Delivering a Secure Cloud based Solution Model for Small Physician Practitioners Practice Management System

UIC
Daniel Addison

University of Illinois at Chicago

College of Applied Health Sciences

The Department of Biomedical and Health Information Sciences (BHIS)

Capstone Project

By

Daniel Addison

UIN 676885989

In partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

IN

HEALTH INFORMATICS

May 6, 2015

Contents

Abstract

Healthcare providers need information technology solutions that can provide the maximum security required, and integration and interoperability of its healthcare information systems like the practice management (PM) system. The significant financial cost of implementing, maintaining, and having inadequate resources to support an in-house traditional information technology paradigm has cause healthcare providers to evaluate, invest, and embark on advanced technologies like the secure Cloud bases services for its medical practices. Over the past decade, practices have been interested in the evolution of Cloud based computing services because of its flexibility, security, and scalability. In addition, the health information exchange (HIE) groups facilitated the need for practices to integrate practice management systems with clinical information systems to improve exchanging workflow processes pertinent for better care coordination. It is claimed that a secure Cloud based service model can provide effective and efficient security needed for a small physician practice to meet the meaningful use (MU) stage requirements, and stay in compliance with the Health Insurance Portability Accountability Act (HIPAA) of regulations and standards.

For practitioners to better streamline their clinical workflow processes and easily manage clinical user access with security and flexibility, the selection of a secure Cloud based service solution seems to be the appropriate choice for them to attain these specific objectives. However, transitioning to the secure cloud based solution model from a privacy and security perspective present some challenges for small physician practitioners and healthcare organizations. Going forward, this document will discuss the secure Cloud based services reliability, compliance with healthcare regulation and legislation, technology, and organizational factors for small physician practices to adopt.

Keywords: Cloud-based Practice Management application, ISO, HIPAA, MU, SECaaS, ICD-10

1. Introduction

Independent and small physician practices are faced with growing volumes of patient data. Therefore, securing and storing the confidentiality, integrity, and availability (CIA) for protection of patient data is very important for healthcare provider medical offices. The traditional practice management (PM) systems used by physicians in-housed of their practices are not robust enough to securely handle such large volumes of patient protected health informational data. Cloud computing technology has been emerging as the solution for small physician practices to handle such large volumes because it enables cost savings and improved productivity of healthcare applications residing in the cloud.

Healthcare practitioners naturally have different clinical and administrative workflow tasks. So, a secure Cloud base service provider must make sure its systems have easy-to-use secure interfaces and uniformity that will allow healthcare providers to transfer their clinical processes between different practices and hospital locations (A. K. Soman, 2011). Also, small physician practices must make sure that they are choosing the right Cloud service provider that will address the complexity of a practice management system and be aware of the risks involved of adopting Cloud based services.

There are some physician practices already hosting a Cloud based computing service platform that is providing the ability to access hosted healthcare applications and patient data regardless of the location. However, in order to assure greater security with healthcare applications, physicians want to use a secure Cloud based service provider that presents secure internet access for their clinical operations. This document is organized as follows. Section 2 is a literature review that briefly discusses Cloud based computing services, SWOT analysis, and its various delivery services models, state of current practice management systems, and upgrades of the practice management to meet security demands; section 3 is a discussion about the technology of secure Cloud services, business economic drivers, healthcare regulations and

legislation, and organizational aspects; section 4 concludes with the summary of the paper and finally section 5 provides some recommendations for a small physician practice to successfully implement a secure Cloud based services model.

2. Literature Review

2.1 Cloud Based Computing Service

This section is a discussion about Cloud computing. It discusses the strengths, weaknesses, opportunities, and threats. When a small physician practice considers adopting a secure Cloud service provider, they must acquire the knowledge and understanding of various Cloud computing delivery services models. The term Cloud computing is a consumption of shared computer resources consisting of groups of hardware, remote servers, and telecommunication networks hosted over the internet (Cloud) to store, manage, and process data resources, rather than on a local server or physical desktop computer. The Cloud computing technology consists of various different models for services delivery: Infrastructure as a Service (IAAS), Platform as a Service (PaaS), Software as a Service (SaaS), Security as a Service (SECaaS), and Desktop as a Service (DaaS). These different services delivery models can be deployed for a small physician practice as a private, hybrid, or public cloud infrastructure. To accommodate small physician practices healthcare business and clinical operational needs, deployment of private cloud is very effective and efficient from a security best practice standpoint.

