Impact of Cloud Computing on Healthcare
Version 2.0

February, 2017

Contents

What is New in Version 2.0

Version 1.0 of this white paper was published in November, 2012. In the interval, the market dynamics of the healthcare industry have changed significantly with the growing impact of consumerism, digitalization, preventative healthcare and regulations. To effectively address these industry trends, cloud computing is playing a more prominent role in healthcare IT – a shift that is expected to accelerate in the future.

Version 2.0 of this paper provides a fresh perspective on the current market dynamics, challenges and benefits of cloud computing on healthcare IT. It also highlights the new sets of services specifically targeted at healthcare that cloud computing enables. Lastly, prescriptive guidance has been added to the paper to help ensure successful deployment of cloud-based healthcare solutions.

Executive Summary

The aim of this paper is to provide a practical reference to help enterprise information technology (IT) and business (i.e., administrative, clinical, research and teaching) decision makers of the healthcare industry as they analyze and consider the implications of cloud computing for their organizations. The paper includes guidance and strategies designed to help decision makers, who may be new to cloud computing, evaluate and compare cloud services offered by commercial cloud service providers (CSPs); taking into account different requirements from patients, medical practices, hospitals, research facilities, insurance companies, governmental/regulatory bodies, and various other professional and organizational actors. This paper serves as a foundation upon which additional, more detailed whitepapers on specific healthcare and cloud computing topics can be developed in the future.

When considering whether to use cloud computing, healthcare actors must have a clear understanding of the unique benefits and risks relative to the purpose and scope of medical practice and healthcare delivery: optimizing case outcomes while maximizing patient safety and the economy, efficiency and effectiveness of care and treatment. Then they must establish appropriate contractual relationships with the CSPs by means of cloud service agreements and service level agreements (SLAs). Consideration also 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); because each model includes different requirements and responsibilities. Cloud deployment models – private, public, and hybrid – also impact strategic decisions; so they must be considered carefully.

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 influence adoption of cloud computing in the healthcare industry, together with an overview of the main barriers that must be addressed. This section also highlights the key considerations for service and deployment models.

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 “High Value Services” section highlights specific cloud

computing services for healthcare currently available that provide substantial potential benefits to both healthcare organizations and patients. The "Considerations for Leveraging Cloud Computing for Healthcare" section highlights the critical areas that must be assessed as part of the planning process for migrating currently implemented healthcare IT systems and applications to the cloud.

The concluding "Guidance" section includes specific recommendations for how best to achieve the benefits of cloud computing while maintaining an acceptable level of risk. Each healthcare organization must perform its own analysis of needs; and it must assess, select, engage and oversee management of the cloud services that can best fulfill those needs.

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

Current Market Dynamics

Continual change in both supply and demand within the healthcare market influences the use of IT and serves as the principal driver for the adoption of cloud computing. Demand for healthcare will continue to rise, mostly because of population aging and growth but also from an increasing interest in wellness by consumers. It is expected that these forces will influence the role of IT in the industry; and, by association, the role of cloud computing. The current estimation is 11-17% growth in demand for healthcare resources between 2014 and 2025 [1]. Also, based on current utilization of healthcare resources, it is estimated that the growth in primary care physician supply will not be adequate to meet demand in 2020 [1]. Taking these statistics into consideration, the following four trends are driving the healthcare market dynamics:

1. *Escalation of consumerism*. This has re-focused the healthcare provider market from volume-based to value-based. Participants are graded based on the value obtained by the consumer as opposed to the volume of services. The fee-for-service model has long rewarded physicians and hospitals for carrying out as many tests and treatments as possible. The value model seeks to reward professional and organizational providers on the basis of care cost-effectiveness and clinical case outcomes. This change requires rapid innovation enabled by the variable on-demand IT resources that cloud computing can provide cost-effectively.

   Patients, a.k.a. consumers, will play an increasingly important decision-making role in the healthcare market, particularly regarding decisions related to healthcare coverage and treatments. Also, many healthy consumers are taking an active role in maintaining their health and well-being by using smartphones and wearables to track their diets, exercise records and their vital signs; or to read reviews of doctors and care facilities. This increasing consumer participation is in turn driving the need for healthcare provider systems that offer more convenient access and facilitate greater interaction. Cloud computing enables consumers to identify and use best-of-breed health services from a range of providers (some of which are consulted remotely via mobile e-visits). [2]

2. *Impact of healthcare regulation and restructuring of financial risks.* Healthcare reform and regulation are changing the healthcare landscape. Regulation impacts the structure of the market and is leading to consolidation, both vertical and horizontal. Healthcare regulations have driven faster growth of mobile health in the consumer wellness space than in the clinical health space. This, in turn, drives the need for native cloud applications that are architected and developed to meet the rapidly changing consumer requirements while complying or enabling compliance with applicable regulations.

   Healthcare data management includes stringent requirements for security, confidentiality, privacy, traceability of access, reversibility of data, and long-term preservation. Hence, cloud service providers must address all of these legal, regulatory and accreditation requirements. Interoperability is a key requirement that has been a chronic impediment to healthcare delivery improvement. IT approaches such as the use of cloud-based enterprise service bus (ESB) software with electronic healthcare record (EHR) connectors can help overcome this barrier.

   Regulations such as the ONC Health IT Certification Program [27] and the EU GDPR [6] are also now requiring new interfaces into healthcare software, including APIs and data access capabilities. These requirements are leading to a need to update, augment or replace existing HIT systems in order to provide the new capabilities.

3. *Influence of digitalization*. IT is the enabler that allows consumers to take greater control over their healthcare choices. Around the globe, healthcare reform has mandated that it is time for healthcare IT to be modernized; and that 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 IT infrastructure that allows hospitals, medical practices, insurance companies, research facilities and other organizational entities in the healthcare ecosystem to leverage improved computing capabilities at lower initial capital outlays than previously required by purchase or long-term licensing. Additionally, cloud environments lower the barriers for innovation and modernization of IT systems and applications. Finally, cloud computing offers an IT platform that is collaborative to facilitate information sharing, knowledge management and predictive analytics across the healthcare ecosystem, enabling cross-industry services.

   IT-enabled fitness monitors and mobile IT applications allow consumers to monitor health metrics such as activity levels and vital signs. The collection of this data on a daily basis by individuals helps populations to be more informed about their health and more capable of making their own care decisions. In addition, people are beginning to share this data with their doctors and other healthcare providers to use when making decisions and working through differential diagnoses. By enabling consumers both to own and have access to their health-related data, digitization has eliminated the information asymmetry that long has benefited

healthcare system incumbents, particularly providers and payers/insurers, and has inhibited the evolution of an informed healthcare consumer.

4. *Focus on preventive healthcare*. Prophylactic interest has led to greater engagement with consumers to provide better aftercare and community based healthcare. Consequently, mobile applications, the Internet of things (IoT) and wearable technologies (most of which are supported by cloud applications) are becoming more commonplace. In addition, healthcare delivery is becoming more decentralized and thereby providing a wider choice of institutions where the patient can receive care (e.g., hospitals, retail clinics or at home using telemedicine and accessing hospital portals).

   Evolving behaviors will change healthcare. Healthcare is currently a "fix-me system"—patients go to the hospital when something is broken or not operating correctly and therefore needs repair or adjustment. By this point in the typical progression of pathology, the cost of care and treatment is expensive and may be applied too late in the progression for medical science and technology to do much good. With the current change in the healthcare incentive structure from volume to value orientation, medical professionals everywhere will be rewarded for guiding people into making behavioral and other choices that are more likely to keep them healthier on a continuing basis.

5. *Need for medical practice and healthcare delivery transformation.* Professional and organizational healthcare providers (predominantly physicians in private practice and general hospitals, respectively) conduct the business of healthcare according to standards and practices that may vary significantly. Standards of care differ by specialty and pathology, clinical care and treatment practices vary with provider experience and locale, and best practices for optimal case outcomes without risk of increased patient morbidity or mortality remain elusive. The most successful mitigation method is the provision of location- and time-independent, collaborative, consistent and real-time cognitive support which only cloud-based information technology can provide. Such IT capabilities as enterprise service bus (ESB) for vendor-/provider-specific EHR connectivity and data communication; intelligent business process management suites (iBPMS) for process automation; and evidence-based, predictive analytics for medical diagnosis and treatment planning can affect the positive transformation of medical practice and healthcare delivery, if deployed on HIPAA enabled (or equivalent) CSP platforms to minimize cost and complexity.

These five trends will result in the following:

- replacing or augmenting traditional healthcare mechanisms with digital options;
- increasing investment in technologies that accelerate the digitization of the healthcare industry;
- shifting the roles played by incumbent healthcare actors;
- employing data integration and/or comparative analysis;
- accelerating the accrual of medical knowledge and practice improvement; and
- employing new business models for lower cost, better efficiency and higher effectiveness.

