of application moving to the cloud (clinical and nonclinical applications). Clinical applications consist of EHRs, physician order entry and software for imaging and pharmacy use. Nonclinical applications include revenue cycle management, automatic patient billing, cost accounting, payroll management, and claims management.

In many cases, the type of application moving to the cloud will dictate the cloud deployment model that’s utilized (private, public, and hybrid), addressing the specific security, privacy and availability requirements for that application. Initially, cloud deployments for clinical applications will take root in private or hybrid clouds given that these applications require the highest level of security, privacy and

availability. Nonclinical applications are a better fit for public deployments but still must be carefully assessed. For example, an appointment with the psychiatry department may imply potential mental issues and, as such, must be protected as sensitive data.

Healthcare actors must also consider the cloud service model (IaaS, PaaS, or SaaS) that best addresses their business requirements. In many cases, SaaS, with its pay-per-use business model will be the most attractive economic option, especially for small physician practices, since the need for full-time IT personnel is eliminated along with capital expenses associated with system hardware, operating systems and software. PaaS is a viable option for larger healthcare institutions that have the resources to develop their own cloud based solutions. For healthcare institutions seeking a more scalable infrastructure, IaaS offers a cost-effective turn-key solution that provides scalability with security, flexibility, defined service level agreements, built-in backup and data protection.

Though still in its early stages, there are clear signs around the world that cloud computing is emerging as a critical technology for the healthcare industry. A large and growing percentage of hospital executives are storing data, including clinical applications and email, in the cloud (Terry, 2012). An increasing number of health care providers are deploying or are planning to deploy cloud technology. A large percentage of IT decision makers currently have budget assigned to cloud computing and most expect to spend more on cloud in the next three years. While there’s still a ways to go, cloud computing may end up being one of the most important IT advances to impact the healthcare industry.

Challenges to Leveraging Cloud Computing for Healthcare

Healthcare organizations (HCOs) are expected to provide new and improved patient care capabilities while simultaneously limiting healthcare cost increases. Information Technology plays a strong role in the health and patient care arenas with cloud computing slowly beginning to make its mark. However, despite the significant advantages for the utilization of cloud computing as part of Healthcare IT (HIT), security and privacy, reliability, integration and data portability are some of the significant challenges and barriers to implementation that are responsible for its slow adoption.

Privacy and Security Challenges

Data maintained in a cloud may contain personal, private or confidential information such as healthcare related information that requires the proper safeguards to prevent disclosure, compromise or misuse. Globally, concerns related to data jurisdiction, security, privacy and compliance are impacting adoption by healthcare organizations.

Challenges Related to Legislation in the U.S.

In the United States, every healthcare entity (e.g., hospital, university research facility, physician’s office) that deals with Protected Health Information (PHI) must adhere to the guidelines stipulated under the Health Information Portability and Accountability Act (HIPAA). HIPAA is a U.S. Federal law that was designed to protect patient privacy, and does so by mandating and enforcing strict privacy and security rules over how medical information is collected, handled, used, disclosed and protected. While the HIPAA Privacy rule pertains to patients’ privacy and rights for their personal health information, the
HIPAA Security rule, focuses on assuring the availability, confidentiality, and integrity, of electronic protected health information through a series of administrative, physical and technical safeguards. Under Title II of HIPAA, most of a patient’s medical record and payment history are considered PHI, and is protected under the law. PHI may only be disclosed to other medical entities on a “need to know” basis, only upon the permission of the individual patient and only the “minimum data fields required for the purpose involved”. As a result, one of the challenges is “Patient Consent Management” and managing PHI in a way that is sufficiently simple to enable use by the general public.

The owner of the data must require the cloud service provider (aka the “business associate”) to contractually agree to maintain all PHI in adherence with HIPAA standards. The HIPAA Privacy rule defines a business associate as “a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity”. Covered entities are institutions, organizations or persons who electronically transmit any health information in connection with transactions for the United States Health and Human Services (HHS) adopted standards. While ultimate responsibility for compliance always resides at the covered entity, the actual implementation of certain operational and control aspects of securing the data occurs at the business associate cloud provider.

