Considerations for the Migration of Electronic Medical Records to Cloud Based Storage*

전자의무기록의 클라우드 기반 저장소 이동시 고려사항

이 명 호(Myongho Yi)**

〈Contents〉

ABSTRACT

As cloud computing becomes more and more popular and ubiquitous, many organizations are deciding to move their whole information infrastructure to the cloud. The healthcare industry is one of those that is beginning to utilize cloud-based solutions en masse. Cloud based computing and storage offers numerous benefits including scalability, cost efficiency, and accessibility, which in turn have the potential to streamline hospital operations. Despite the potential benefits of acquiring this system, considerations must still be given to the migration of the massive amounts of personal and highly protected data to a cloud-based solution. Health care organizations must consider all matters of security, reliability, and availability, to ensure that patients' data remains compliant to the Health Insurance Portability and Accountability Act (HIPAA) compliant. This paper will examine the benefits and challenges of such operation to determine the best practices for the utilization of Electronic Medical Record (EMR) cloud based networking and storage for small to mid-sized hospitals.

Keywords: Cloud computing, Cloud storage, Electronic medical records, HIPAA

초 록

클라우드 컴퓨팅에 대한 관심이 많아짐으로 인해 많은 기관들이 클라우드 컴퓨팅으로 전환을 결정하고 있다. 확장성, 비용 효율성, 접근성 등 다양한 장점으로 인해 의료 기관들도 정보 인프라를 클라우드 기반으로 전환하는 것을 추진하고 있다. 이러한 장점에도 불구하고 많은 양의 민감한 개인정보를 이동 (migration) 하는 것에 대한 여러 가지가 고려되어야 한다. 의료 기관은 민감한 환자 정보에 대한 보안, 안정성, 가용성을 고려하고 또한 HIPPA와 같은 법적인 요구 사항을 만족시켜야 한다. 본 연구는 전자의무기록을 클라우드 기반 저장소로 이동시 장점 및 문제점을 조사하고 또한 고려사항을 제안하고자 한다.

키워드: 클라우드 컴퓨팅, 클라우드 저장소, 전자의무기록, HIPPA

* 본 논문은 2014년도 상명대학교 교내연구비를 지원받아 수행하였음.

** 상명대학교 문헌정보학과 조교수(josephlee@smu.ac.kr)

•논문접수: 2016년 2월 26일 •최초심사: 2016년 2월 26일 •게재확정: 2016년 3월 23일
•한국도서관·정보학회지 47(1), 149-173, 2016. [http://dx.doi.org/10.16981/kliss.47.201603.149]

Ⅰ. Introduction

Hospital data such as medical records are produced and recorded in paper form; however, patients and hospital staff have limited or no access to these medical records after business hours. In addition, managing medical paper records such as sorting and searching for them is not easy. Paper records require a lot of staff members to manage and a space to store in records. On the other hand, Electronic Medical Record (EMR) costs less to manage and maintain records. Also, paper records stored in file cabinets are not secured enough. Files can be stolen or damaged by natural disaster such as fire and flood. To be prepared for any loss, we need to have backups. However, managing, maintaining, and preparing a backup for paper records can be costly and taxing for a small to mid-sized hospitals. The introduction of using a cloud-based storage system can settle these major concerns. EMR is a collection of electronic health information of a patient (Gunter and Terry 2005). After Hurricane Katrina hit the US, the value of EMR has been re-emphasized, since the tragedy highlighted the difficulties in accessing medical records during an emergency situation. Medical professionals could not treat patients efficiently without easy access to their medical records (Williams and Boren 2008a). The demand for implementing EMRs and telemedicine in Africa is very high because the burden of disease there is great and there is an extreme shortage of health professionals (Mars 2013). These situations show the limitations of medical paper records and an immediate need to consider transitioning to EMR.

Adapting EMR over paper medical records has four major benefits: cost, storage, security, and accessibility (Carpathia 2013). As the number of patients grow, storing records becomes an unavoidable issue. Hospitals need a large space to store a patient's record. Preserving records in this way also becomes problematic. EMR can be stored in a secured online place and be monitored for any suspicious activity; in contrast, paper records file cabinets are not as secured. We can duplicate copies easily for EMR; however, paper records take a lot effort to create a backup. Time is critical in medical settings. To access paper medical records, they must be mailed or scanned and sent via email which take a lot of time. The use of electronic medical records allows medical professionals to access the information they need almost instantly. This information can now be created in an electronic form supported by laws. In order to meet the internationally-accepted standards, healthcare organizations are rapidly implementing health

information technology. Once an organization chooses to upgrade its information systems, it must then make the critical decision of choosing how to go about doing so. There are three major available options. They can build it themselves, purchase new systems from vendors, or have their systems run “in the cloud.” The healthcare industry in particular must also take into account special considerations when moving its electronic records and its information infrastructure to the cloud. Particularly, this paper will examine the benefits, drawbacks and ramifications as healthcare organizations attempt to utilize a cloud-based solution for its electronic medical record storage needs. In doing so, we can gain greater understanding of the challenges in leveraging cloud computing networking by addressing the issues of security, reliability, integration and interoperability, and scalability. This will in turn provide strategic recommendations on how hospitals may utilize this technology for reliable data sharing of electronic medical records.

The purpose of this study is to address the benefits and challenges of cloud computing to determine the best practices for the utilization of Electronic Medical Record (EMR) cloud based networking and storage for small to mid-sized hospitals. This article is organized as follows: discussion of regulations to manage medical records, description of benefits of electronic medical records, benefits and drawbacks of cloud-based EMR, solutions for challenges, and finally, concluding comments.

Ⅱ. Health Record and Cloud Computing

1. Regulations about Health Record

When we deal with medical records in paper or electronic form, we need regulations to provide standards and regulate them. Here are the major regulations that lay out ways on how to manage and protect medical records.

(1) Health Insurance Portability and Accountability Act

In the US, Health Insurance Portability and Accountability Act (HIPPA) is one of the major regulations related to electronic medical records. HIPPA describes the potential and benefits of EMR. It was enacted in 1996 to protect health insurance of workers when they change or lose

their jobs. HIPPA also requires the establishment of national standards for electronic healthcare transactions and national identifiers for providers, health insurance plans, and employers.