Benefits of Cloud Computing for Healthcare

The five aforementioned trends in the healthcare industry are having significant impact on HIT systems. There is substantial growth in demand for healthcare services because of aging populations, the increasing prevalence of chronic diseases and comorbidities. Concurrently, there are cost pressures stemming from the need to do more and higher quality work with fewer and more costly resources and also reduced revenue. Expectations for better outcomes, higher quality treatment and more value from the healthcare services provided increase the need for point-of-care access to medical data and the parallel evolution and adoption of mobile devices, both for medical staff and for patients, are forcing the need for IT systems to adapt. Also, the significant increase in digitization of medical records – including the accelerating increase in adoption of electronic medical records (EMR), electronic health records (EHR) and personal health records (PHR) – and the increasing prevalence of digital outputs from scanning and monitoring devices, such as magnetic resonance imaging (MRI) scanners and bedside monitors and infusers, provide more voluminous and varied digital data to maximize the potential benefit of cloud solutions.

Healthcare provider systems leveraging cloud-based computing and cloud services offer an array of benefits in comparison to in-house client-server systems; including economic, operational and functional advantages.

The *economic* benefits of cloud computing can be significant since cloud computing provides cost flexibility and the potential for reduced costs. Heavy capital expenditure can be avoided, because IT resources are acquired on demand as needed and paid for as an operating expense. Also, the cost of staff resources required to deploy and maintain IT resources are included in the cost of cloud computing. Therefore, the need for additional healthcare provider skilled IT staff resources and related costs may be reduced when using cloud services for IaaS and PaaS platforms but even more so for SaaS solutions where the cloud service provider takes the lion's share of responsibility.

From an *operational* perspective, cloud services offer scalability and the ability to adjust to demand rapidly. Cloud services can offer better security and privacy for health data and health systems. Cloud service provider data centers are typically highly secure and well protected against outsider and insider threats using administrative, physical and technical methods implemented and maintained by expert professional staff. Cloud services can offer sophisticated security controls, including data encryption and fine-grained access controls and access logging. Medical systems built using cloud services can provide web access to data, avoiding the need to store information on client devices. The need for scarce IT security skills within the healthcare organization also is minimized. Cloud service providers typically operate on such a scale that they have all the necessary IT skills, with the costs of those skills spread across many customers.

Healthcare *functionality* can be enhanced by cloud-based healthcare IT systems that offer the potential for broad interoperability and integration. Healthcare cloud services are Internet-based and generally use standard protocols, so connecting them to other systems and applications is typically straightforward, although EHR/EMR vendor contractual and technical impediments continue to present a challenge. The ability to share information easily and securely is a critical capability, and cloud services are good enablers for this. Cloud services also support rapid development and innovation, especially for

mobile and Internet of Things (IoT) devices; thereby satisfying the demands placed on healthcare IT systems by these new and rapidly advancing technologies. Cloud services can *enable remote access* to applications and data via the Internet using wired and wireless systems to enable access at anytime from anywhere that internet connectivity can be established. Support for access by mobile devices is often a feature supported by healthcare cloud services. Also, cloud services offer access to a much larger ecosystem of healthcare provider, payer, life sciences and IT solution partners; all of which increase the potential for a wide range of services to healthcare provider organizations.

Arguably, the greatest functional benefit of healthcare cloud services is the wide range of new capabilities that they are able to offer. These services offer the opportunity to extend the capabilities available to health organization staff, in order to implement better ways of working and to offer new services to patients.

Sophisticated analytic capabilities can be brought to bear to improve both patient-specific and population-based assessment and management. Some cloud services such as intelligent business process management suites (iBPMSs) and case management frameworks (CMFs) can support healthcare provider staff cognitive capabilities, which in turn can mitigate medical mistakes and minimize patient adverse events (PAEs). Some of the most advanced analytic services could enable healthcare provider subject matter experts (SMEs) to access a vast body of medical knowledge to better deal with such problematic healthcare provider use cases as differential diagnosis and treatment planning, the potential for which has not been realized to date owing to the cost and complexity of analytics solutions that cloud availability can obviate.

The capabilities offered by health cloud services can be expected to facilitate personal health maintenance, improve diagnoses, obtain better case outcomes, optimize healthcare delivery operations and facilitate the transformation from volume- to value-based care.

High Value Cloud Computing Services for Healthcare

Today, there are already many and varied cloud service offerings for healthcare, covering a wide range of capabilities. The following list is a representative set of the cloud service offerings available as of late 2016; the number and range of offerings is continuing to expand over time.

Population Health Management

Analysis of larger data sets across industries and deep learning are yielding important insights not previously available. Healthcare is no exception. Cloud and big data services can be used to track diseases; map them geospatially and inform the population where risk exists. Healthcare organizations can implement the services and infrastructure required to support these services for a fraction of the cost by utilizing cloud computing. Some of the tooling that exists in the marketplace today:

- Centers for Disease Control and Prevention (CDC)

The Office of Public Health Scientific Services (OPHSS) launched the CDC Information Innovation Consortium (CHIIC), as part of the agency's surveillance strategy to foster and promote creative solutions to surveillance challenges that are unique to public health.
http://www.cdc.gov/epiinfo/cloud.html

- IBM Explorys
  Health population management, analytics and data management.
  http://www.ibm.com/watson/health/explorys/
- eClinicalWorks
  https://www.eclinicalworks.com/
- McKesson
  http://www.mckesson.com/health-plans/population-health/
- Cerner
  https://www.cerner.com/solutions/population-health-management
- IBM Phytel Population Health Management
  https://www.ibm.com/watson/health/population-health-management/resources/phytel-solution

Care Management Support

Hospitals and physicians are more and more utilizing cloud based practice management, medical records and medical image archiving solutions. These solutions provide cost effective implementations offloading tasks from hospital IT departments allowing them to focus on supporting other operational and clinical support systems. Some of the tooling that exists in the marketplace today:

- IBM Watson Care Manager
  Manage care for a patient across all steps in the care process.
  https://www.ibm.com/watson/health/population-health-management/care-management
- Diabetes Care
  https://sweetspotdiabetes.com/
- eClinicalWorks EHR
  https://www.eclinicalworks.com
- McKesson
  http://www.mckesson.com/bps/ehr-and-practice-management-software-solutions/

Diagnostic Support

Organizations are developing new SaaS products and services to both concentrate the expertise required and lower the cost of operations for healthcare providers. Some of the tooling that exists in the marketplace today:

- Eyenuk EyeArt retinal screening
  Combines automated image analysis tools with a user-friendly telemedicine/cloud-based interface to address the need for faster screening of more diabetic patients.
  http://www.eyenuk.com/eyeart.html

- IBM Merge iConnect Retinal Screening
  Enables capture, storage and sharing of images and notes between providers performing diagnoses and those creating care plans.
  http://www.merge.com/Solutions/Eye-Care.aspx

Image Handling Services

Image handling services are at the forefront of the high value services for healthcare providers utilizing cloud based services and/or infrastructure. These services allow healthcare organizations to scale storage services at a fraction of the cost that would be required to implement them internally by minimizing the overall TCO (reduced capital expense, reduced staffing costs, geographic distribution). Some of the tooling that exists in the marketplace today:

- IBM Merge iConnect Access
  Enables medical image viewing across a wide range of devices.
  http://www.merge.com/Solutions/Interoperability/iConnect-Access.aspx
- IBM Merge iConnect Cloud Archive
  Secure cloud-based storage and access of medical images.
  http://www.merge.com/Solutions/Interoperability/IConnect-Cloud-Archive.aspx
- McKesson
  Picture archiving and distribution, Radiology information, Cardiovascular imaging.
  http://www.mckesson.com/providers/health-systems/diagnostic-imaging/diagnostic-imaging/
- RxEye Cloud
  Infrastructure for networked diagnostic imaging.
  http://rxeye.com/features/

Medical Practitioner Assistance

The opportunities for cognitive assistance abound with the introduction of machine learning, natural language processing and advanced analytics. Cloud services allow medical practitioners to search vast amounts of data to produce more reasoned treatment plans. Patients can utilize these services to explore their medical issues and collaborate with their treatment provider. Some of the tooling that exists in the marketplace today:

- Flatiron OncologyCloud
  Suite of tools for Oncology.
  https://www.flatiron.com/oncology-cloud
- Varian Fullscale Oncology IT solution
  Oncology and treatment planning system.
  https://www.varian.com/en-gb/oncology/products/software/it/fullscale
- IBM Watson for Oncology
  Cognitive assistance for oncology professionals.
  http://www.ibm.com/watson/watson-oncology.html