The Cloud based services innovative platform offers many advantages. In order for physician practices to identify the business objectives of adopting the various Cloud based delivery services models, they must understand its advantages, beware of its weaknesses, what are the opportunities, and understand the threats to determine its path for adoption. One

advantage is its secure integrated web portals that enable you to engage more with the patients for sharing information regarding their personal health records (PHRs), lab results, administration of medicines, and checking of vital signs. Second advantage of the cloud is cost containment. If the practice correctly implements the Cloud based service delivery models, it could offer the practice enormous benefits such as better return on investment (ROI). Next, are secure controlled interfaces that allow a physician practices to create an IT infrastructure that is responsive to their specific user requirements (Hadidi Rassule, 2010). Another advantage is its resiliency in disaster recovery situations. In the event of a natural disaster, the Cloud services models has backup capabilities to ensure practices continue to have access to mission critical healthcare applications.

However, there are some challenges or weaknesses of a secure cloud based service that needs to be addressed. Improperly applying the strengths of the secure Cloud based service delivery model can cause a practice to have a decrease in productivity of clinical operations plus increases in costs of running the practice. Another weakness of the secure Cloud based service provider is global concerns relating to data jurisdiction. To combat the latter concern, physician practitioners and the Cloud based service provider must establish a business associate (BA) contract agreement between them that states the responsibility for management of patient data. Because secure Cloud service providers can't definitively guarantee security of its services, this presents a lack of trust from some physicians so, they refuse to adopt Cloud based services all together. Therefore, continual examination and monitoring of security policies and features can aid in removing some of the distrust in the cloud based technology.

A major opportunity of Cloud based service provider for small physician practices include, eliminating in-house health information technology (HIT) infrastructure cost, IT support

and maintenance burdens as well as increases in return on investment. Second opportunity of a secure Cloud based service is "location independence," a practice can use their personal computers, mobile, and BYOD devices to access clinical information from anywhere externally and internally to the enterprise. Next opportunity of using Cloud based service is marketability of the physician practices itself. Physicians are able to promote accountable care services such as provisions for population health and results of evidence based care. Another opportunity is that the practice medical staff users get to learn and use advanced health information technologies.

As the document describes the threats of Cloud based services delivery models, it is important for physicians to keep in mind that these threats can be overcome. With that said, security concerns are one major threat to adoption of the Cloud services. Another threat is loss or intermittent connectivity which reduces performance. And, there are difficulties with integrating it with another Cloud platform that is different. Also, lack of training and education on the use of the Cloud based services models can pose threats.

2.2 Practice Management System

The physician practice has been using computerized practice management (PM) systems for many years. Small to mid-size physician medical offices have been using the practice management system to capture all of their data regarding patient demographics from a clinical encounter of care necessary for reimbursements of services provided (Ziesemer & Hoyt, 2012). The PM system also maintains a list of insurance payers, generating reports, and scheduling of appointments. It is classified among three setup components, desktop-only software, client-server software, and internet based software. The desktop-only software is intended to be used only for an independent physician practice that has one computer with just a handful of clinical staff users sharing access. The client-server software is intended for the small to mid-size or group of physician practices needing to acquire lease server equipment. The server software

operates on a hardware device inside the practice for medical staff user's workstations containing the client software having access to that server. The advantage of client-server PM software is that it allows multiple users to share the workload and data. The internet based software is an advance healthcare information technology application that small physician practices are planning to adopt because of its integration and expansion capabilities.

The most prevalent practice management systems wildly in use today for a small practice are a combination of both the desktop-only software and client-server software. The demand for increase efficiency and accuracy of billing and claims submission processes has caused physician practices to make the commitment of integrating practice management systems with electronic health records (EHRs). However, integration of PM systems with EHR systems has been very challenging to do because it lacks the adaptability to interface with other healthcare information systems at different locations. Also, there are minimum provisions for security, issues, and increases in costs of running the physical servers with desktop-only software or client-server software installed on them. To purchase a server infrastructure for its medical offices, it could cost an upward investment of $25,000 or more per physician practice (Karen Wager el at, 2009). Physician practices need to facilitate high-quality and very cost-effective delivery of patient care services. The opportunities for advanced healthcare applications like the internet based PM software gives small physician practices the flexibility to deliver more cost effective care. Nevertheless, as internet based software becomes popular amongst physician practices, the security still remains a significant concern.