(https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act) There are five rules or acts under Title II. Among these rules, the Privacy rule is integral to record security for electronic medical records. Privacy rule is related to security for electronic medical records. HITECH Act requires hospitals to transform their paper medical records to electronic medical records. HITECH Act was created in 2009 to encourage the implementation of EMR in the United States. Privacy rules focus on protecting health information either in paper and electronic form. One of these is the Security Rule which deals specifically with Electronic Protected Health Information (EPHI). This provides three controls, the administrative, physical, and technical safeguards, to protect electronic medical records. In addition, the HITECH Act of the United States Department of Health and Human Services is spending $25.9 billion in 2016 to implement nationwide network of electronic health records by using health information technology. These special considerations include security and the HIPAA compliance issues in regards to electronic medical data. Network security of electronic health records is governed by US Federal regulatory requirements where they must meet HIPAA security and privacy standards. The HIPPA Act of 1996 (HIPAA) includes the HIPAA Security Rule, which are national security standards for protection of health information that is stored or transferred electronically (Yadron and Beck 2015). Requirements under HIPAA are flexible and intended to allow technological growth and implementation by a range of institutions. It requires covered entities to perform risk analysis, identifying the likelihood and impact of risks to electronic PHI (protected health information). The organization then implements and documents security measures that address these risks (Yadron and Beck 2015). These measures can include administrative, physical, and technical safeguards on both sides of the organization and its business associates, or vendors. The most applicable to distributed computing and networking are the technical safeguards-access controls, audit controls, integrity controls, and transmission security (Yadron and Beck 2015). The area where cloud computing stands to deliver great benefits is that of patient health data storage. The storage and facilitation of EMR is a major draw for utilizing cloud based solutions. The nature of EMRs means they contain highly sensitive and personal data about individuals which must be safeguarded. HIPAA mandates strict enforcement of privacy and security rules over how medical information is collected, handled, used, disclosed, and protected. In particular, HIPAA security

rules center on information assurance regarding the availability, confidentiality, and integrity of patients' data (Schweitzer 2012).

(2) HIPPA and Cloud Computing

These regulations are of concern to the healthcare provider because as the custodian of the data, any cloud service provider they utilize must also adhere to HIPAA standards. By sharing responsibility with the cloud service provider, the healthcare organization gives up a measure of control over sensitive data and its processes, since it is the third party which handles the operational and control aspects of the stored EMRs. However, Maheu (2014) stresses that while "even with a signed Business Associates Agreement, the burden would still fall on hospitals to secure the data, even when hosted at a HIPAA compliant cloud storage provider." It would be the health care provider that remains wholly culpable in case the data would be somehow compromised and would face the brunt of any and all legal and financial ramifications that would result thereof. A critical component required to satisfy HIPAA compliance is accurate identification and authentication of users in addition to comprehensive authorized privilege and role-based access control. Passwords and other methods will be necessary in any system regarding sensitive data and are especially paramount here. Security of the cloud stored EMRs will be of great priority when deciding the cloud service method. For productive use in a healthcare setting, cloud solution providers must guarantee security, scalability, reliability, HIPAA compliance, and uninterrupted service. Any lack of these qualities will present significant negative repercussions for any healthcare organization utilizing that cloud based service. Aside from vendor's choice, the means and method by which the hospital transfers its data will also be under scrutiny. While the hospital is a generic fictional one, the solutions to its data storage concerns can be used by other health care organizations when considering their decision to move to a cloud-based storage service. EMRs are "mission critical systems" for hospitals; losing access can be detrimental to patients' safety and disruptive for staff. As such, information availability is essential, and network safeguards should be in place to help prevent unauthorized access and attacks that could take down the network. Once an EMR has been implemented, it can be difficult to revert to paper documentation in the event of a network failure. Three-hospital Martin Health System in Florida experienced a network failure in early 2014 that lasted for three days (McCann 2014). While processes are available to ensure patients' safety in these events, it leaves existing documentation,

orders, and alerts inaccessible (HealthcareITnews.com 2014). In a hospital environment, EMRs are used for both documentation and ordering, including medication orders, which needs to be communicated with ordering providers (physicians), nurses, and pharmacy (Hanuscak, Szeinbach, Seoane-Vazquez, Reichert, and McCluskey 2009). As such, downtime has been shown to disrupt this communication and has been linked to increased medication errors since users cannot see recent doses administered or review potentially interfering medications (Hanuscak et al. 2009). This type of unscheduled downtime can be attributed to network security issues such as viruses, which can be combatted through strong network security such as firewalls (HealthcareITnews.com 2014). Systems should also have hardware redundancy, backup, and disaster recovery policies and infrastructure (Kahn and Sheshadri 2008). The mission critical nature of EMRs must also be considered in the implementation of network security measures that aim to prevent unauthorized access. Since EMR must be readily accessible, both in daily activities and in emergency situations, traditionally robust network security measures such as multi-factor authentication may not fit into the healthcare environment. While traditional access controls require advance planning, of which exact users or roles should have access to a particular record or feature, healthcare users who are not on the patient's planned care team should have the ability to "break the glass" in the event of an emergency (Ardagna et al. 2010). Although we have electronic medical records available in hospitals, if not centralized, we discredit the benefits of networked EMRs. One of the best options to make networked EMR is using Cloud where we can efficiently access the local EMRs.