Patient Connectivity
Services which address patient connectivity enable patients to connect to the health services of providers. Examples include:

- eClinicalWorks
  https://www.eclinicalworks.com/
- Cerner
  http://www.cerner.com/Solutions/Member_Engagement/
- IBM Truven Micromedex Patient Connect Suite
  http://micromedex.com/patient-connect

Data Distribution Services
Data distribution services enable the exchange of key health-related data between organizations, such as electronic health records, patient images, and so on. Some of the cloud services in the marketplace today:

- IBM Merge eMix
  Exchange of patient images and other health information.
  http://www.merge.com/Solutions/Interoperability/Merge-eMix%E2%84%A2.aspx
- Medical Interoperability Gateway
  Provides a system for exchanging medical data in the UK.
  http://healthcaregateway.co.uk/
- Cal INDEX
  California Integrated Data Exchange is a health information exchange system for the state of California.
  https://www.calindex.org/

Laboratory Services
Laboratory services support clinical laboratories in their work. Some of the tooling that exists in the marketplace today:

- Cerner Laboratory
  http://www.cerner.com/solutions/hospitals_and_health_systems/laboratory/
- MediaLab Cloud-Based Software for the Lab
  https://www.medialabinc.net/
- IBM Merge LIS
  Clinical laboratory information system.
  http://www.merge.com/Solutions/Clinical-Labs/Merge-LIS.aspx

Clinical research
Many pharmacology vendors are delivering PaaS and SaaS solutions 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 computing an increasingly important aspect of R&D. Pharma firms no longer are required to implement the capacity to handle large datasets in their computing facilities lowering the barrier to entry and increasing the velocity of change.
Some of the tooling that exists in the marketplace today:

- Medidata Clinical Cloud
  https://www.mdsol.com/en/what-we-do
- IBM Merge eClinicalOS
  Management system for conducting medical research
  http://pages.eclinicalos.com/tour

Intelligent Business Process Management and Case Management Low/No-Code Services
Gartner defines business process as a service (BPaaS) as the delivery of business process outsourcing (BPO) services that are sourced from the cloud and constructed for multitenancy. Services are often automated, and where human process actors are required, there is no overtly dedicated labor pool per client. The pricing models are consumption-based or subscription-based commercial terms. As a cloud service, the BPaaS model is accessed via Internet-based technologies. Some of the tooling that exists in the marketplace today:

- Gartner Research (BPaaS)
  http://blogs.gartner.com/it-glossary/business-process-as-a-service-bpaas/
- Gartner Research (iBPMS)
  https://www.gartner.com/doc/reprints?id=1-3F1C5YC&ct=160817&st=sb
- IBM Merge Financials
  Back office automation for billing, accounting, etc.
  http://www.merge.com/Solutions/Radiology/Merge-Financials.aspx
- IBM Merge Document Management
  Paperless office solution for healthcare organizations.
  http://www.merge.com/Solutions/Radiology/Merge-Document-Management.aspx

Considerations for Leveraging Cloud Computing for Healthcare

Healthcare organizations (HCOs) are expected to provide new and improved patient care capabilities while simultaneously limiting healthcare cost increases. IT plays an important role in the health and patient care arenas, with cloud computing beginning to make its mark. There are substantial advantages for the utilization of cloud computing as part of healthcare IT; however, specific considerations must be addressed by customers as outlined in the following table.

Technical Areas	Cloud Computing Considerations
Privacy & Security	• Healthcare entities need to establish strong cloud service agreements with detailed provisions relating to security and privacy in order to fully understand their liabilities and risks as well as being able to absorb those risks in the event of non-compliance. • Healthcare entities must stay informed of where and how electronic protected health information (ePHI) is moved, handled, or stored by their CSP. For example, if a CSP moves data to another country, it may be subject to international laws and therefore non-compliant with government regulations. • Additional physical security controls may be necessary for the healthcare entity and background screenings may be required for those CSP personnel who will "touch" the ePHI in some form. • Varying forms of user authentication and authorization may be used to provide access to cloud based capabilities; the use of third party authentication based on a central Identity and Access Management system belonging to the healthcare organization is highly recommended. • It is important for the healthcare entities to be able to track the creation, modification and deletion of ePHI when it is stored and processed by a cloud service. • The movement of health-related data between devices, in-house HIT systems and cloud services must be done in a way that meets security and privacy requirements. • Refer to Step 4 in the Guidance section below for details on security and privacy considerations.
Regulation & Compliance	• Implementation of certain operational and control aspects of securing ePHI is done by the CSP; however, ultimate responsibility for compliance always resides with the healthcare entity. • Owners of ePHI must require CSPs to contractually agree to maintain all ePHI in adherence with government standards and regulations including HIPAA [4] and GDPR [6]. • It is common for CSPs offering healthcare cloud services to have certifications which can assure customers that the cloud services are operated in accordance with specific standards and/or regulations. Examples include HIPAA, ISO 27001, 27017 and 27018. • Healthcare entities must be aware of country-specific regulations associated with connected medical devices that require

	compliance from both medical device manufacturers and associated service providers including the U.S. Food & Drug Administration Medical Device Regulation [7] and Japan's Updated Pharmaceutical and Medical Device Act [8].
Service Reliability	● Key performance indicators associated with CSP reliability and performance must be defined and monitored on a regular basis. ● Disaster recovery is critical. Healthcare entities need to ensure that their cloud service agreements provide sufficient treatment of disaster recovery issues, procedures and processes (refer to Step 6 below for more detail). ● Change management is also important. The CSP's ability to perform system and software upgrades in a timely manner is critical (refer to Step 7 below for more detail).
Integration, Interoperability and Portability	● Delivering an end-to-end system that fully integrates all patient information, including emergency and inpatient care, pharmacies, billing, reimbursement, and more requires standardization and interoperability across cloud services and in-house HIT systems. ● Standards associated with HL7, for example, Fast Healthcare Interoperability Resources (FHIR) and the Continua Health Alliance can be of assistance in enabling data portability and interoperability of systems and devices (see Appendix A). ● The use of standard healthcare interfaces and data models facilitates migration to different cloud service providers. ● As part of the migration to use cloud services, healthcare entities must work with their CSP to ensure compatible business and operational processes, transparency, and smooth integration with existing enterprise systems.
Standards	● There are numerous standards that apply to different aspects of healthcare solutions; it is useful for customers to understand the available standards and to understand whether cloud services adhere to relevant standards for the capabilities provided. A list of the most important sets of standards is provided in Appendix A.

Table 1: Cloud computing considerations

Guidance for Leveraging Cloud Computing in Healthcare

This section provides a prescriptive series of steps that should be taken by cloud service customers to ensure successful deployment of cloud-based healthcare solutions. The following steps are discussed in detail:

1. Build the business case for cloud computing
2. Identify and prioritize specific cloud-based healthcare solutions
3. Determine the appropriate cloud deployment and service models
4. Ensure all security and privacy requirements are addressed
5. Integrate with existing enterprise systems
6. Negotiate cloud service agreements and monitor key performance indicators
7. Manage the cloud environment

Step 1: Build the Business Case for Cloud Computing

Many healthcare organizations, from clinics to hospitals to solution providers and insurance companies, have already embraced private cloud consumption models. Healthcare compliance and regulations have been updated to reflect the requirements of cloud computing. To meet this demand, many CSPs have moved rapidly to add HIPAA enabled offerings in accordance with the HITECH Act of 2009. [3]

As healthcare providers and suppliers seek to enable the digital enterprise, they are quickly realizing the potential benefits of cloud computing solutions to automate management and orchestration of virtual assets, provide 'built in' local/global disaster protection, deliver real-time business intelligence, and enable IoT augmented patient care, big data analytics, cognitive assistance to medical professionals, economies of scale, and flexible payment models.

Conventional wisdom says that the financial benefits of launching a cloud computing initiative can move costs from a capital expense (CAPEX) centric model to an operational expense (OPEX) centric model. While many healthcare organizations may prefer the OPEX model, some may opt to defer cloud services costs through a CAPEX financial model. As a result, many CSPs are offering reserved instances of services with an upfront financial commitment for a multi-year term. This flexibility enables each healthcare organization to optimize financial treatment of cloud services to meet their needs.

Between the digitalization of the enterprise and the prevalence of SaaS offerings that support the healthcare industry, many of the barriers to entry have disappeared. In addition to this reduced barrier to entry, greater value and improved cloud service agreements are now available. In fact, most CSPs are able to deliver significantly higher levels of service for application availability and disaster recovery for substantially lower costs than with on premises or co-located data centers. These benefits extend beyond cost and service level drivers to improved responsiveness with internal business partners and decreased administrative overhead.