2.3 Cloud based Practice Management

The Cloud based practice management system is an internet based software that enables physician practices to have the flexibility with managing its clinical operations and workflow processes. They are currently being used today for integration and interoperability with clinical information systems like the EMRs/EHRs to better streamline the efficiency and accuracy of

billing and claims submission processes. In addition, an advantage of internet based PM software is it enables integration of the entire outpatient office workflow process with other practices and health information exchange (HIE) groups that have different clinical operations and workflows. Another benefit of the internet based PM software is decrease in cost of entry for purchasing equipment and mobility. Physician practices are able to use personal devices like "Bring Your Own Devices (BYOD)" to have virtual access to schedules and tracking patient appointments and generating reports of the shared patient health information. According to author Forrest Burnson, 80 percent of healthcare professionals now access their clinical work documents on personal devices outside of the medical offices (Forrest Burnson, 2014). However, security weaknesses still remains a major concern for internet based PM software. Due to these security concerns, physician practices have fears about trusting and transmitting patient protected health information (PHI) across the internet.

3. Discussion

3.1 Technology

There are plenty of technological benefits of Cloud based services. Going back to the characteristics of Cloud computing, it is to build a virtualized computing resource pool by centralizing abundant computing resources connected with network and present the service as infrastructure, platform, and software as on-demand access (Jianhua Che et al. 2011). The foundation of Cloud based service is a converged infrastructure that includes servers, networking equipment, data storage devices, and software for management and automation. This converged infrastructure is housed within a physical data center location. The secure Cloud based service model is monthly or yearly subscription based elasticity models of Pay-As-You-Go fees. The fee model varies per physician practices utilization during a certain period. That means a physician practice can utilize the service only to the extent they need it. In the case of an unexpected natural disaster, a secure Cloud based service provider gives health providers the ability to backup securely and store patient data geographically separated from the primary location.

Reliability of Service: The secure Cloud based service has authentication and authorization validation checks to ensure reliability of healthcare users accessing their health information. In order to meet physician practices request to have high quality performance of its mission critical clinical information systems (CIS) and healthcare applications, the service capability of the Cloud must meet their expectation. Therefore, the service level agreement (SLA) must be established within a business associate (BA) contract negotiated between the secure Cloud service provider and the physician practice. Inside the BA contract, the SLA stipulates how incidents are handled involving patient data loss, and how conflicts get resolved. Also, the service level agreement (SLA) must detail types of performances such as uptime keep of the network, how service requests are charged, i.e. peak/off-peak, rates fix or changing, availability, and actual capacity utilization for current and future increase volume of operations (Christian Senk, 2011).

Multi-tenancy*:* Multi-tenancy architecture is a very important feature of secure Cloud services because it enables sharing of resources and costs across a large pool of users within a single instance. Each cloud end user is called a "tenant" which means they have the ability to customize the business rules according to their specification. The advantage of secure cloud based service multi-tenancy is that the physical servers (within the datacenter) partitions and process different health client demands in a virtualized environment. However, there are some vulnerabilities of multi-tenancy that need to be addressed. Multi-tenancy can cause data isolation and human weakness. Data isolation means that the business data of multiple clients do not intervene mutually (Jianhua Che et al. 2011). The human weakness stems from individuals not properly implementing or deploying multi-tenancy architecture correctly. Because of the human weakness, data can be inadvertently exposed to other users of cloud increasing threat. Therefore, a secure Cloud service provider platform is needed.

Security as a Service (SECaaS): The most popular service models of the Cloud are SaaS, PaaS, and IaaS. However, security is still a major issue with hosting mission critical clinical applications and storing data with these service models because they provide on-demand access through use of the public cloud. Therefore, security as a service (SECaaS) platform is gaining ground as the preferred choice amongst small physician practices because it provides a holistic approach to addressing their security concerns. The security as a service (SECaaS) architecture is a business model in which a service provider integrates its managed security services into a corporate infrastructure. It is a subcategory of the software as a service (SaaS) model. According to the authors Mohammed Hussain and Hanady Abdulsalam, SECaaS takes a user-centric approach so that the cloud users have more control of their security. Also, it provides greater security means for both the secure Cloud provider and cloud users (Hussain & Abdulsalam, 2011). There are many benefits or advantages of the SECaaS manager cloud for a small physician practice. Indicated below are the four most important benefits of SECaaS Cloud service adoption:

- Identity and access management to increase protection of patient health information
- Security information monitoring and event management (SIEM) to ensure its operational compliance to healthcare regulations and standards
- Data loss management and control of patient data through reporting, prevention, and monitoring
- Protection of physician practices assets such as patient data and healthcare applications as well as the software, platform, and infrastructure of its secure cloud services (Hussain & Abdulsalam, 2011)

Another benefit of SECaaS Cloud base service is its auditing control mechanisms to examine and record activity of health information systems for auditing, monitoring, and reporting purposes. The secure Cloud service environment also is certified as a Statement of

Auditing Standard No. 70 (SAS 70) type II. That means the SECaaS Cloud service provider datacenters are certified and required to have safeguards in place to evaluate and measure security over time to keep the patient protected health information safe from corruption, and against mishandling of that data during access through the secure internet cloud. The auditing and reporting results must be discussed with the stakeholders or physicians of the practice as added measures to ensure compliance and privacy.

Encryption: To ensure high levels of privacy, confidentiality, integrity, and availability (CIA) of patient data, SECaaS Cloud service model use cryptographic separation of data. Cryptographic separation of data guarantees the privacy of the healthcare user data. It also conceals computations and data in such a way that they appear intangible to outsiders (Zissis & Lekkas, 2010). Cryptographic is an encryption algorithm used for converting health informational data that is in plain text to unreadable or unintelligible text known as ciphertext.

3.2 Business Economics

Cost*:* The business economic impact of a secure Cloud base services model for a small physician practice is significant. For a small physician practice, building an in-house health information technology (HIT) infrastructure for its medical offices has enormous upfront cost, and it is difficult to maintain in comparison to adopting a secure Cloud based service paradigm. The upfront cost including maintenance and support for a small physician practice is in the range from $15,000 to $50,000 per physician practice (Blumenthal & Glaser, 2007). Because of the colossal amount of upfront cost, it has caused small physician practices to seek out advanced technologies that can assist with provisions for security, integration, and quality of patient care required. The secure Cloud based service solution eliminates this HIT upfront cost because the HIT infrastructure is in the private cloud based system. The benefit is that small practices do not

have to worry about purchasing hardware equipment and hiring IT staff for support and maintenance.

A recent survey study was conducted on 200 smaller physician group practices and it showed that adoption of a Cloud based computing service has a cost reduction of $4,400 per physician (Frank Irving, 2012). This seems to be a major opportunity for a small physician practice to consider adopting secure cloud technology. According to Forbes Magazine, based from the Health Information and Management Systems Society (HIMSS) Analytics Cloud Survey, 83 percent of healthcare organizations and providers are currently using cloud services today. Further, the HIMSS Analytics survey states that 61.4 percent of healthcare organizations' main concern is the security of cloud services resulting in 38.4 percent of them refusing to adopt the cloud services all together (Louis Columbus, 2014). The high percentage of these small physician practices still having security concerns alone is enough for them to invest and fund in a secure Cloud service provider.

3.3 Regulations and Legislation

The secure Cloud based service provider is able to assist physician practices with meeting healthcare regulatory requirements and standards. In addition, the secure Cloud service provider themselves must be in compliance with these same healthcare regulatory requirements. To mitigate the security breach concerns, secure Cloud based solution providers must establish security controls, policies and procedures. Also they have to establish risk management methods, auditing, reporting tools, and functionalities that are in accordance to HIPAA certified security measures and Meaningful Use (MU) stage criteria to protect patient health information from possible breach situations (William Gillespie, 2010). Penalties and ongoing cost can occur if physician practices are not demonstrating or failing to neglect the use of MU under stage 2 criteria.

HIPAA Act: is the Federal Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a rule that sets the primary goal of the law to protect the privacy of individual identifiable health information. The HIPAA privacy and security Act makes it convenient for individuals to keep health insurance and access personal health record information (PHR) in a protected, confidential, and secure manner. It also assists the physician practices with control of administrative costs. The secure Cloud based provider has ease of management and operations tools like the web-interface consoles that alerts the practice of any security incidents requiring attention and it provides auditable reports to ensure compliance is in place. It is important for a secure Cloud based service provider to understand HIPAA has two main parts to ensure compliance is met. These two parts are labeled as Title Legislation Acts indicated below:

1. Title I addresses health care access, portability and renewability, offering protection for the person who changes health insurance policies. This legislation is important for a secure Cloud provider to know because these policies are being maintained and managed in the integrated Cloud system.
2. Title II includes the Administrative Simplification. It has the requirements to establish privacy regulations for individually identifiable health information. The Administrative Simplification also has a subsection that details the transaction and code sets of security standards as it relates to HIPAA security regulations (Karen Wager et al. 2009).