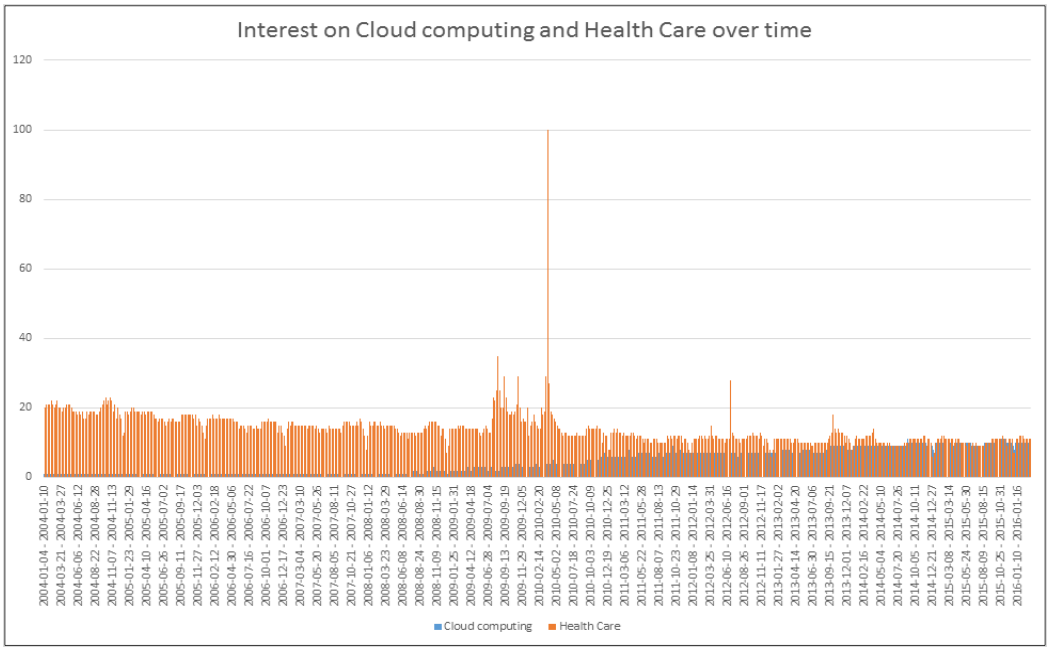
2. The Impact of Cloud Computing on Health Care

Cloud computing is like renting a car. Whenever we need more IT resources, we can pay based on our usage. Cloud Computing is a model for providing an ever present, convenient and an on demand access to a shared collection of configurable computing resources such as networks, servers, storage and services. Users can, on a moment's notice, access and utilize these resources with minimal management effort or service provider interaction, possibly from any location and on any device, granted they have an internet connection and the necessary software. There are generally five critical characteristics, three service models, and four deployment models that compose the cloud model that will be defined as follows by the National Institute of Standards

and Technology (Mell and Grance 2011). The essential characteristics are on-demand service, broad network access, resource pooling, rapid elasticity, and measured service. On demand service refers to users accessing computing capabilities where and when they want automatically, without resorting to getting in touch with the service provider personally. Broad network access means capabilities of the cloud are available over a network and accessed by the users through standard mechanisms such as mobile phones, tablets, laptops and workstations. Resource pooling denotes providers combining computing resources such as storage and memory to service multiple users, which are then dynamically assigned to users based on user demand. The characteristic of rapid elasticity signifies that the capabilities of the cloud are released automatically, scaling in and out. Depending on consumer demand, this normally represents itself to the user as an unlimited resource, able to be accessed and utilized immediately when requested. Finally, measured service refers to the cloud system automatically controlling and optimizing performance by monitoring, controlling, reporting and providing transparency for both the service provider and the end user (Curran and Carlin 2013). The three service models are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) (Sabahi 2001). Briefly, for comparison's sake, SaaS and PaaS respectively refers to the capability provided to the consumer allowing the consumer to either use the provider's applications running on the cloud's infrastructure (SaaS) or the capability to deploy onto the cloud consumer-created or acquired applications using tools provided and supported by the provider (PaaS). IaaS is the capability by which the providers allow the user to process, utilize store, network, and use other fundamental computing resources. The consumer in this case does not manage or control the cloud infrastructure itself but has control over operating systems, storage, and deployed applications (Mell & Grance, 2013). These key aspects afforded by IaaS will serve best the needs of the hospitals as they look to store and move their information infrastructure to the cloud. The deployment models are private, community, public, and hybrid. Private clouds are available for use by an organization comprising multiple consumers, owned and managed by the organization. Community clouds are for exclusive use by a community of users from organizations that have shared concerns such as specific security requirements and missions. The public cloud is for use by the general public and is normally owned by businesses, academic organizations or government. Lastly, the hybrid cloud is a combination of the former three, which while remaining separate entities, are tied together through standardized or proprietary technology that enables data

and application portability (Mell and Grance 2013). While there may be some practical overlap among these models, this paper will focus specifically on a private cloud deployment model for a small community hospital.

Cloud computing is an emerging technology that is rapidly gaining ground for organizations in all industries. Forward looking healthcare providers are beginning to realize the potential behind this new technology and a small number of them are quick to implement cloud solutions in a bid for greater efficiency and affordability. Healthcare organizations will need to adapt and make their operations more streamlined and agile. Using cloud solutions is a major step towards those goals. Despite this, compared to other industries, the healthcare sector has significantly underutilized this new technology to do so, and many healthcare systems are still reliant upon paper medical records (Cloud Standards Customer Council 2012). Cloud computing represents an opportunity and means for the healthcare industry to abandon this outdated paradigm to become a more modern industry. The Cloud Standards Customer Council asserts, “cloud computing provides an infrastructure that allows hospitals, medical practices, insurance companies and research facilities to tap improved computing resources at lower initial outlays.” In other words,



<Figure 1> Interest on Cloud computing and Health Care 2004–2016

cloud computing enables greater capabilities at a lower financial investment. As shown in Figure 1, interest on cloud computing and healthcare Cloud computing from 2004-2016 has been increasing (Google Trends 2016).

Cloud computing allows fulfillment of key business requirements of the healthcare organization to include on-demand access to computing and data storage facilities for electronic health records, as well as facilitating the sharing of those records, and improving the ability to track and analyze information so that data on treatments, costs, etc. can be acted upon (Cloud Standards Customer Council 2012).

3. Cloud-based EMR and Server-based EMR

Information sharing is a key feature of the electronic health record. Information sharing happens over a network, either within a single hospital building or across a broader network to share information among the several hospitals in the city that make up this healthcare organization. Information sharing is a key benefit of electronic health records; a patient's records (medical history, allergies, medications, surgical notes) are available to all members of the patient's medical team within the organization, improving care coordination (HealthIT.gov 2014a). To make use of this information sharing, there are several requirements. Users must be able to access information documented by other users and at other sites. Mobile access is also an important feature of an EMR used across multiple platforms. A physician, for example, may access patient charts from an office using a laptop, and bring that laptop to care coordination team meetings in another location. The HITECH Act establishes that encryption of e-PHI is a requirement, and a comprehensive risk assessment should take into account the various devices and locations that employees use to access the EMR (Miller and Blass 2010). Information sharing and mobile access necessitate a cloud or server-based system to share information across a geographic area in near-real-time, rather than periodic transfer of data. A single user must be able to log on to the system in a variety of locations, such as a physician practicing in multiple locations or a nurse charting in multiple patients' rooms.