Care must be taken to ensure that the best service category and deployment model are picked that fits the business objectives and goals.

The key dependencies to achieve all of these benefits are network connectivity and security. Whether you are ensuring insurance coverage for the public, developing the next generation of cancer drugs, or

providing critical care/tier I trauma services, the new emphasis is being put on providing network availability, performance and security. Although creating a highly available network might be expensive, those costs can be offset by the capabilities provided to the organization.

Cloud security continues to be a priority with many CSPs now offering government certified services through initiatives such as FedRAMP, FISMA and FIPS. Security systems, tools and software solutions are now available with full cloud integration and management. Many of these solutions were born on the cloud and provide everything from access control, authentication, firewall, encryption, intrusion detection, and monitoring services. Be sure to explore your provider's network and security services portfolio as you consider your next cloud solution. See Step 4 of this paper for detailed advice.

Finally, as part of your business case, it will be key to complete an application / workload assessment study to identify which applications and services should be migrated to cloud computing; determine which applications can be replaced with available cloud services and where entirely new capabilities can be provided by cloud services. Not every existing application can be migrated to cloud services. For example; hospitals may have applications like the nurse/doctor paging system, pneumatic tube system, seismic monitoring system, and others that must continue to be offered through a traditional private IT infrastructure. The implication is that some form of hybrid cloud solution is the most likely architecture for most healthcare organizations (Step 3 below provides more information).

Step 2: Identify and Prioritize Specific Cloud-based Healthcare Solutions

The financial benefits to launching a cloud computing initiative can often accrue significant business benefits. These benefits can include cost savings, however, this may take time to realize as there could be incremental up front investment required to make use of cloud services.

To fully capitalize on this shift to cloud computing, healthcare organizations 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 solution.

1. Avoid platform bias. This may seem obvious to some and unneeded to others. Regardless of which camp you are in, there are a number of factors that can quickly minimize the benefit of going to cloud. Be sure to align your effort with a person or organization that has been there before. In addition, try to leverage standards-based and open source-based services where possible to avoid platform bias.

2. Understand your current state. Determine what is appropriate to move to the cloud from three perspectives: infrastructure/platform, application, and operational capabilities.

3. Define your future state. Determine if you will be using SaaS applications or deploying your own applications using VMs or containers. Determine your network requirements. How will storage be handled? What resilience and disaster recovery capabilities are required? What DevOps capabilities are required? What orchestration and management facilities are necessary? Is a service catalog required?

4. Select your cloud service provider(s). Evaluate the TCO of viable CSPs. Select. Establish your business associate agreement (BAA) (or equivalent) if ePHI will be part of the cloud service. Negotiate your cloud service agreements per Step 6 below.

5. Plan a phased approach. How will entirely new applications be handled? What existing applications are candidates for early adoption? Is it best to build, migrate, replace or upgrade?

6. Establish a proof of concept. Create a test bed. Find a qualified cloud mentor to guide you through the strategic decisions. Work through the startup issues that arise in most migrations.

7. Scale to Production. Manage the introduction of new applications and migration of existing applications. Focus on the customer experience, analytics, preventative controls and optimization.

Potential Cloud Drivers and Use Cases

In addition to the standard cost incurred during the process of migrating to a successful cloud solution, there can be technical and organizational challenges as well as a significant learning curve. Simultaneously, the benefits can go well beyond reducing long-term IT and healthcare costs to increased revenue by providing differentiated services and increased patient satisfaction by better integrating healthcare and treatment into day to day life. Although this is not an exhaustive list, some of the potential use cases are listed below.

IT Cost Reduction: Reducing the cost to deliver services is a driver of IT modernization. This has never been truer than it is today. Example areas within healthcare enterprises that can greatly benefit from cloud computing technology are: Finance and Administration, IT Management, Application Development and Support, Data and Voice Networking, Service Desk, End User Computing, and Data Center.

Connected Healthcare: Connected healthcare is a model for healthcare delivery that uses technology to provide healthcare seamlessly across multiple providers. It can provide new and unique opportunities for patients to engage with medical staff to better manage their care. It also leverages emerging technologies to enable care outside of the physical hospital or doctor's office, through the ability for mobile and wearable devices to connect to cloud-based smart healthcare systems.

Big Data Analytics: The adoption of advanced healthcare 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 like genomic research can be securely shared among authorized health care industry organizations to provide access to potentially life-saving information and accelerate research and development.

Telemedicine: Telemedicine technology offers much promise for patients by bringing highly specialized and preventative medical advice to rural areas. Its biggest impact may be felt in parts of the developing world where healthcare services are equal parts scarce and inaccessible. Remote consultations can help address relatively minor conditions before they become major; treating cataracts before they cause blindness, for example, or ensuring that new mothers receive the educational resources they need to raise a child and take care of their own medical needs. Cloud computing is well suited to providing the connectivity channels required to support telemedicine, avoiding the need to install and support in-house what can be complex and specialized technologies. Additionally, for HIPPA compliance it is possible to handle the necessary recording and long-term storage via the cloud in a centralized way for geographically diverse organizations. EU and other local requirements are still under development in various countries.

IoT Enabled Health Care: With the plethora of new consumer wearable devices and application specific home health monitoring devices able to provide near-real time data, IoT enabled healthcare is becoming more and more appealing for patients of any age range. These devices can provide actionable vital sign data from a patient anywhere in the world to the hospital staff. It allows them to monitor a patient's health while giving the patient the flexibility to live their life. Cloud systems can make it straightforward to handle the connectivity requirements of IoT devices, from registration to support of IoT communication protocols and the management of device data.

Diagnostic Support: Services to assist in diagnosis are becoming a useful tool to guide medical practitioners, helping to reduce time spent and improving productivity. Increasingly, these cloud-based systems are gaining cognitive features, based on learning from the very large datasets of medical data available. These features enable clinicians to keep abreast of the latest research and most up-to-date information from colleagues around the world.

Application Development and Development Operations (DevOps): DevOps is a philosophy of shared responsibilities that when coupled with agile software development processes can lead to rapid development and reliable delivery of application services. DevOps endeavors to manage the process as an application moves from the innovation/development context to the mission critical operations context required to ensure consistent and reliable patient care. Cloud computing services are available to support DevOps activities, enabling greater productivity while reducing the skills required in-house.

Disaster Recovery as a Service (DRaaS): Healthcare systems can often be crucial to the provision of correct and timely health services to patients and to professionals. As a result, there is a need to ensure availability of these systems even in the face of IT failure. DRaaS means that organizations don't have to invest in or maintain their own disaster recovery environments. DRaaS contracts can be flexible and adapt to meet the changing needs of the business. This option requires a high level of trust in that the DRaaS provider can implement the plan in the event of a disaster and meet the defined recovery time and recovery point (RTO/RPO) objectives to ensure timely availability of the affected systems with minimal loss of data during an outage.

Backup as a Service (BaaS): Backup as a service (BaaS) is an approach to data backup and retention where the organization outsources their backup and recovery services to an online data backup cloud service provider. Usually part of a tiered retention model, it is easier to manage than many other onsite or offsite services. Care must be taken to ensure the recovery point and time objectives (RPO/RTO) can be met and emphasis placed on proving that full and complete backup sets are available and useable.

Step 3: Determine the Appropriate Cloud Deployment and Service Models

When deciding to deploy a particular workload to the cloud, healthcare organizations must take into account a number of factors to determine the most appropriate deployment model (public, dedicated, private or hybrid).

Public cloud deployment is where the cloud service is run on data center resources belonging to a cloud service provider and resources are shared amongst many different cloud service customers. The environment is termed multi-tenant. Dedicated cloud deployment is where the cloud service is run on data center resources belonging to a cloud service provider, and those resources are used by a single

customer and not shared with any other customers. The environment is termed single-tenant. Private cloud deployment is where the cloud service is run on data center resources belonging to the cloud service customer, typically on-premises and run and controlled by the customer. Dedicated cloud deployment is often regarded as a form of private cloud deployment due to the isolation provided to the customer's applications and data. Hybrid cloud deployment is where cloud services using multiple deployment models are used together, often in combination with non-cloud resources of the cloud service customer.