HITECH Act: The Health Information Technology for Economic and Clinical Health Act known as HITECH Act enacted under the American Recovery and Reinvestment Act (ARRA) of 2009 was created by the Federal Government to promote EHR systems adoption and provide aid (through financial incentives) to physician practices to commit to adopting EHR systems for integration with their practice management systems. It enforces the rules for neglecting or failing to meet Meaningful Use stages criteria could cost them and secure Cloud based service provider penalties and violation costs going up to $1.5 million (A.K. Soman, 2011).

Meaningful Use: The meaningful use (MU) stage criteria are guidelines for physician practices to follow when implementing an EHR system together with its practice management systems. It also ensures that practices are using health information systems that results in care efficiency and effectiveness, patient-centered setting the stage for evidence based care. The Meaningful Use criteria consist of three primary stages for health providers to follow indicated below.

1. Started in year 2011. It involves attesting to the use of EHRs to capture clinical data and sharing that data electronically.
2. Begin in year 2014. This stage promotes electronic health information exchanges (HIEs) and carries the option of reporting performance and quality measurements using advance clinical processes (i.e. Cloud base practice management systems).
3. Expected to begin in year 2017. This stage supports financial rewarding to physician practices for reporting levels of improved results of performance quality measurements and security compliance (Samal et al, 2014).

Transition to ICD-10-CM: The International Classification of Diseases (ICD) is the diagnostic tool for health management and clinical purposes. It is used by physicians, researchers, nurses, policy makers, and healthcare organizations for reimbursement of care services and resource allocation-decision making. To keep up with the widespread expansion of diagnostic data code sets, the ICD-9-Clinical Modification (ICD-9-CM) was revised to the ICD-10-CM. The transition to the ICD-10-CM is causing financial challenges resulting in decline of reimbursements for some small physician practices. The current practice management system is not robust enough to be compliant, and cannot handle the ICD-10 diagnosis code sets of 69,000 in comparison to ICD-9 diagnosis code sets of 14,000. Therefore, adoption of a secure Cloud based practice management system is helping physician practices to facilitate that transition because it can provide the expansion, flexibility, and security needed. Also practices must evaluate the secure cloud based system to determine if it fits with the timing and path of transitioning to ICD-10-CM.

HIEs: To facilitate the quality and cost-effective delivery of care services across various healthcare organizations, hospitals, and other group practices, small physician practices are converting their practice management (PMs) with clinical information systems (CIS). The health information exchange groups (HIEs) was created to integrate health data between two or more group practices and health organizations in different locations. The HIEs consist of the technology, standards, and governance that enable of the exchange of data between the health information systems (HIS) (Karen Wager et al. 2009). This is a main reason why healthcare providers should consider adopting a secure Cloud base service. It offers portability and interoperability as a risk management mechanism and security assurance to assist health providers to adhere follows the standards of HIEs.

3.4 Organizational

The adoption of a secure Cloud based service model has definitely changed the organizational structure of a physician practice. Because of the adoption, roles and responsibilities of the practice's administrative staff have been impacted. Physicians don't need to have a huge administrative staff to perform basic tasks for example patient coming in the office to schedule an appointment. This process is automated. Another organizational impact is management system change. According to the author containment of service contracts with client requirements and measurement systems in the Cloud can grow exponentially making it challenging to managing it service individually as compared to managing service contracts with a traditional in-house management system (Edwin Schouten, 2012).

4. Conclusion

Inevitably, secure Cloud based service provides plenty of opportunities for a small physician practices to be successful with health information technology applications like the Cloud based Practice Management system. The secure cloud based service provider offers a security architecture like the security as a service (SECaaS) that has integration and interoperability, enabling physician practices to provide better care coordination, security,

flexibility, lower cost of operations, and usefulness and trust. This document should have given a better understanding of the strengths, weakness, opportunities, and threats of secure Cloud based services solution and the some of the reasons why a small physician practice should attempt to adopt its solution to improve quality of care coordination, improve clinical workflow processes and ensure that they are meeting the HIPAA regulations of privacy and security, and Meaningful Use (MU) requirement criteria.