(1) Server-based EMR

Cloud-based EMRs and server-based EMRs are the two options for sharing information to meet

the healthcare organization's needs. The client-server architecture is commonly used, and offers client-customized installation and centralized control. For example, Epic Systems, one of the most widely used EMR vendors with approximately 20% market share, uses traditional client-server architecture (Congdon 2014). While the exact network configurations are customized based on the organization's needs, it will require hardware installation or the servers, as well as physical safeguards such as a secure server room to prevent unauthorized access that could compromise the system or data (Egdom, 2013).

(2) Cloud-based EMR

Cloud-based systems, on the other hand, operate using a software as a service (SaaS) model. Through a subscription fee, the organization gets access to the software, and data is housed in a remote data center operated by the vendor. This model is complete with physical safeguards, data redundancy/backup, high speed servers, and robust, HIPAA compliant encryption (Egdom 2013). Updates and risk assessments are handled by the vendor. The SaaS model of EMR implementation supports information sharing and mobile needs by offering access from any approved device into a common cloud-based system, without the need for additional software licenses.

(3) Comparison of Cloud-based EMR and Server-based EMR

While both cloud-based SaaS and client-server EMR implementations are available and currently in use, security can be achieved more easily, at a lower cost, and kept robust and up-to-date by using a cloud-based system. Table 1 shows the comparison between cloud-based EMR and server-based EMR.

<Table 1> Cloud-based EMR vs. Server-based EMR

	Cloud-based EMR	Server-based EMR
Setup Fee	Low	High
Security	Included with Fee	In-House setup
Mobility	High	Low
Control	Low	High
Realibility	High	Medicum

Several of these vendors certified by the Office of the National Coordinator for Health IT are on the market, including Athenahealth, Meditouch, and Carecloud. While studies have not been conducted on the security comparability of these SaaS vendors versus traditional client-server types such as Epic and Cerner, materials from the vendors explain the benefits. As web-based software, these systems can run on any authorized hardware on a subscription basis. This includes desktop or patient-room workstations, computer-on-wheels (COWs) that are often wheeled between patient rooms in a hospital setting, laptops, and mobile devices such as tablets and smartphones. By using SaaS, the organization is able to assess the security controls that have already been implemented by each vendor, and compare them to their own risk assessments that have been conducted as a part of HIPAA Security Rule Compliance. While a client-server architecture would require costly upfront expenditure to purchase the hardware, install it in a physically secure location, install backup systems, and hire IT and security employees for ongoing security monitoring, the SaaS model includes these security services on a monthly subscription fee (Meditouch 2014). The organization would be able to assess which vendor has the security controls that meet its needs, rather than attempting to implement robust network security features into its own network with limited resources. Because the cloud provider is receiving e-PHI from the healthcare organization and storing it in the cloud, the cloud provider qualifies as a "business associate" under HIPAA and the HITECH Act (Gilmer 2013). This has implications for its performance under this legislation, setting expectations for their network security measures. While using a cloud-based EMR places the burden of implementing and upgrading security on the vendor, it is important that clients understand that risks still exist with the cloud-based model; under HIPAA and HITECH, whoever has control of the e-PHI is responsible for "access security, data-breach monitoring, audits, and risk management"(Gilmer 2013 p. 9). The cloud-based vendor that is selected should use a private cloud model, which is open only to a single consumer, preventing access from other clients or unauthorized users (Gilmer 2013). The vendor also must ensure information availability, in compliance with the Security Rule (Gilmer 2013). Cloud services can reduce network downtime by having a robust architecture that stores redundant data in multiple locations, preventing downtime due to a server crash or natural disaster. They also may have on-demand resource capacity that allows improved performance during peak demand periods, and that can compensate when there is scheduled maintenance (Gilmer 2013). This redundancy also limits the effectiveness of denial-of-service attacks, which overwhelms a server's

capacity using repetitive, false requests and preventing data from being sent to real users. If such an attack occurs, the redundant servers can come online to compensate (Gilmer 2013).

Ⅲ. Benefits of Cloud Computing in Healthcare Operations

Cloud computing both has advantages and disadvantages. Table 2 shows the general advantages and disadvantages of cloud computing (Apostu et al. 2013). Section 3 and 4 describe major benefits and challenges of cloud computing from the healthcare industry perspective.

<Table 2> Advantage and Disadvantage over Cloud Computing

Advantage	Disadvantage
Cost efficient and lower expenses	Prone to attack
Backup and Recovery	Slow Speed
Quick Deployment	Limited Features
Almost Unlimited Storage	Technical Issues
Easy Access to Information	Possible downtime
Easier scale of services	Inflexibility
Reliability	Lack of support

1. Cost Efficiency

One of the great attractions of a cloud-based service is the cost. Cloud computing can be a good option for healthcare institutions because they seek for a cost-effective turn-key solution that provides scalability with built-in backup and data protection (Cloud Standards Customer Council 2012). Compared to the alternatives of developing an on-premise system, cloud services require a significantly lower initial monetary investment as well as avoiding certain recurring costs. According to Kuo (2011), “An organization can easily get a cost-effective and on-premise IT solution through cloud computing without the need to purchase or evaluate hardware or software, or to hire internal IT staff to maintain and service in-house infrastructure.” Such cloud-based systems forego the need and costs for internal IT staffing and training, so that organizations may instead focus on critical tasks. With a pay-as-you-go method, hospitals will only need to pay for

what it uses. Therefore, if there is no need to acquire expensive hardware and infrastructure, licensing, staff, and security, hospitals will be able to save significant funds since cloud computing providers will take care of those aspects (Ahuja, Sindhu, and Zambrano 2012). The cloud service provider is responsible for providing all terminals regardless of location. The costs for cloud-based systems are generally lower compared to the other options, with third parties doing most, if not all of the work. According to Taylor (2013) quoting Brian Bruffey, CEO of cloud-based AMS provider Protech Associates, "cloud systems bring world class technology to a market that historically has not had big budgets and staff." Considering hospital sizes, budget and staff, cloud systems can be cost effective.