From a legal perspective, business associates have certain privacy and security requirements that other generic “third party” entities don’t. This is a nebulous area and somewhat open for interpretation, with no consensus established. It is the responsibility of the cloud service provider to get the necessary certifications for HIPAA compliance. While there is no “true” HIPAA hosting certification, the strict guidelines established within the law must be met. A covered entity needs to establish a strong Service Level Agreement (SLA) with the Cloud Service Provider (CSP) to fully understand their liabilities and risks as well as being able to absorb those risks in the event of HIPAA non-compliance.

Under the HIPAA Security Rule, there are a number of items to be taken into account such as administrative controls, physical security, and technical security. New encryption technologies can protect resources required to meet stringent regulatory requirements even when they are sharing physical infrastructure with less sensitive resources. Additional physical security controls may be necessary at the covered entity and background screenings may be required for those CSP personnel who will in some form “touch” the data.

While healthcare entities are ultimately responsible under mandated HIPAA regulations for the security of PHI in the cloud, they often have little or no control where or how this data is moved, handled, or stored. For example, if a CSP moves data off shore to another country, it will be outside of U.S. jurisdiction and subject to international laws and therefore HIPAA non-compliant. This is a significant challenge for adoption of cloud technology for healthcare purposes. Cases like these that address cloud

2 Depending on the type of healthcare application, additional laws and regulations such as Sarbanes-Oxley (SOC), Gramm-Leach-Bliley (GLBA) and Payment Card Industry Data Security Standards (PCI DSS) may need to be applied.
provider control and compliance issues need to be clearly addressed in a cloud SLA established by the covered entity.3

Per Title II of HIPAA, technical and transmission security measures need to be implemented to facilitate the transfer of ePHI data among institutions over communications networks and guard against any unauthorized access. Whenever PHI data flows over open networks, it must be encrypted as should PHI data at rest. HCOs have expanded their use of mobile devices (smartphones, Personal Digital Assistants (PDAs), tablets, and notebooks). Those devices are rapidly becoming the dominant client end user device and are increasingly being tied to their use of cloud based applications. A lack of technical knowledge or detailed familiarity of the underlying communications processes and data sharing among applications may put the health care provider in direct violation of HIPAA rules.

Data leaving a mobile device onto a commercial 3G or 4G network is typically the responsibility of the network operator to ensure that the data is securely transported. All major domestic carriers have developed encryption measures designed to safeguard data flowing through their cellular networks. Without proper data encryption methods in place, sensitive or PHI data may be passed through non-secure networks such as the Internet or transmitted through an open Wi-Fi hot spot.

Medical devices also pose potential privacy risks. As medical devices and sensors become more sophisticated, they may allow for not only external monitoring and data gathering for storage in a Big Data cloud but for their control as well. Improper controls or management of these patient medical devices may compromise patient information or the HCO infrastructure, or provide a mechanism for inappropriate access to or tampering of the device itself.

Another critical component that is required to meet HIPAA compliance is the process of correctly identifying and authenticating users along with a comprehensive authorized privilege and role-based access control. Passwords or other safeguards are necessary to confirm the identity of all those seeking to access PHI information. Currently, varying forms of user authentication and authorization are used to provide access to cloud based capabilities with personal access information required for each system or application. This results in a potential plethora of user accounts, account IDs and passwords, which not only makes it challenging for the user but also reduces privacy and security.

Future Identity Management advances should provide for end-to-end full life-cycle capabilities, including change management, that will not only provide a single point of user authentication / authorization but a single site for user control and access to their related PII (personally identifiable information). Additionally, such a capability should also work across all device types (PCs, cell phone, mobile computing devices and sensors) to provide a unified user-centric secure and private digital identity. Associated with user access is the necessity to track the actions or behaviors of users in audit logs to determine PHI data usage. In order to maintain PHI data confidentiality and data integrity, the

appropriate access controls should be in place so no accidental or unauthorized disclosure of data takes place or that data does not get unintentionally or maliciously altered.

**Global Challenges for Healthcare Clouds Related to Data Privacy Legislation**

The governments of many countries in the mature markets are currently struggling to address and coordinate the combined needs of privacy and freedom of information. On 1 July 2012, the Article 29 Data Protection Working Party (the independent European advisory body on data protection and privacy) adopted an opinion on cloud computing (WP196) that is expected to be used as a standard guide for cloud requirements in the EU. Their opinion stated that the cloud client should be considered as the data controller while the cloud provider acts as the data processor, except where the provider processes the personal data for its own purposes. One effect of that definition is that the applicable law will usually be the legislation of the country in which the cloud client is established, rather than the place where the cloud computing providers are located.