5. Recommendation

The adoption of a secure Cloud based service provider for a small practice critically needed. In order for a practice to adopt a secure Cloud service provider, careful evaluation is fundamental. Having a thoughtful approach to how a practice can adopt a cloud technology is predicated on the recommendation as follows:

- Increased training (or cross-training) of smaller physician practice office staffs, clinicians, and others to enable the transition to a secure Cloud based service provider to improve the practice's clinical operational and administrative performance.
- Physician practices and stakeholders must be very diligent with requesting that the secure Cloud service provider are auditing and reporting and submitting the status of those reports of the patient protected health information within its data centers are in compliance to HIPAA regulation and laws and MU requirements of the practice.
- Ensure that the secure cloud service provider is certified by the International Organization for Standardization (ISO) 27001 and are controlled and directed by the Organization for Economic Co-operation and Development (OECD) principles of corporate governance.
- Ensure that the adoption of a secure Cloud based service provider is appropriate for the practice.

References

1. Blumenthal David, Glaser P. John. (June 14, 2007). Information Technology Comes to Medicine. Retrieve from http://www.allhealth.org/publications/Health_information_technology/Information_Technology_Comes_to_Medicine_71.pdf

2. Brocato Lori, Emery Steven, McDavid Jan. (2011). Keeping Compliant. Managing Risking Risk in Physician Practices. Retrieve from http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_049297.hcsp?dDocName=bok1_049297

3. Columbus Louis. (July 17, 2014). 83% Of Healthcare Organizations Are Using Cloud-Based Apps Today. Retrieve from http://www.forbes.com/sites/louiscolumbus/2014/07/17/83-of-healthcare-organizations-are-using-cloud-based-apps-today/

   Gillespie William. (November 10, 2010). Cloud Computing and Achieving Meaningful Use. Retrieve from http://www.hitechanswers.net/cloud-computing-and-meaningful-use/

4. Harrison I. Michael, Koppel Ross, Bar-Lev. (2007). Unintended consequences of information technologies in health care--An interactive sociotechnical analysis. J Am Med Inform Assoc 14:542-549. Link to library: http://jamia.bmj.com.proxy.cc.uic.edu/content/14/5.toc

5. Hussain, Mohammed and Abdulsalam, Hanady. (April, 2011). SECaaS: Security as a Service for Cloud-based Applications. Retrieve from http://uichicago.summon.serialssolutions.com/search?s.q=SECaaS%3A+Security+as+a+Service+for+Cloud-based+Applications

6. Irving, Frank. (November 27, 2012). Smaller practices find cost savings in the cloud. Retrieve from http://www.medicalpracticeinsider.com/best-practices/technology/business/patient-care/professional-development/smaller-practices-find-cost

7. Kuo M. Alex. (September 21, 2011). Opportunities and Challenges of Cloud Computing to Improve Health Care Services. Retrieve from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3222190/

8. Lukan Dejan. (September 17, 2014). Top Cloud Computing Threats in Enterprise Environments. Infosec Institute. Retrieve from http://resources.infosecinstitute.com/top-cloud-computing-threats-enterprise-environments/

9. Quinn Frank. (November 21, 2012). Practice Management Software – How it keeps the practice running. Retrieve from http://medcitynews.com/2012/11/practice-management-software-how-it-keeps-the-practice-running/

10. Rassule Hadidi. (September 1, 2010). Exploring the use of SWOT analysis in the adoption of Cloud Computing services for small and medium-sized enterprises (SMEs). Retrieve from http://www.freepatentsonline.com/article/European-Journal-Management/260256392.html

11. Samal, Lipika, Wright Adam, Linder, J. Jeffrey, Bates W. David. (April 14, 2014). Meaningful Use and Quality of Care. Jama Internal Medicine. Volume 174, Number 6. 997-999. doi:10.1001/jamainternmed.2014.662.

12. Schouten, Edwin. (2012). The Organizational Impact of The Cloud. Retrieve from http://www.wired.com/2012/11/the-organizational-impact-of-the-cloud/

13. Senk Christian. (April 11, 2013). Adoption of Security as a Service. Journal of Internet Services and Applications. doi:10.1186/1869-0238-4-11

14. Soman, A.K. (2011). Cloud-based Solutions for Healthcare IT: (Chapter 4 and 6, pp. 84 - 182). CRC Press.

15. Wager A. Karen, Lee W. Frances, Glaser P. John. (2009). Health Care Information Systems. A Practical Approach for Health Care Management.