2. Easy Access and Portability

Information sharing can be facilitated through the use of cloud computing services. Broad network access will allow the hospital to use a number of devices within the hospital to connect to the cloud, these include workstations, tablets, laptops, etc. This can increase organizational flow, and reduce treatment time and delays (Cloud Customer Council 2012). For instance, before the advent of EMRs, paper medical records had to be physically tracked down if a doctor or nurse needed that information. Now, with broad network access, anyone with a device and correct authorization may look up information right away. In addition, non-collocated medical providers would be able to view the same record if needed.

For any movement to the cloud, healthcare organizations must consider the matter of data portability. This concern addresses the ability to transfer data from different sources to another cloud provider or back to the hospital system without disrupting operations or creating conflicting claims to the data (Cloud Standards Customer Council 2012). If in any case, the cloud service provider is unable to maintain operations, it will be impossible for hospitals to access its records. Therefore, a high capability for data portability will allow some risk mitigation, if in case the hospital needs to switch services. Data portability also refers to the necessary management strategies that allow EMRs to be available to authorized personnel on a number of devices. These devices should include workstations and mobile devices that can readily access the EMRs virtually anywhere in the hospital. These devices would of course, require the necessary

technologies such as data encryption to comply with all the required regulations and organizational procedures.

3. Scalability

Planning for growth is essential. As healthcare organizations grow, so will their demands for a computing capacity and IT resources. The cloud service provider must be able to handle this growing demand. Scalability is an important consideration when choosing a cloud service provider. The hospital will need to know when or if it needs to expand so that the cloud service provider will be able to scale the services. According to Ahuja, Mani and Zambrano (2012), "since the cloud provides a scalable infrastructure, the organization may be able to better adjust and optimize their resource capacity planning." If the healthcare organization is a smaller hospital, it will be able to take advantage of this aspect to scale up if they grow, or scale down if they experience some lack of demand. With a cloud-based system comes increased flexibility for the hospital in terms of rapid elasticity and measured services. As the hospital's needs grow, so may the capabilities of their chosen cloud service. Rapid elasticity allows the cloud service to be scaled in and out, depending upon the hospital's demands while measured service optimizes the system by monitoring, controlling, reporting, and providing transparency for both the service provider and the end user (Curran and Carlin 2013). On demand service allows the hospital a measure of autonomy from the service provider, allowing the hospital staff (with the correct rights and privileges) the opportunity to use the system when and how they want without resorting to contacting the service provider.

4. Reliability

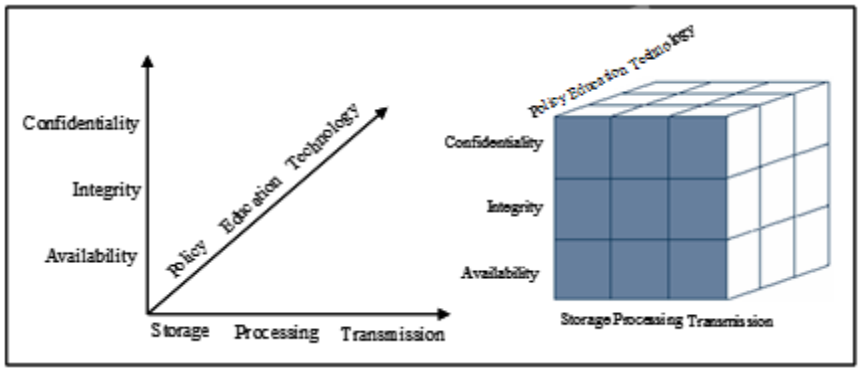
Any cloud service must provide an excellent level of reliability. Imagine if the necessary EMRs are needed to be retrieved but cannot for any reason, people may lose their lives. While any cloud system may suffer outages, the service must meet demands that call for high performance, availability, and reliability standards. According to the Cloud Standards Customer Council (2012) report, cloud service providers on the average maintain an uptime of 99.948% every year with the best providing 99.9994%. This equates to 273 minutes per year of unavailability for the

average and 3 minutes at its best. This level of uninterrupted service is especially necessary for any healthcare organization to have unfettered access to its records if and when it needs them. Lives may depend on it. Aside from the normal day to day service availability that must be maintained, the cloud service provider must have a disaster recovery plan in place to assure business continuance. Any service level agreements with a cloud service provider should detail these processes and procedures in a manner acceptable to the hospitals to maintain critical operations in case of a catastrophe at the provider level. Rodriguez et al. (2013) recommend any cloud services to provide technical support and coverage to solve any type of problem 24 hours a day, 365 days a week.

Ⅳ. Challenges of Cloud Computing in Healthcare Operations

1. Security in Healthcare

Transitioning health information to the cloud has had some challenges, particularly in terms of information security and privacy. In order to deal with various security threats or dangers, the National Security Telecommunications and Information Systems Security Committee (NSTISSC) security model has been utilized because it suggests a more detailed perspective on security (see Figure 2) (Krisnamurthy, Clifton, and Bishop 2004).



<Figure 2> NSTISSC Security Model

With HIPAA compliance mandatory, storing EMRs in a cloud-based architecture means taking extra precaution to ensure the data's safety and confidentiality. The hospital must trust its trade to cloud service providers, so any provider in turn must place all due priority on security measures to avoid any unauthorized access and data breaches. Security issues that must be considered by both client and provider include role-based access, network security mechanisms, data encryption, digital signatures, and access monitoring (Rodriguez et al. 2013). Any security measures will be meant to ensure that the data maintains confidentiality and integrity while being available to the organization at a moment's notice. This means that the cloud-based provider must guarantee the same level of security as if the healthcare organization was hosting the data in on-site systems. A security mechanism integral to any EMR storage system is the role-based access. Ensuring that only the correct personnel have access to the EMRs is paramount to its success. Rodriguez et al. (2013) recommend "ID codes or numbers be assigned to each person allowed access to the stored information." Different personnel will have different rights. Doctors will be able to have access to the whole medical record while IT staff only has access to the information needed for maintaining proper system capability. In addition, data encryption ensures that the data in the EMR is controlled, so that only doctors or medical personnel may share it. Digital signatures provides authenticity, integrity and non-repudiation. These will help against unauthorized transactions and detrimental changes to the data, as well as providing confidence that sent data is coming from a verified and trusted source. To that end, also monitoring system access will enable incident mitigation if in case there is one. There are, as always, some drawbacks to any solution and this has its share of it. According to Kuo (2011), the main challenges to the implementation of cloud computing in a healthcare setting are "lack of trust in data security, privacy by users, organizational inertial, loss of governance, and uncertain provider's compliance." All these matters must be weighed against the potential benefits, and any concerns must be addressed. Lee (2013) proposes official electronic document system as a trusted organization to store and manage electronic medical record in Korea.