Although the European Commission’s standard contractual clauses offer adequate safeguards, they do not apply to a situation where the cloud provider acting as a processor is established in the EU and uses non-EU subcontractors. In fact, the Working Party is particularly concerned about data protection risks related to international law enforcement requests such as those related to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act. The Act gives the US government the right to demand data if it declares conditions as being an emergency or necessary to homeland security. Because the location of data is abstracted in cloud computing, a cloud service provider could move data between countries and jurisdictions without the awareness of the data owner. In fact, data could reside in more than one country, each having a different legal stance on privacy.

As a result, the European Commission is working on a call for a prohibition of corresponding disclosures of personal data to be included in the future General Data Protection Regulation, subject to specific exceptions.

**Service Reliability**

From an operational standpoint, the reality is that all cloud ecosystems and enterprise infrastructures will have disruptions to some degree at some point in time. Mission critical HIT applications must meet very high performance, availability, and reliability standards. The growing reliance on distributed network-based solutions, such as Service-Oriented Architecture (SOA) web services, Cloud-based service providers and Software as a Service (SaaS) solutions, are only increasing the complexities of managing, securing and maintaining these dynamic environments. These types of services may be hosted by multiple heterogeneous, geographically distributed CSPs or in local on-premise data centers. In order to meet overall mission performance goals, the service capabilities may have their workloads shifted across the cloud ecosystem in order to optimize processing and storage resources.

Despite some well publicized CSP disruptions, cloud based services overall have been remarkably reliable, which may be fostering a dangerous complacency among customers who are putting all their trust in them. It’s important to note that CSPs continue to spend significant sums of money to maintain
security and reliability of their capabilities for their customers. Their business is dependent on delivering capabilities that meet the expectations of the most demanding enterprise. The data compiled by AppNeta on the uptime reliability of 40 of the largest providers of cloud-based services provides some basic statistics on how CSPs are performing. The overall industry yearly average of uptime for all the CSPs monitored is 99.948% or 273 minutes of unavailability per year. The best providers achieve 99.9994%, (three minutes of unavailability each year) and the worst providers achieve 99.92%, (420 minutes of unavailability each year). These statistics indicate a low outage risk from cloud providers (Thibideaux, 2011).

Disaster recovery is a component of service reliability that focuses on processes and technology for resumption of applications, data, hardware, communications (such as networking), and other IT infrastructure in case of a disaster. The process of devising a disaster recovery plan starts with identifying and prioritizing applications, services and data, and determining for each one the amount of downtime that’s acceptable before there is a significant business impact. In general, current cloud SLAs provide inadequate guarantees in case of a service outage due to a disaster. Most cloud SLAs provide cursory treatment of disaster recovery issues, procedures and processes.

The healthcare industry’s dependence on the availability and reliability of information can be a matter of life and death. Performance is another factor that is slowing the pace at which cloud computing is adopted by healthcare organizations. Globally, hospitals, physicians and patients have different types of Internet connections that can impact performance of a healthcare system. For example, many rural healthcare facilities still use modems to connect to the Internet. Uptime and other appropriate service levels should be reviewed and included as part of the service level agreement.

**Integration and Interoperability**

A key component to healthcare that transcends the IT domain is the reliable exchange of commonly understood information to facilitate coordinated patient care. Different participants (e.g., surgeons, pediatricians, nurses) in the healthcare ecosystem have different terminologies and requirements. Delivering an end-to-end system that fully integrates all patient information, including emergency and in-patient care, pharmacies, billing, reimbursement and more requires standardization and interoperability.

Certain standards are needed to help drive the transfer and storage of data within the cloud through common and unifying components. To help facilitate these issues, the HCOs have many Standards Development Organizations (SDOs) developing specifications and standards to support healthcare informatics, information exchange, and systems integration.4

Most SDOs produce standards for a particular healthcare domain such as pharmacy, medical devices, imaging or insurance (claims processing) transactions. The large number of healthcare organizations

---

4 Some of the American National Standards Institute (ANSI) accredited SDOs include Health Level Seven (HL7) International, IEEE-11073, and NCPDP. The National Institute of Standards and Technology (NIST) also monitors and engages with the SDOs to facilitate the process.
and standards that exist, or are in-development, make it difficult to monitor and track the overall landscape of healthcare standards. Even with standards such as Digital Imaging and Communications in Medicine (DICOM), many manufacturers implement or interpret technology standards differently, so data interchange and interoperability remains difficult.