Factors that influence the choice of deployment models include:

- *Security*. IT security (confidentiality/privacy, integrity, and availability) is a crucial factor that influences the selection of the appropriate deployment model. Security considers the level of control and compliance regulation the healthcare organization requires with regards to governance, data privacy and patient data. For example, with public cloud, there is a relinquishing of control to the cloud provider. In addition, public cloud services are typically multi-tenant. HCOs assume greater responsibility and control of the security environment for private cloud. Obstacles with regards to security can be avoided in a private cloud, but in case of natural disaster and internal data theft the private cloud may be prone to vulnerabilities, in a similar way to on-premises non-cloud systems. Healthcare workloads that are critical or sensitive may be better deployed on a private or a dedicated cloud. Alternatively, such workloads could be placed onto cloud services that are certified to meet standards and regulations which apply to such workloads.
- *Data Classification* (including privacy and locality requirements). The sensitivity of data and the criticality of data are significant factors to be considered in selecting the appropriate cloud deployment model. It is difficult to envision all potential threats and risk to the organization's data, hence workloads with sensitive data may be more appropriate for private cloud deployment. Dedicated cloud deployment can be considered if the necessary controls to protect the data are in place and are proven to work effectively. Private cloud deployment may be more acceptable as they give the organization greater and direct control over their data, but only if the on-premises deployment is actually more secure than deployment to provider infrastructure. If the data in question is non-sensitive and non-critical, then public cloud deployment is appropriate.
- *Business Model*. An important consideration is the place of the workload in the business model. One perspective is the shift from a volume-based model to a value-based model. This is causing innovative providers to redesign their models which provide opportunities to consider cloud computing as a deployment model for the changing consumer landscape. If the workload is a critical business process, then private cloud deployment or dedicated cloud deployment might be more appropriate, although public cloud service with high availability options might also be suitable – indeed possibly more suitable than deployment to a vulnerable on-premises datacenter. In addition, it is important to consider how mature the business model and processes are, as this will help ascertain the predictable nature of the capacity and whether there are fluctuations that need to be understood. This will consequently impact SLAs and capacity requirements.

- *Target Operating Model*. In addition to the technical architecture considerations that HCOs need to consider, there is a broader range of characteristics that demand a different target operating model (TOM) to support the cloud deployment model. As *bobsguide* states: "It requires new people (or at least skills, with more of a service centric approach), governance (one example being a greater focus on vendor management), processes (traditional IT organizations differ from cloud service providers), tools (particularly with regards to service integration and monitoring), and controls (with careful consideration to all aspects of information security)." [9] Where the HCO has a low level of the necessary skills, public deployment or at a minimum a hybrid cloud may be more appropriate.
- *Application Architecture*. To meet the changing needs of their various users, healthcare providers need to rapidly provide flexible technology systems and business processes. This demands a transformation of their architecture from primarily legacy systems to modern platforms. A hybrid cloud deployment model may be the best option. Typically, in most healthcare organizations, there is substantial legacy IT, so a 2-Speed IT architecture using hybrid cloud deployment may be the best fit. Refer to the CSCC's *Practical Guide to Hybrid Cloud Computing* [17] for more details.
- *Cost*. Cost is always a big driver in deciding what deployment model to select. Organizations need to consider the cost effectiveness of the deployment model and the ability to quickly adapt to changing scenarios. Typically, public cloud deployment is more economical compared with private and dedicated cloud deployment. However, it is important that cost measurements are not just limited to TCO but also include reputational cost and risk if the right security or data controls are not put in place. So there may be cases where cloud computing is not the answer.
- *Performance*. Private cloud deployment might be the best option if there is a requirement for high data I/O and low network latency between the applications and end users and internet access cannot provide the right level of network performance. Where a workload has unpredictable growth, public cloud might be more suitable as it is easier to scale up and scale down. Typically, private cloud deployment might be a better fit for consistent 24×7 workloads, whereas public cloud's attractive per hour billing model will suit temporary workloads, seasonal or spiky traffic.

Most healthcare deployments are likely to be hybrid (i.e., a mix of private and public) given the specific requirements and benefits of different types of workloads. Some will lend themselves to public cloud resulting in cost savings or access to innovative capabilities; others will require private cloud (due to security sensitive data, etc.). In addition, there will be scenarios where prototyping is carried out on a public cloud and then the production application deployed on a private or dedicated cloud system. For hybrid environments where healthcare data exchange will take place between CSPs in different geographies, regulations must be followed and security policies will be required to safeguard sensitive information – these policies must be monitored and enforced.

The cloud service model selected by an HCO depends mainly on existing in-house solutions and IT skills. In cases where an in-house healthcare service does not exist and IT skills are limited, a Software-as-a-Service (SaaS) offering will be preferred. Many of the high value healthcare services highlighted earlier in

this document are provided as SaaS offerings requiring minimal technical support from the acquiring HCO. In cases where in-house IT skills are available, Platform-as-a-Service (PaaS) offerings are an option allowing HCOs to quickly acquire new healthcare services and, at the same time, provide the ability to extend and enhance these services to satisfy unique requirements. In cases where an HCO is simply looking for additional storage and compute capacity to support existing in-house healthcare solutions, Infrastructure-as-a-Service (IaaS) offerings provide a cost effective alternative.

Step 4: Ensure All Security and Privacy Requirements are Addressed

Security and data protection issues are of vital importance in the adoption of any IT-based healthcare solution. Not only must the appropriate security be implemented for the cloud solution but it must also be built into the underlying cloud service monitoring and management processes.

One of the key differences between cloud services and traditional IT is the concept of shared responsibility. In traditional IT, the IT organization is responsible for almost everything. With cloud services, responsibility is shared between the cloud service provider and the healthcare organization as cloud service customer. The customer's responsibility will vary, depending upon the service model and the particular service. The division of roles and responsibilities relating to security and data protection requirements between the cloud service provider and the customer organization and its end users must be well understood. The well-documented recommendations found in the CSCC*'s Security for Cloud Computing: 10 Steps to Ensure Success, Version 2.0* [10], NIST 800-160 [11], Cloud Security Alliance [12], ISO/IEC 27017 [13], and ISO/IEC 27018 [14] papers and standards should be followed.

There are regulations in many countries that govern the privacy and security of healthcare data. HIPAA (USA) and GDPR (EU) are two examples, and these impose certain obligations on anyone who stores or processes certain healthcare data. This healthcare data is labeled ePHI by HIPAA. All of these obligations must be met by the cloud service customer, the cloud service providers, or some combination thereof. HIPAA is discussed in more detail in Appendix B while the GDPR is discussed in more detail in Appendix C.

The requirements are broken down into physical, administrative, and technical safeguards. Physical safeguards are extremely important, but almost all cloud providers have sufficient facility access controls to meet the requirements, although this must be validated. Physical workstation and device media controls are generally the same in both cloud and traditional environments. Mobile devices are a particular challenge, both IoT devices associated with patients and also medical practitioner devices such as tablets and mobile phones – however, many cloud service providers have facilities which help deal with the security challenges of such devices. Likewise, the administrative controls are similar in both cloud and traditional deployments, although both the cloud customer and the cloud provider must meet the administrative requirements. The healthcare organization's systems are likely to need extending or upgrading to deal with the security and privacy issues related to using cloud services.

For technical controls, it's important to ensure that the cloud provider encrypts protected health information in transit and at rest. The encryption controls must manage the keys properly, and must use standard (not custom) implementations of secure algorithms. NIST 800-131A R1 [15] and FIPS 140-2 Annex A [16] are good references for determining acceptable encryption algorithms. In addition to

keeping the data confidential and preventing tampering, encryption may also be used to securely render data unreadable if the cloud customer has control over the encryption keys, which may be marketed as "enterprise key management."

Authentication is an essential feature of systems dealing with healthcare information; unauthorized access is a major problem. Authentication and authorization is made more complex by hybrid cloud solutions, where there are multiple systems involved, each of which must employ authentication. The use of third party authentication based on a central Identity and Access Management system belonging to the healthcare organization is highly recommended; support for this should be required of any cloud service that is used. While two factor authentication is not explicitly required by HIPAA, it is strongly recommended whenever protected health information is accessed by a person, especially if this access is over an unsecured network like the Internet. Two factor authentication systems are now standardized and affordable, and are commonly used by web sites today, so there is little excuse for a new implementation to not support its use.

Organizations need to manage both the logical and physical security of their infrastructure carefully, taking into consideration everything that could happen throughout the lifecycle of ePHI. The US HIPAA HITECH Act presents one of the better ways to support the exchange of ePHI, built on a HIPAA baseline.

In addition to proper controls, one of the simplest ways to avoid ePHI data loss is to not store it in any system unless absolutely necessary. Do not collect ePHI unnecessarily, do not allow it to spread to systems where it's not required, and securely dispose of it when it is no longer needed.

A final issue which presents a challenge to healthcare IT systems is the need to provide access for patients to their ePHI; regulations often give the right to patients to have this access, for example the GDPR. There is the challenge of providing a suitable user interface to patients, especially where ePHI may be spread over multiple applications and systems. There is also the serious security challenge of authenticating the patient so that it is assured that only the patient gets to see their own data.