(1) Managerial Security

Successful implementation of the system is not just a technical matter but an organizational one. To utilize the cloud, users must have trust in it. As Kuo (2012) points out, "trust is at the heart of the resistance many customers have to the cloud." These trust issues arise whenever there

is a change, but also when there is a new technology being introduced that is still in its infancy. Hospitals would also lack full control over data and processes, since it is the third party which would handle confidential data. Any service provider that a hospital chooses must share in the responsibility of data security. Furthermore, any vendor that the healthcare organization decides to utilize must absolutely be HIPAA compliant. Regardless of that requirement, any security breach that occurs would be purely the hospital's responsibility, as per HIPAA regulations. The drawbacks for a cloud computing solution are significant. While less costly upfront, and perhaps mostly over time, a subscription service has the potential to become more and more expensive as the hospital grows.

(2) Technical Security

With customization and integration of the new hardware, the hospital purchases can become an issue. In addition, the system must also be internet dependent, meaning, any possible internet outages for the hospital can be potentially disastrous. Managing these risks has had limited success in the realm of healthcare. Lohr, Sadeghi and Winandy (2010) identified several cloud vulnerabilities in the areas of data storage and processing areas that require improvement, particularly in the area of the authentication of users. Additional security concerns that require attention prior to transitioning health records to the cloud are access control, network security, data encryption, digital signatures and access monitoring (Rodrigues, de la Torre, and Lopez-Cornado 2013). Shin and Park (2005) propose digital signatures to protect and manage electronic medical records in Korea. Basic implementation of access controls is insufficient in managing the security risks in the cloud. Lohr et al (2010) suggest an oversight of key encryptions keys to audit and manage the use of ciphers in this environment in order to authenticate and/or regulate users of the system so that there is prevention of security protocol violations. Another example that increases vulnerability is end-user systems. It may be vulnerable to viruses or other malware, particularly in a small practice environment. It is suggested that security mechanisms are implemented prior to information migration to the cloud, as well as, regular maintenance of both hardware and software to ensure adequate protections. To bolster the security and privacy of e-health cloud systems, there are several technical solutions. Lohr et al (2010) suggests the implementation of 'privacy domains', which isolates certain healthcare applications (billing, electronic health record, ancillary) from one another. This adds an additional

level of security as only authenticated personnel can access sensitive health information, restricting those who are not authorized. Furthermore, the use of a security framework such as the trusted virtual domain is invaluable to ensuring information security. Qualities of a trusted virtual environment include isolation protocols, authentication measurements and secure communications. Additionally, there is a concern that some cloud providers are not adequately prepared to manage the security and privacy protocols dictated by the US Federal Information Security Management Act. Prior to adopting the use of the cloud platform, health organizations must carefully assess the cloud provider's ability to manage a variety of security issues, such as monitoring and auditing protocols, physical security of data storage, employee practices and environmental safeguards (Rodrigues, de la Torre, and Lopez-Cornado 2013). These mechanisms encourage a dialogue between customer and vendor to ensure transparency and increase trust. Furthermore, in order to ensure best practices from both parties, an external auditing company that monitors business practices is essential.

2. Inflexibility

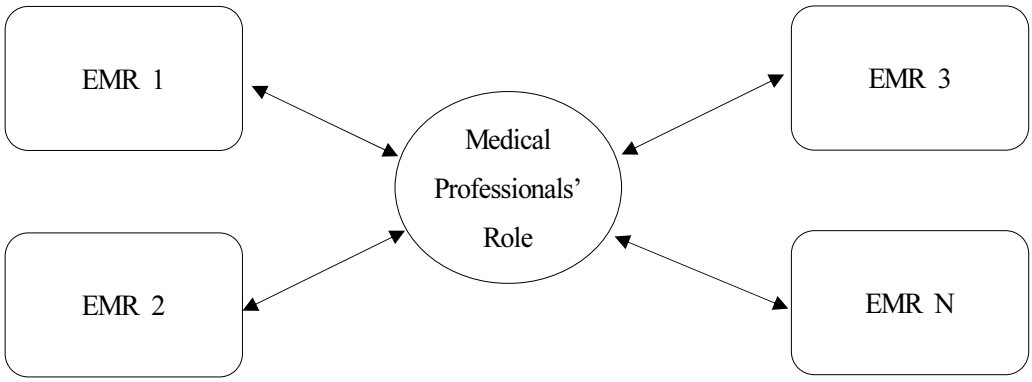
Integration and interoperability will prove to have some big challenges in moving EMRs to the cloud. According to Myers (2012), interoperability for health care systems must occur at the provider, software, computer and data levels. This is due to the many health care systems utilizing uncommon data modeling constructs which result in different database architectures as well as incompatible systems. In preparation for movement to the cloud, the healthcare organization and the cloud service provider must integrate their existing systems with modern web and cloud based systems as well as standardizing the processes and procedures. Such integration must occur at both the system and data level across all parties involved.

Ⅴ. Discussions

1. Role-Based Access Controls

Regardless of the software and hardware type chosen for the EMR, role-based access controls

are an essential network security method that needs to be implemented. There are two types of access controls: Mandatory Access Controls (MAC) and Discretionary Access Controls (DAC). MAC is appropriate for military operations and DAC is often used in industry management. Role-based access control is a type of DAC (Ferraiolo and Kuhn 1992). As shown in Figure 3, medical professionals take different roles to access electronic medical records.