Some of the risks associated with migration to the cloud include incompatibilities with the enterprise organization, strategic vision, its business or operational processes, managing a new services-based financial/billing chargeback model, dealing with the lack of transparency of off-loaded data and applications, or leveraging existing system architecture. A typical cloud computing environment consists of disparate components from multiple CSPs and legacy on-premise data center applications. Ultimately the legacy system infrastructure, business process improvements, financial management, and Operations and Maintenance (O&M) all need to be an integral part of the HIT cloud strategy.

**Data Portability**

Another barrier that impacts some healthcare organizations’ willingness to adopt cloud computing is the concern regarding the ability to transition to another cloud vendor or back to the healthcare organization without disrupting operations or introducing conflicting claims to the data. With traditional IT, the healthcare organization has physical control of systems, services and data. The concern is that if a provider were to suspend its services or refuse access to data, a healthcare organization may suddenly be unable to service its patients or customers. Or, if the healthcare organization were given notice that the cloud service would be discontinued, the lack of interoperability across cloud systems could make it very challenging to migrate to a new cloud service provider. This risk highlights the need for provider agreements that address termination rights, rights to access and retrieve data at any time, termination assistance in moving to another provider and “cure periods” to allow breach of contract to be remedied before the provider terminates or suspends services.

**Benefits of Cloud Computing for Healthcare**

“Patient centricity” has become the key trend in healthcare provisioning and is leading to the steady growth in adoption of electronic medical records (EMR), electronic health records (EHR), personal health records (PHR), and technologies related to integrated care, patient safety, point-of-care access to demographic and clinical information, and clinical decision support. Availability of data, irrespective of the location of the patient and the clinician, has become the key to both patient satisfaction and improved clinical outcomes. Cloud technologies can significantly facilitate this trend.

Cloud computing offers significant benefits to the healthcare sector: doctor’s clinics, hospitals, and health clinics require quick access to computing and large storage facilities which are not provided in the traditional settings. Moreover, healthcare data needs to be shared across various settings and geographies which further burden the healthcare provider and the patient causing significant delay in treatment and loss of time. Cloud caters to all these requirements thus providing the healthcare organizations an incredible opportunity to improve services to their customers, the patients, to share information more easily than ever before, and improve operational efficiency at the same time.
• **Clinical Research.** Many pharmacology vendors are starting to tap the cloud to improve research and drug development. The ‘explosion of data’ from next generation sequencing as well as the growing importance of biologics in the research process is making cloud-based computing “an increasingly important aspect of R&D”. Currently, pharma firms do not have the capacity to run large datasets – especially DNA sequencing - as the size of the data can overwhelm their computers. Commercial cloud vendors have developed pharma-specific clinical research cloud offerings with the goal of lowering the cost and development of new drugs.

• **Electronic Medical Records.** Hospitals and physicians are starting to see cloud-based medical records and medical image archiving services coming on line. The objective is to offload a burdensome task from hospital IT departments and allow them to focus on supporting other imperatives such as EMR adoption and improved clinical support systems.

• **Collaboration solutions.** Early successes of cloud-based physician collaboration solutions such as remote video conference physician visits are being trialed. Extending such offerings to a mobile environment for rural telehealth or disaster response is becoming more real with broader wireless broadband and smartphone adoption. Cloud technology supports collaboration and team-based care delivery and the ability to use applications based on business model requirements and a common set of clinical information.

• **Telemedicine.** With the increase in availability of mobile technologies and intelligent medical devices, telemedicine has grown to include not only tele-consultations and tele-surgeries, but also health record exchange, video-conferencing, and home monitoring. Cloud computing and the related ease of services deployment and data storage is an enabler for telemedicine.

• **Big Data.** Healthcare organizations turn to cloud computing to save on the costs of storing hardware locally. The cloud holds big data sets for EHRs, radiology images and genomic data for clinical drug trials. Attempting to share EHRs among facilities in various geographic areas without the benefits of cloud storage could delay treatment of patients.