Step 5: Integrate with Existing Enterprise Systems

New cloud deployments present health care organizations with a diverse array of enterprise integration challenges. This step is intended to identify integration tasks and challenges that arise at different phases of cloud deployment and in subsequent IT operations. Beyond one-off migration staging, which could be vendor-assisted, this step can become quite involved, depending on many factors.

Hybrid Cloud: As described in the CSCC's *Practical Guide to Hybrid Cloud Computing* [17], hybrid cloud implementations entail "interlinking cloud-deployed applications and data with traditional non-cloud enterprise applications." An illustrative scenario could involve a multi-hospital operation which chooses to retain on-premises EHR for inpatient operations, but wants to leverage public cloud services for geographically distributed outpatient clinics. Organizations that seek to track patients across inpatient and outpatient facilities face some integration requirements.

Identity and Access Management: Certain healthcare providers and staff will require access to both applications and data deployed on cloud systems as well as traditional applications. Identity and access management, such as through LDAP and Active Directory, must be extended to include cloud services.

IT Administration and Management: Healthcare organizations will need to develop expertise in managing cloud systems along with their traditional facilities. Some existing tools can be extended to encompass cloud systems, but some organizations may need to implement new processes and/or tools. Operational intelligence, security, and capacity management are all likely to be affected, as well as IT and developer staff training.

Medical Device IoT: The Internet of Things and wearable devices are creating new streaming data sources, many of which are best serviced through cloud deployed services. “Designing methods for streaming data capture, real-time data aggregation, machine learning, predictive analytics and visualization solutions to integrate wellness or health monitoring data elements with the electronic medical records (EMRs) maintained by health care providers permits better utilization,” researchers say. [18] Device IoT will often entail hybrid solutions.

Advanced Analytics: Research institutions as well as healthcare organizations are likely to seek cloud services to fulfill needs for advanced analytics. For instance, a US Veterans Affairs health application “distributes data, metadata and compute jobs across on-premises and remote resources” to leverage a genotype-phenotype graphic analysis engine. [19] Such integrations are likely to require a measure of customization.

Telemedicine: Adoption of cloud services in healthcare may be driven by the need to expand telemedicine offerings – not only for medical but also for pharmacy services. These services typically require expanded network infrastructure and integration with traditional “examining room” oriented applications. Telemedicine is cited as an accelerator for right-provider, right-time, right-place medicine [20], resulting in reduced waste and duplication of effort, but requires coordination with traditional systems – including staff training and updated business processes and medical procedures.

Standards Conformance: A number of private and public organizations have developed or are developing health information standards. Conformance with these standards may require integration between cloud services and other applications, such as through third party APIs, middleware or other approaches. A significant effort by the Office of the National Coordinator for Health Information Technology (ONC) manages a non-binding Interoperability Standards Advisory (ISA) process to ”. . . coordinate the identification, assessment, and public awareness of interoperability standards and implementation specifications that can be used by industry to fulfill specific clinical health IT interoperability needs.” [21]

Audit, Compliance and Operational Intelligence: Maintaining compliance with HIPAA and other regulations will require specific additional auditing. (Some cloud providers in the broader marketplace specifically exclude patient information in their terms of service.) For example, organizations may need to extend cloud software to comply with HL7 guidelines such as PASS [22].

Middleware: Organizations which have adopted enterprise service bus or SOA approaches to service implementations will want to examine how these tools can support cloud services. In addition, new approaches to cloud should be considered, such as mobile cloud middleware frameworks. [23]

Step 6: Negotiate Cloud Service Agreements and Monitor Key Performance Indicators

A healthcare organization's cloud strategy can be crafted in such a way to illustrate the immediate productivity gains and/or cost reductions at the same time promoting an approach to leverage metrics to show ongoing value or the need to modify technologies to meet new market requirements. This involves a continual examination and monitoring of the key technology factors in the context of the healthcare organization's 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.

This plan typically begins with comparisons of the organization specific business process metrics (KPIs), their internal or other traditional IT KPIs and other possibly non-IT methods (e.g., paper based EMR, current imagery scan retrieval) compared to the improvements expected of the target cloud-based solutions. These 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 the cloud computing solutions and service delivery. Some of these are contractual matters as defined in cloud service agreements (CSAs) with the cloud service provider and may or may not be negotiable. Although IT metrics are important, the KPIs that generally support the adoption of a specific vendor or solution are usually business-centric and focus on such things as patient care quality or time to process records, reports, etc.

The CSCC*'s Practical Guide to Cloud Service Agreements* [5] summarizes the primary considerations for performance metrics in cloud service agreements as:

- Understand the business level performance objectives (for example, reduce cost and time to market per unit of software functionality).
- Identify the metrics that are critical to achieving and managing the business level performance objectives.
- Ensure these metrics are defined at the right level of granularity that can be monitored on a continuous basis (in a cost-effective manner).
- Identify standards that provide consistency in metric definitions and methods of collection.
- Analyze and leverage the metrics on an ongoing basis as a tool for influencing business decisions.

The introduction of cloud services, especially those supporting mobile and internet of things (IoT) applications opens up new opportunities for measurement and the introduction of new KPIs. For example, where a wearable device is used to measure certain vital parameters of a patient, the time taken to react to out-of-normal measurements might be a new KPI. The advent of commonly used social media can also imply new measurements and KPIs. Medical centers and physician groups might want to keep track of positive and negative media mentions and consumer sentiment as they relate to public health issues, and then also measure how quickly they are able to respond to sentiment through their own communication channels. Patient wait times, examining room usage, bed and room turnover,

claim processing time are all metrics that matter to patient satisfaction and operational effectiveness. New streams of information may, over time, allow the provider organization to come up with very specific means to measure operational effectiveness through better visibility into inpatient flow, revenue cycles and patient feedback loops built into the care process.

In recent years, there has been wider adoption of cloud service solutions by healthcare organizations with careful consideration for compliance and risk weighed against potential cost-savings and productivity gains. There has also been a strong movement towards the creation of shared services whereby a healthcare parent company consists of two entities: one a provider of traditional healthcare services, the other a provider of cloud services to multiple healthcare organizations.

The CSCC papers *Practical Guide to Cloud Service Agreements* [5] and *Public Cloud Service Agreements: What to Expect and What to Negotiate [24]* offer a vendor neutral foundation for healthcare organizations to define KPIs and agree on necessary service levels from the perspective of the cloud service customer. It is likely that some readers of this paper will be considering SLAs and negotiations from the viewpoint of a service provider. The advice and guidance offered to customers is also a good foundation for healthcare CSPs to consider the structure of their cloud service agreements and terms of service.

When using a cloud service, it is necessary for the customer to understand whether disaster recovery is provided by the CSP (usually at some cost to the customer) or whether disaster recovery processes must be built by the customer. 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 is acceptable before there is a significant business impact. In cases where the CSP does not provide disaster recovery directly, the CSP may provide advice to the customer on how they can organize disaster recovery, for example, by having standby instances of applications and data hosted in separate backup cloud data centers.

As for any well-established industry with strict compliance oversight, the likelihood of a healthcare organization adopting a hybrid architecture is high. The hybrid environment requires measurement and monitoring beyond the fundamental indicators. To better define the service levels and terms of service for connectivity, change notification and other operational support from the CSP the CSCC's *Practical Guide to Hybrid Cloud Computing* [17] can assist in assessing all the process and integration touch points that could or should be covered by cloud service agreements and monitored as a KPI. Figure 1 shows the Service Responsibility Line for different categories of cloud service; typically everything above is the responsibility of the customer, below the responsibility of the cloud service provider. In some hybrid architectures this line may be in different places for the different cloud services used and it is essential to keep these areas documented and monitored.