<Figure 3> Role-based Access Controls in Healthcare

According to a legal report published by IBM in response to HIPAA and HITECH regulations on business associates, "it is the customer's responsibility to define who should have access to the data it stores in the cloud, and the cloud provider's responsibility to enforce these decisions" (Gilmer 2013). Due to the flexibility and "care comes first" nature of the hospital environment, role-based access controls should be flexible enough to allow emergency access, yet strong enough to prevent unauthorized access and allow monitoring. The controls should identify employees uniquely; each employee should have a distinct log-in (Kahn and Sheshadri 2008). For both information security and patient safety reasons, users should use their own log-in when documenting care in the EMR, rather than having generic roles such as "nurse" or "pharmacist" that are on shared computers. The role-based access controls should provide the minimum access necessary for job performance (Kahn and Sheshadri 2008). For example, a nursing aid may have no reason to be able to view the patient's demographic information, such as address and social security number. Unlike in a business environment, where access to an account might be limited based on the sales team assigned to the client, in emergency situations there may be unexpected changes to the care team, and there is no time to wait for advance authorization of actions

(Ardagna et al. 2010). For example, when a patient arrives in the emergency room, physicians and nurses assigned to the patient need to immediately have access to that patient's medical history. Even in longer inpatient stays, there is a potential that a physician who primarily practices at one of the hospital's other physical locations may be filling in at a different location; in this case, the physician should be able to override access controls to instantly obtain access to information needed for patient care. To balance out this required flexibility, auditing and user tracking are important. These audit logs can be analyzed using data mining for actions that are unexpected and should be reviewed for potentially unauthorized access. Companies can also employ multi-factor authentication for riskier scenarios that are not time-critical. For example, someone accessing the EMR over a home internet connection is clearly in a setting of doing follow-up or preparing for appointments, rather than making life-or-death decisions in a hospital setting. Since they are accessing the system outside of the hospital, it also poses a higher level of risk that the user is not the authorized user. In this case, two-factor authentication, such as requiring a randomized passcode that is sent by text-message to a pre-enrolled smartphone, can improve the strength of the authorization without detracting from patient care.

2. Network Security

If networks are left vulnerable and data unencrypted, potential data breaches due to unauthorized access must be reported under the HITECH Breach Notification Final Rule. However, this requirement does not apply if the organization appropriately secures the information using network and information security methods. According to the Department of Health and Human Services, this regulation is in place as part of meaningful use requirements in order to maintain consumer trust (Department of Health and Human Services, 2009). Data breaches affecting over 500 individuals must be promptly reported to the affected individuals, the HHS Secretary, and the media, while smaller breaches are reported annually to the HHS Secretary. In order to be exempted from this rule, and to have network security best practices for their health information systems, organizations such as those in healthcare must employ encryption and destruction security methods as specified by the HHS and FTC regulation. To be classified as secured, the technology must make the protected health information "unusable, unreadable, or indecipherable to unauthorized individuals (Department of Health and Human Services, 2009).

3. Mobile Device Management

Along with the benefits of rapid access to electronic health record using mobile devices comes a risk of unauthorized access if the device is lost or stolen. The organization should have policies in place regarding storing health information on the mobile device, and plans to wipe or disable it if lost. Logging in to the EMR, especially a web-based SaaS EMR, over a mobile device may be as simple as a username and password. Passwords are required to be strong and should be changed frequently. Organizations should have policies that prevent users from storing PHI directly on their mobile device (HealthIT.gov 2014b). All information should be kept within the web-based EMR software, so it can be password protected and backed up in a secured server. In fact, having an EMR that is mobile-accessible may help encourage users to keep activities within the secure system, rather than emailing themselves information, copying into documents, or storing it in some other less secure way for future mobile use. In addition, users should enroll the mobile devices they will be using to log in to the EMR. This will allow the organization to remotely wipe the device, erasing all of its data, or remotely disable the device, by locking it, if it is lost (HealthIT.gov 2014b). With an appropriate policy and user compliance with not storing any information on the device, these mobile device management processes offer an extra layer of security. A key component to a mobile device privacy and security plan is training. In the words of HealthIT.gov, “safeguards will not protect health information unless providers and professionals are trained to follow and enforce those safeguards (HealthIT.gov 2014b).” Training should include security training specific to mobile devices, security awareness, reinforcement of steps to take if a device is lost, and security best practices.

Ⅵ. Conclusion

Organizations must leverage the benefits against the challenges and detriments of upgrading their information systems to include a cloud-based storage system. However, unlike other organizations, as health care providers, hospitals must take special considerations when choosing a cloud storage. Any strategic planning must examine factors such as HIPAA compliant security, data portability, integration and interoperability, and uninterrupted service. This paper examined

the benefits from the healthcare perspective that the cloud has to offer while cautioning about the challenges. Cloud computing can be a good decision for healthcare industries because they look for a cost-effective solution that provides scalability, backup, and data protection. Cloud computing also provides a broad network access that allow the hospital to use a number of devices such as tablet within the hospital to connect to the cloud. Therefore, medical professionals can access the EMRs virtually anywhere in the hospital. The system can also be easily expanded. However, there are some challenges in using cloud computing for healthcare. While any cloud system may suffer outages, the service must meet demands that call for high performance, availability, and reliability standards. In addition, HIPAA requires EMRs records in a cloud-based architecture to meet the data's safety and confidentiality standards. Since hospital systems have been developed under different vendors and standards, integration and interoperability of systems are critical challenges in moving EMRs to the cloud. Cloud computing offers compelling advantages, and should hospitals overcome those challenges, they will find themselves better for it. In order to maximize the benefits of cloud-based EMR, role-based access controls, security, and mobile device management must be considered.

References

Ahuja, S. P., Mani, S., and Zambrano, J. 2012. "A survey of the state of cloud computing in healthcare." *Network and Communication Technologies*, 1(2): 12-19

Apostu, A., Puican, F., Ularu, G., Suciu, G., and Todoran, G. 2013. "Study on advantages and disadvantages of Cloud Computing-the advantages of Telemetry Applications in the Cloud." *Recent Advances in Applied Computer Science and Digital Services*. New York: Wseas: 118-123.

Ardagna, C. A., De Capitani di Vimercati, S., Foresti, S., Grandison, T. W., Jajodia, S., and Samarati, P. 2010. "Access control for smarter healthcare using policy spaces." *Computers & Security*, 29(8): 848-858.

Botts, N., Thoms, B., Noamani, A., and Horan, T. A. 2010. Cloud computing architectures for the underserved: Public health cyberinfrastructures through a network of healthatms. In System Sciences (HICSS), 43rd Hawaii International Conference.

CareCloud. 2012. How Modern Technology Helped a Multi-Location Orthopedic Group Boost Financial Results and Reporting. White Paper.