• **Analytics.** Cloud computing facilitates practice and population scale information and insights are available in near real-time. This availability ensures that the most current, complete insights and clinical knowledge are available to support care provider decisions and to enable a focus on value creation related to improving outcomes rather than consumption. Information contained within a cloud can also be better analyzed and tracked (with the proper information governance) so that data on treatments, costs, performance, and effectiveness studies can be analyzed and acted upon. Information can be harvested and repurposed for more appropriate referrals and medical research to support the promise of personalized health and care.

• **Health Information Exchange.** Health information exchanges help healthcare organizations to share data contained in largely proprietary EHR systems. CIOs may accelerate the deployment of HIE via a linkage to a strategic cloud implementation.
Healthcare organizations continue to depend on computer systems that are extremely vulnerable to data breaches caused by technology deficiencies, theft and insider misconduct. Cloud-computing systems can be designed to be safer than traditional client-server systems against the prevailing causes of healthcare data breaches. But while adoption of cloud computing is growing in healthcare, the vast majority of hospitals and healthcare systems still use client-server systems, almost universally for enterprise-wide electronic medical records.

These systems center on local servers, usually housed in poorly-secured server rooms, directly accessed by desktop computers and laptops scattered throughout the enterprise. Patient health data is routinely downloaded and uploaded back and forth from desktop and laptop computers to the local servers.

A web-based secure private cloud also better addresses the insider threat to patient data from disgruntled employees – or even larcenous employees – or from patient-record snoopers and human error, the simplest of which can lead to disastrous results. The security differences between secure private cloud and client-server systems come down to the proximity of sensitive data to those who might misuse it, the number of people who have access and the number and safety of access portals.

By consolidating applications on shared infrastructure, there is an opportunity to share security controls, including overall penetration testing for web-based applications.

Far from lacking in security – the prevailing fear in healthcare and elsewhere – secure private cloud can provide better physical security and equal or better cyber security when compared to traditional client-server computing systems.

Few industries can benefit as much from the application of cloud computing as healthcare, where government mandates, security requirements and a need to replace outdated technology make a CIO's job difficult. They must balance stringent security and privacy regulations with a pressing need to improve IT infrastructure and a mandate to implement electronic health record (EHR) software—all amid the political firestorm of healthcare reform, increasing pressure to cut costs, general reluctance among health care professionals to trust technology and a shortage of IT talent in the industry.

**Strategic Recommendations**

Cloud computing requires an integrated and orchestrated strategy. A strategy assessment is fundamental to the thoughtful definition of how you will take advantage of cloud computing and the value it will create for your healthcare organization. This will include:

- **Understanding the value proposition for cloud.**

  Advances in Information Technologies such as mobile computing, wireless networks, and cloud computing are creating exciting value propositions as well as new opportunities to improve the healthcare ecosystem. These three tightly linked key technologies are supplemented with new healthcare processes and advances such as Healthcare Information Exchanges, Electronic Medical Records, virtual care solutions, and connected healthcare appliances that are focused on improving patient care and patient outcomes.
A value proposition is an offer that describes the quantifiable benefits that the cloud is delivering and is highlighted in several examples.

Most health care IT infrastructures would require a significant upgrade to capture, share, and protect EMR information. Cloud-based offerings provide alternative approaches to help healthcare providers better address the otherwise large capital IT investment required for a delivery of EMR services. A related example is the portable and open medical image archiving services that are becoming available from several significant cloud providers that enable the offloading of these tasks from hospital IT departments.

Mobile health (mHealth) applications for smart phones are used for health related activities such as counting calories, calculating body mass index, exercise management, chronic disease monitoring, heart rate monitoring and smoking cessation. The number of healthcare applications in the iTunes store alone exceeds 10,000. Since mobile devices have limited computational capacity and storage capabilities, more sophisticated applications rely on a cloud computing framework to perform the key back-end related services. Other related solutions for remote monitoring, eHealth or telehealth, are similarly increasing based on improved wireless broadband capabilities. Monitored patient data is maintained in the cloud and can be tied to cloud-based EMR data. These forms of remote monitoring can deliver new services to previously untapped markets as well as provide new revenue sources to the healthcare industry.

The adoption of advanced health IT will bring forth a new information era through the harnessing of “Big Data” which provides the mechanisms for aggregating, mining, and analyzing large amounts of medical data on processes, treatments, effectiveness, costs, and conditions. Cloud-based big data solutions can be shared among authorized health care providers to provide access to potentially life-saving information.