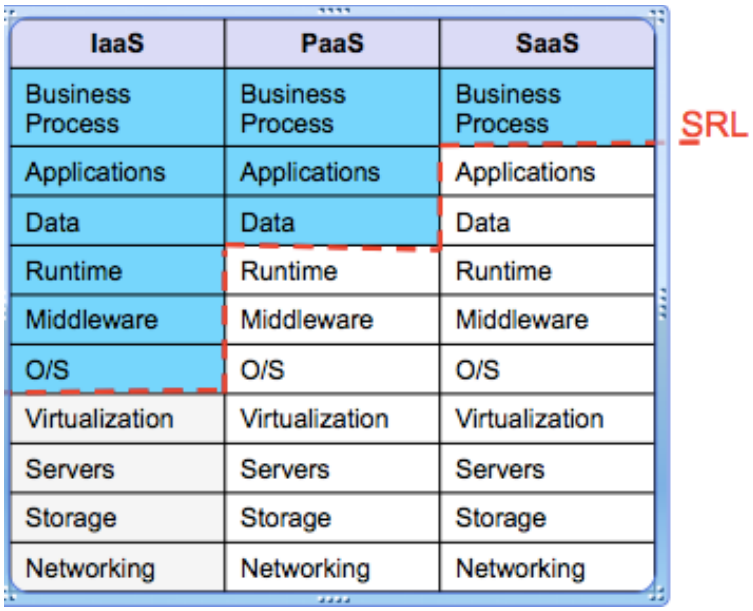

Figure 1: Service Responsibility Line for Different Cloud Service Models

Step 7: Manage the Cloud Environment

Management of cloud environments is similar to managing traditional IT environments, except that it must be done across the boundary between the cloud service customer and the cloud service provider. The traditional management parameters for IT environments such as cost (CapEx, OpEx), support, service management, security, efficiency, staffing are all valid for the management of cloud environments. There are however a few leading edge aspects of IT which may pose a particular challenge in a cloud setting. These include management of electronic health records (including sharing), automation of internet connected devices with real time data (IoT), field devices (including physician/nurse's tablet for capturing or displaying data), intelligent cognitive assistants (physician assistant), etc.

Electronic Health Records

EHR is now used to a certain degree in various parts of the world and there is a general movement towards adopting them. The following characteristics of EHRs pose specific management concerns in a hybrid cloud environment:

1. Retrieving and transmitting health data for patients to/from external sources which have security, privacy and provenance issues.
2. Managing the privacy and security of patient health data generally.
3. Ensuring availability of patient health data.
4. Ensuring timely synchronization of patient health data

All of these concerns listed above, require the cloud environment to be supportive of the specific function listed. Systems need to be available, connected, secured and appropriately monitored and logged for proper implementation of regulatory, compliance and internal security and privacy controls.

Specific controls are typically required by the relevant regulatory regime which is applicable, such as HIPAA in the USA.

Internet of Things

Patients equipped with connected devices for automated monitoring require unique cloud service management support. These healthcare devices support a wide range of capabilities including:

1. Fall detection for elderly patients
2. Health monitoring for patients with chronic disorders such as diabetes and heart disease
3. Detection of escalating symptoms for patients with mental disorders (such as Alzheimer's, schizophrenia, etc.)

Devices of these types are typically connected to the internet and are capable of notifying / alerting a designated health care service center with data and other pertinent incident information. This will require the cloud environment to address systems availability, connectivity, privacy and security. The security challenge of any device connected to the internet is of particular concern and care must be taken to secure the endpoints concerned and ensure confidentiality of the patient information transmitted. Use of more specialized transmission protocols such as MQTT may be advisable, along with encryption of the data traffic.

Field Devices

These devices (usually PDAs, tablets, laptops, etc.) are used by healthcare staff to retrieve and record patient data on the spot. These devices require an asynchronous data upload mechanism in order to prevent data loss and keep the global EHR repository updated. Here are a few management considerations that need to be addressed for these devices (refer to FDA guidelines [7] for more information):

- Protect device and network resources against interruption and suspended services caused by attacks on hospital or device manufacturer's web servers, when the flow of external communication requests will obstruct and not allow responses to legitimate service requests.
- Regularly update medical devices and network software. It is crucial to establish a trusted maintenance ecosystem, setting up access with maintenance and support services.
- Provide security protection for Android devices and applications that utilize weak passwords, creating an easy access path for hackers to steal broadband signals and abuse VPN connections. There is no hardware data encryption on Android devices so there is greater risk personally identifiable data that may be stored on the device.
- Set up secure communications through a variety of networking mechanisms. Communication paths between devices and systems must be secured. In both HTTP-based and event-based models, the use of SSL/TLS to set up protected communications is pervasive. Provide strong cryptographic algorithms to establish a secure communications channel ; this allows most of the logic that is running on devices, in gateways, and in cloud-hosted systems to assume a secure communications channel, and to focus on providing the capability of the device or application.

Intelligent Automated Assistance

Physicians, nurses and other healthcare providers are able to use any number of cognitive solutions that help analyze vast amount of anonymous data from global sources, correlate against any specific data flagged on the patient, and provide assistance in decision making to the service provider. This would only be possible in the case of cloud connected systems. It is also expected that such a system would generally require internet access (i.e., cloud delivered) and therefore require applicability of all cloud management principles.

Systems Maintenance

Maintenance of information systems applies to cloud services as it does to in-house systems, with the difference that some aspects of the cloud service environment are the responsibility of the cloud service provider, as indicated in Figure 1 above.

It is necessary for the cloud service customer to have assurance about the cloud vendor's capacity for:

1. Patching of software and systems to deal with known issues in a timely manner, particularly critical security vulnerabilities.
2. Maintenance and tuning, such as database indexing and cache resets.
3. System updates, particularly of vendor generated updates.
4. System upgrades, including moving to newer versions of software with added features and functionality.
5. Synchronizing maintenance activities with the cloud service customer's IT management plan, typically through a system of notifications.
6. Ensuring availability and performance service level objectives (SLOs) are met even during maintenance cycles.

HCOs must ensure that the SLA is met for each cloud service, while keeping in mind the criticality of certain service level objectives and the consequences of failure to meet those objectives. For many cloud services, the onus is on the cloud service customer to detect if the SLOs are not satisfied and to demand action on the part of the cloud service provider to rectify the situation. Refer to Step 6 above for more details.

Conclusion

Adoption of cloud computing in the healthcare industry will continue to evolve and accelerate in the coming years. Expanding usage of healthcare IoT devices and the need to store and analyze vast amounts of healthcare information to deliver both personal and population health management services necessitates the need for cloud computing from both a business and technology perspective.

Added to this are the increasingly sophisticated and wide ranging healthcare cloud service offerings available in the marketplace, which healthcare providers might struggle to reproduce as in-house applications. Cloud computing facilitates the application of technologies like big data analytics, cognitive computing, mobile collaboration and information exchange to accelerate the delivery of advanced healthcare solutions.

In support of expanding healthcare market requirements, hybrid cloud deployments will be prevalent since this model offers healthcare providers the flexibility to deploy workloads and data based on business related risk/reward analysis. Security and privacy requirements along with regulation compliance will be key determining factors in hybrid cloud deployment decisions. Hybrid cloud environments will increase the importance of integration and provide challenges to healthcare providers as they negotiate CSAs from different cloud service providers.

The challenges with cloud-based healthcare solutions persist for many healthcare providers, however, the benefits of cloud computing are too compelling to ignore. Healthcare providers are advised to develop a cloud computing business strategy immediately if they have not done so already.

Appendix A: Healthcare Standards

There are a variety of standards and best practices available which apply to specific aspects of healthcare IT and can be useful when considering the use of specific cloud services. Cloud services which support relevant standards should offer a better level of interoperability:

- Continua Health Alliance
  http://www.pchalliance.org/continua/
  An industry consortium producing design guidelines for interoperable personal connected health devices and systems
  http://www.pchalliance.org/continua/products/design-guidelines
  List of certified products:
  http://www.pchalliance.org/continua/products/product-showcase
- ISO TC215
  http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=54960
  ISO/IEEE 11073 series of standards
  cover Personal Health Devices – e.g. ISO/IEEE 11073
  Health Data exchange – e.g. ISO/HL7 27932
  Security for Health informatics – e.g. ISO 27799:2016
- Health Level Seven (HL7)
  http://www.hl7.org/
  Electronic Health Information exchange standards
  - Clinical Document Architecture (CDA) – ISO 27932:2009
  - Fast Healthcare Interoperability Resources (FHIR)
- Healthcare Information and Management Systems Society (HIMSS)
  https://www.himss.org/
  - Health Information Exchange
  - Privacy & Security for RHIOs/HIEs
- Healthcare Information Technology Standards Panel (HITSP)
  http://www.hitsp.org/

- Interoperability specifications
- USA oriented

- CEN TC 251 – Health Informatics
https://standards.cen.eu/dyn/www/f?p=204:32:0::::FSP_ORG_ID,FSP_LANG_ID:6232,25&cs=1FFF281A84075B985DD039F95A2CAB820
- European oriented
- Health record interchange

Appendix B: HIPAA Privacy and Security Legislation

In the United States, every healthcare entity (e.g., hospital, university research facility, physician's office) that deals with PHI must adhere to the guidelines stipulated by HIPAA [4]**.** 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 HIPAA, most of a patient's medical record and payment history are considered PHI, and are 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 particularly managing PHI in a way that is sufficiently simple to enable use by the general public.