Carpathia. 2013. *5 Benefits of EMR vs. Paper Medical Records*. <http://carpathia.com/blog/5-benefits-of-emr-vs-paper-medical-records/>

Congdon, K. 2014. *Is Epic Future Proof?*. <http://www.healthitoutcomes.com/doc/is-epic-future-proof-0001> [cited 2015. 7. 28].

Cloud Standards Customer Council. 2012. *Impact of Cloud Computing on Healthcare*. <http://www.cloud-council.org/deliverables/CSCC-Impact-of-Cloud-Computing-on-Healthcare.pdf> [cited 2016. 3. 10].

Curran, K., and Carlin, S. 2013. Cloud Computing Security. In Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments. Hershey: IGI Global.

Danny Yadron, and Beck, M. 2015. *Health Insurer Anthem Didn't Encrypt Data in Theft.* <http://www.wsj.com/articles/investigators-eye-china-in-anthem-hack-1423167560> [cited 2015. 4. 28].

Department of Health and Human Services. 2009. *HITECH Breach Notification Interim Final Rule*. <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html> [cited 2015. 4. 28].

Egdom, R. V. 2013. *7 Benefits of a Cloud-Based EHR*. <http://www.hitechanswers.net/7-benefits-cloud-based-ehr/> [cited 2015. 5. 2].

Ferraiolo, D. F., and Kuhn, D. R. 1992. Role-Based Access Controls. Paper presented at the 15th National Computer Security Conference, Baltimore MD.

Gilmer, E. 2013. Privacy and security of patient data in the cloud. IBM Developer Works. <http://www.ibm.com/developerworks/cloud/library/cl-hipaa/> [cited 2015. 5. 28].

Gunter, T., and Terry, N. 2005. “The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions.” *Journal of Medical Internet Research*, 7(1).

Hanuscak TL, Szeinbach SL, Seoane-Vazquez E, Reichert BJ, and McCluskey CF. 2009. “Evaluation of causes and frequency of medication errors during information technology downtime.” *American Journal of Health System Pharmacy*, 66(12): 1119-1124.

HealthcareITnews.com. 2014. *Network Glitch Brings Down Epic EMR*. healthcareITnews.com: <http://www.healthcareitnews.com/news/network-glitch-brings-down-epic-emr> [cited 2015. 5. 18].

HealthIT.gov. 2014. Benefits of EHRs. <http://www.healthit.gov/providers-professionals/improved-care-coordination> [cited 2015. 5. 13].

Kahn, S., and Sheshadri, V. 2008. “Medical record privacy and security in a digital environment.” *IT Professional*, 10(2): 46-52.

ICare.com, 2013. *The Enterprise Cloud EHR – Products*. White Paper.

Krisnamurthy, Prasant, Chris Clifton, and Matt Bishop. 2010. *Introduction of Computer Security*. <http://www.sis.pitt.edu/~jjoshi/TELCOM2813/Spring2005/> [cited 2016. 3. 11].

Kuo, A. M. H. 2011. “Opportunities and challenges of cloud computing to improve health care services.” *Journal of medical Internet research,* 13(3).

Lee, H. 2013. “The Storage of Electronic Medical Record and Trusted Third Party.” *Han Yang Law Review*, 44: 123-149.

Löhr, H., Sadeghi, A. R., and Winandy, M. 2010. Securing the e-health cloud. Paper presented at the 1st ACM International Health Informatics Symposium.

Maheu, M. 2014. Which Cloud Storage Services are HIPAA Compliant |TMHI Blog. <http://telehealth.org/blog/which-cloud-storage-services-are-hipaa-compliant> [cited 2015. 5. 28].

Mars, M. 2013. “Telemedicine and Advances in Urban and Rural Healthcare Delivery in Africa.” *Progress in Cardiovascular Diseases*, 56(3): 326-335.

McCann, E. 2014. Network glitch brings down Epic EMR. <http://www.healthcareitnews.com/news/network-glitch-brings-down-epic-emr> [cited 2016. 3. 10].

Meditouch. 2014. *Web-Based EHR – Cloud-Based, SaaS, ASP*. HealthFusion.com. <http://www.healthfusion.com/ehr-software/web-based-ehr/> [cited 2015. 2. 23].

Myers, J. E. 2012. *Data Modeling for Healthcare Systems Integration: Use of the Meta Model*. <http://www.metadata.com/whitepapers/myers1.pdf> [cited 2015. 6. 28].

Mell, P., and Grance, T. 2011. *The NIST definition of cloud computing*. <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> [cited 2016. 3. 2].

Miller, S. A., and Blass, G. 2010. “Protection detail: Protecting against breach of electronic protected health information.” *Journal of Healthcare Information Management*, 24(3): 7-8.

Rodrigues, J. J., Torre, I. d. l., Fernández, G., and López-Coronado, M. (2013). “Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems.” *Journal of Medical Internet Research*, 15(8): 186.

Rolim, C. O., Koch, F. L., Westphall, C. B., Werner, J., Fracalossi, A., and Salvador, G. S. 2010. “A cloud computing solution for patient's data collection in health care institutions. In eHealth, Telemedicine, and Social Medicine, 2010.” ETELEMED'10. Second International Conference: 95-99

Roney, K. 2012. *5 Best Practices for Negotiating, Beginning the Transition to Cloud Servers*. <http://www.beckershospitalreview.com/healthcare-information-technology/5-best-practices-for-negotiating-beginning-the-transition-to-cloud-servers.html> [cited 2015. 6. 12].

Sabahi, F. 2011. Cloud computing security threats and responses. In Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference.

Schweitzer, E. J. 2012. "Reconciliation of the cloud computing model with US federal electronic health record regulations." *Journal of the American Medical Informatics Association*, 19(2): 161-165.

Shin, Y, and Park, J. 2005. "Development of Guideline on Electronic Signatures for Electronic Medical Record." *Journal of the Korea Contents Association*, 5(6): 120-128.

Taylor, K. 2013. ASAE ® The Center for Association Leadership. <http://www.asaecenter.org/Resources/ANowDetail.cfm?ItemNumber=331733> [cited 2015. 6. 20].

Williams, F., and Boren, S. A. 2008. "The role of electronic medical record in care delivery in developing countries." *International Journal of Information Management*, 28(6): 503-507.