- **Exploring cloud workloads and deployment models.**

While much attention is being paid on meeting the requirements for implementing EMR, healthcare organizations should not lose sight of key opportunities for infrastructure improvements and enhancements that in many cases complement EMR initiatives. New infrastructure technologies that are facilitated by the cloud computing paradigm can reduce costs, improve performance and accelerate efforts to achieve meaningful use. Cloud-based environments will lower the barriers for innovation and modernization of health care IT systems and applications.

As noted in the Overview section, different cloud deployment models offer different benefits, capabilities and risks that should factor into the development of a business strategy and forward looking plan. Despite the promising capabilities of the cloud, there are numerous technical approaches and factors (e.g., security, service level availability, maintenance, system utilization) that must be considered. As an example, a private cloud whose resources are off-premise may be a cost benefit to the organization but data latency in the application use may pose a negative factor. This would indicate that a private cloud might be better suited for commodity enterprise workloads and applications like email, collaboration, financial systems and resource planning.
• **Developing a cloud solution based on the value proposition, workload and deployment model.**

The basic value proposition of cloud computing is purchasing only the resources (e.g., virtual CPUs, memory, storage, network) that the organization needs to consume at the time they require it, and then pay accordingly. This value proposition is critical as organizations are driven to become as lean as possible, without sacrificing patient care. Depending on the deployment and delivery models, multiple organizations can safely share common infrastructure, which reduces the cost of the infrastructure due to resource sharing. Provisioning new resources, workloads or applications now becomes a faster process and can be controlled through a single IT administrated control system. The typically extended procurement process for acquiring new IT resources or dealing with multiple organizations to accomplish IT related tasking can now be avoided.

In addition to shortening the procurement process, infrastructure sharing by multiple organizations naturally leads to standardization of the surrounding IT processes required to manage the infrastructure. Once standardization is achieved, additional automation can be used to further shorten process times. A side benefit of automation is the reduction of human error, thus increasing service availability.

• **Developing a plan to monitor key performance indicators to validate business benefits.**

An important strategy is the development of the necessary models that show the benefits of cloud computing adoption to both healthcare providers and consumers. This involves a continual examination and monitoring of the key technology factors in the context of the healthcare operating model. It is impossible to optimize an organization and determine benefits without regular and accurate analytics. The process begins by outlining a plan that includes identifying the **Key Performance Indicators (KPIs)** for the given healthcare entity and the setting of success criteria goals.

The plan would include comparing specific metrics with traditional IT or potentially non-IT methods (e.g., paper based EMR, current imagery scan retrieval) with the adopted cloud computing solution. The factors are generally classified as cost, infrastructure utilization, security, quality, availability, user satisfaction, audit controls, profitability indicators, and return on investment as it relates to cloud computing characteristics and service delivery. Some of these are contractual matters as defined in Service Level Agreements (SLAs) with the cloud service provider. Although these IT metrics are important, the KPIs that support the overall healthcare related goals (e.g., patient care quality) will ultimately validate the role of cloud-based solutions.

When transitioning to cloud computing, healthcare organizations must ensure the following:

• **Systems must be adaptable to various departmental needs and organizational sizes.**

Different healthcare organizations and departments will have their respective diverse sensitivities as to the uptime availability, system responsiveness, latency, and scalability requirements for their healthcare IT applications and workflow. This factors back to whether a cloud solution deployment model is public or private, is located on-premise or off-premise, the cloud delivery method (e.g., SaaS), and the contractual Service Level Agreement (SLA) for the provided services. Different cloud based design patterns can be appropriately applied to
address these sensitivities dependent upon the healthcare providers’ needs and sizes but must be evaluated on a case-by-case basis.

- **Architectures must encourage a more open sharing of information and data sources.**

  The healthcare industry is slowly moving toward an information-centric care delivery model that facilitates data / information sharing and collaborative workflow. While steps have been made in standardizing medical data formats and vocabularies, the adoption of secure mechanisms for widespread, interoperable information exchange between all of the healthcare players (e.g., providers, patients, government agencies, insurance companies) is slow in coming.