The healthcare entity that owns the PHI ("covered entity") must require the CSP, a.k.a. the "business associate," to agree contractually to maintain all PHI in compliance with HIPAA standards. While ultimate responsibility for compliance always resides with the covered entity, responsibility for implementation of various operational and control aspects of protecting the data extends to the business associate, which for this situation includes the CSP.

From a legal perspective, business associates have certain privacy and security requirements that other generic "third party" entities do not. This is a nebulous area and open for interpretation, with no consensus established. It is the responsibility of the CSP to obtain 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 have a detailed cloud service agreement (CSA) with the CSP to understand fully their responsibilities, exposures and risks, as well as being able to absorb the financial and other impacts in the event of HIPAA non-compliance.

Under the HIPAA Security Rule, there are a number of considerations to be taken into account such as administrative, physical, and technical exposures. State-of-the-art encryption technologies can protect IIHI and PHI in the manner required to meet stringent HIPAA and other regulatory requirements, even when IIHI- and PHI-related IT applications are sharing physical and virtual infrastructure with less sensitive resources.

Another critical component that is required to meet HIPAA regulations is the process of correctly identifying and authenticating users, together 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.

For more detailed information on HIPAA please refer to the Health and Human Services web site and to the HIPAA Survival Guide [4].

Appendix C: EU Data Privacy Legislation

Currently, the governments of many countries in the mature markets are 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 Union (EU) 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 service customer should be considered as the data controller while the CSP acts as the data processor, except when the CSP processes the personal data for its own purposes. One effect of that definition is that the applicable law usually is the legislation of the country in which the cloud service customer is established, rather than the place where the CSP is located.

Although the EU Commission's standard contractual clauses offer adequate safeguards, they do not apply to a situation in which the CSP, 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.

In 2016, the EU passed into law the General Data Protection Regulation (GDPR) [6], which addresses the handling of personal data of EU citizens in two broad areas – the protection of personal data and the free movement of that data within the borders of the EU. Healthcare data is specifically addressed in the GDPR. Healthcare data in general is treated as personal data and requires the security and privacy protection that applies to all personal data.

One feature of the GDPR is that consent is required from the "data subject" (the person to whom the personal data relates) for the collection and processing of any personal data – and that this must be informed consent where the details of the purposes of collection and processing are spelled out. A parallel feature of the GDPR is that the data subject has a right of access to their personal data, and this right explicitly covers personal health data: "*This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided*" (GDPR clause 63 [6]).

The right of access has implications for IT systems, since the data subject should be able to access their health data electronically: "*Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data*" (GDPR clause 63 [6]).

There are specific powers regarding the use of personal health information by public authorities for the purposes of public health (e.g., dealing with epidemics), where the information can be used without the consent of the data subject, but these are exceptional cases.

The "free movement of data" principle in the GDPR also has significant consequences for healthcare organizations. Each data subject / patient has a right to data portability – the capability to obtain all their personal data in a commonly used electronic format and to move it elsewhere – for example, to a different healthcare organization. This right imposes a requirement on the IT systems of healthcare organizations to be able to identify and retrieve all the personal health information of a particular patient and make it available in a suitable format. Equally, the IT systems should be able to accept patient information coming from another healthcare provider in an electronic format.

The EU GDPR applies to the countries of the European Union, but applies to organizations, including CSPs, who are based or operate outside the EU, where the personal data concerned relates to citizens of the EU. Healthcare providers need to obtain assurance that any cloud service that they use conforms to the requirements of the GDPR; explicit statements are required in the CSA.

The situation in a EU country is more complex in that there may also be specific local laws and regulations relating to health data that go beyond the provisions of the GDPR. An example is the UK, where there is a country-specific Data Protection Act [25] with some provisions for the handling of health data [26].

References

[1] IHS 2016 Update: The Complexities of Physician Supply and Demand: Projections from 2014 to 2025 https://www.aamc.org/download/458082/data/2016_complexities_of_supply_and_demand_projections.pdf

[2] Mckinsey & Company (August, 2016): How tech-enabled consumers are reordering the healthcare landscape. http://healthcare.mckinsey.com/how-tech-enabled-consumers-are-reordering-healthcare-landscape

[3] Search Health IT: HITECH Act http://searchhealthit.techtarget.com/definition/HITECH-Act

[4] HIPAA http://www.hhs.gov/hipaa/

[5] Cloud Standards Customer Council 2015, *Practical Guide to Cloud Service Level Agreements, Version 2.0.* http://www.cloud-council.org/deliverables/practical-guide-to-cloud-service-agreements.htm

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council (2016): EU General Data Protection Regulation. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[7] U.S. Food & Drug Administration Medical Device Regulation http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/

[8] Japan's Updated Pharmaceutical and Medical Device Act https://www.pmda.go.jp/english/

[9] bobsguide: Cloud Target Operating Model: Revolution, Evolution or a Bit of Both? http://www.bobsguide.com/guide/news/2015/Sep/25/cloud-target-operating-model-tom-revolution-evolution-or-a-bit-of-both/

[10] Cloud Standards Customer Council 2015, *Security for Cloud Computing: 10 Steps to Ensure Success, Version 2.0.* http://www.cloud-council.org/deliverables/security-for-cloud-computing-10-steps-to-ensure-success.htm

[11] NIST 800-160 http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf

[12] Cloud Security Alliance https://cloudsecurityalliance.org/group/security-guidance/

[13] ISO/IEC 27017 (2015). Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services. http://www.iso.org/iso/catalogue_detail?csnumber=43757

[14] ISO/IEC 27018 (2014). Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498

[15] NIST 800-131 A http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf

[16] FIPS 140-2 Annex A http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf

[17] Cloud Standards Customer Council 2016, *Practical Guide to Hybrid Cloud Computing*. http://www.cloud-council.org/deliverables/practical-guide-to-hybrid-cloud-computing.htm

[18] K. Shameer, M. Badgeley, R. Miotto, B. Glicksberg, J. Morgan, and J. Dudley, "Translational bioinformatics in the era of real-time biomedical, healthcare and wellness data streams," Brief. Bioinform, p. bbv118, Feb. 2016 http://dx.doi.org/10.1093/bib/bbv118

[19] D. Major, "Million Veteran Program signs up bio analysis firm for hybrid cloud," GCN, Apr. 2016. https://gcn.com/articles/2016/04/15/mvp-cloud.aspx

[20] K. Terry, "Why Telemedicine Should Be Integrated With EHRs, ACOs," Inf. Week, 2013. http://www.informationweek.com/interoperability/why-telemedicine-should-be-integrated-with-ehrs-acos/d/d-id/1109882?

[21] T. Office_of_the_National_Coordinator_for_Health_I, Ed., “Draft 2017 Interoperability Standards Advisory,” CMS, Washington DC, RPRT, Aug. 2016. https://www.healthit.gov/sites/default/files/2017_draft_interoperability_standards_advisory_8.16.16.pdf

[22] D. Proud-Madruga, “Project Summary for Privacy, Access and Security Services (PASS) Healthcare Audit Services Conceptual Model.” HL7, Ann Arbor, MI OR - HL7, 09-May-2016. https://www.hl7.org/special/Committees/projman/searchableProjectIndex.cfm?action=edit&ProjectNumber=1264

[23] H. Flores and S. Srirama, “Mobile Cloud Middleware,” J. Syst. Softw., Sep. 2013 http://dx.doi.org/10.1016/j.jss.2013.09.012

[24] Cloud Standards Customer Council 2016, *Public Cloud Service Agreements: What to Expect and What to Negotiate*, *Version 2.0*. http://www.cloud-council.org/deliverables/public-cloud-service-agreements-what-to-expect-and-what-to-negotiate.htm

[25] UK Government 1998: Data Protection Act https://www.gov.uk/data-protection/the-data-protection-act

[26] UK Information Commissioners Office (undated): Guidance for Health Organizations https://ico.org.uk/for-organisations/health/

[27] ONC Health IT Certification Program https://www.healthit.gov/policy-researchers-implementers/about-onc-health-it-certification-program

Acknowledgements

The major contributors to this whitepaper are: John Barton (Pillsbury Law), Frank Chin (*i*TGRC Asia Advisory and Consulting), Chris Dotson (IBM), Mike Edwards (IBM), Melvin Greer (Intel), Elizabeth Koumpan (IBM), John Meegan (IBM), Peter Melrose (Independent IT consultant for Healthcare), Rahat Mujib (IBM), Osakpamwan Osaigbovo (IBM), Bill Parker (Presidio), John Sanders (CIO Management Group, Inc.), Karolyn Schalk (IBM), Karl Scott (Satori Consulting), Joel Thimsen (Perficient) and Mark Underwood (Krypton Brothers).