- **Technology refreshes cannot overburden the already brittle budgetary environments.**

  The financial benefits to launching a cloud computing initiative can often accrue capital expense (CAPEX) savings relatively quickly by transitioning costs from CAPEX to an operational expense (OPEX). However, the healthcare organization should first develop a strategy that complements its business goals / timelines with its current IT infrastructure and technology refresh cycle with the necessary elements of the cloud. There is the hidden cost that in the migration to a successful cloud computing-based solution, there can be both technical and organizational challenges as well as a learning curve.

- **Scalability is a must as more patients enter the system and more data becomes digitized.**

  A cloud infrastructure, such as one utilized for EMR, can quickly “burst” above its initial designed workload capability, when the need arises. This distinguishes cloud computing as a utility-like resource whose resources change based on the healthcare providers changing needs.

- **Portability is needed as doctors and patients would benefit from the ability to remotely access systems and data.**

  Cloud based solutions provide ease of healthcare data and application access as they are ubiquitous and available virtually anywhere there is an Internet connection or Wi-Fi connectivity. Strategies must include the necessary management policies (e.g., change management), technologies (e.g., encryption), and software tools for mobile / remote device access to comply with all pertinent regulations, laws and organizational procedures.

- **Security and data protection are paramount.**

  Security and data privacy issues are of vital importance in the adoption of any IT-based healthcare solution. Not only must the appropriate security be implemented and potentially enhanced in the existing IT infrastructure but into the underlying cloud monitoring and management processes. An understanding of the SLA responsibilities as to the distinction of security and data privacy requirements between the cloud provider and the end users must be well understood. The well-documented recommendations found in CSCC, NIST and Cloud Security Alliance (CSA) papers should be followed.
Organizations need to manage both the logistical and physical security of their infrastructure carefully, taking into consideration everything that could happen throughout the life cycle of PHI. The US HIPAA HITECH Act presents one of the better ways to support the exchange of PHI, built on a HIPAA baseline. At the same time, the epSOS European eHealth project is on a path to create a Europe-wide system for patient data exchange between member states.

To optimize the effectiveness of cloud computing and to achieve efficiencies, we expect organizations to adopt standardized processes and focus on achieving differentiation through collaborative partnerships and use of information. Common processes, data and standards can improve quality and operational effectiveness. Rapid, flexible and scalable IT can change how information is used and delivered.

Cloud activity should take root in private or hybrid clouds (because of security and other industry nuances) rather than public cloud infrastructures. A secure private cloud system is built around a high-security private database, networked to users through web-based software-as-a-service (SaaS), where each client’s data is protected in its own database schema. Public cloud refers to storage infrastructure available to the general public where data may be stored in various database locations depending on availability. Patient health information should not reside in a public cloud.

**Bibliography**

5 Steps to Assess Health Data Breach Risks:  

Cloud Computing in Health Care to Reach $5.4 Billion by 2017:  

Cloud computing in healthcare: the question is not if, but when:  

Cloud in the Western European Healthcare Sector: Trends and Strategies For 2012 and Beyond:  
[http://www.idc-hi.com/getdoc.jsp?containerId=HIOH02U](http://www.idc-hi.com/getdoc.jsp?containerId=HIOH02U)

CSCC Practical Guide to Cloud Service Level Agreements  

CSCC Security for Cloud Computing: 10 Steps to Ensure Success  

European Commission Article 29 Data Protection Working Party Opinion 05/2012 on Cloud Computing:  
Gramm-Leach-Bliley Act:

HHS.gov HHS.gov/Recovery:
http://www.hhs.gov/recovery/programs/index.html

http://www.himss.org/content/files/BasicFactsAboutMeaningfulUseARRA.pdf

HIPAA 101 The Basics and Business Associates:
http://www.colorado.gov/dpa/dfp/hipaa/hipaaa20presentation.pdf

IDC Singapore’s Integrated Healthcare System is Aligned with eGov2015, says IDC Health Insights:
http://www.idc.com/getdoc.jsp?containerId=PRSG23066611

Lateral Economics The potential for cloud computing services in Australia: A Lateral Economics report to Macquarie Telecom:


PCI Security Standards Council PCI SSC Data Security Standards Overview:

Spotlight on Sarbanes-Oxley Rulemaking and Reports:
http://www.sec.gov/spotlight/sarbanes-oxley.htm

The power of cloud: Driving business model innovation:

U.S. Department of Health and Human Services Health Information Privacy:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/index.html