Proposing an Intelligent Cloud-Based Electronic Health Record System

Lara Khansa, Virginia Tech, USA
Jonathan Forcade, Virginia Tech, USA
Girivaraprasad Nambari, Virginia Tech, USA
Saravanan Parasuraman, Virginia Tech, USA
Patrick Cox, Virginia Tech, USA

ABSTRACT

With the aging United States population, healthcare costs have considerably increased and are expected to keep rising in the foreseeable future. In this paper, the authors propose an intelligent cloud-based electronic health record (ICEHR) system that has the potential to reduce medical errors and improve patients' quality of life, in addition to reducing costs and increasing the productivity of healthcare organizations. They developed a set of best practices that encompass end-user policies and regulations, identity and access management, network resilience and service level agreements, advanced computational power, “Big Data” mining abilities, and other operational/managerial controls that are meant to improve the privacy and security of the ICEHR, and make it inherently compliant to healthcare regulations. These best practices serve as a framework that offers a single interconnection agreement between the cloud host and healthcare entities, and streamlines access to private patient information based on a unified set of access principles.

Keywords: Clinical Decision Support System, Cloud Computing, Electronic Health Record System, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Privacy, Security

INTRODUCTION

Healthcare expenditures in the United States (U.S.) reached 17.9% of the country’s gross domestic product (GDP) in 2011, and healthcare spending is projected to grow at a rate of 6.2% annually through 2021 (Centers for Medicare & Medicaid Services, 2010). According to the health division of the Organization for Economic Co-operation and Development (OECD Health Division, 2011), the United States spent over $8,000 per capita on healthcare in 2010, two-and-a-half times higher than the corresponding average per capita health expenditures of all other developed nations. As people live...
longer, and the U.S. population gets older, this trend is expected to continue with no easy fix.

With its ability to reduce medical errors and improve patient safety and quality of living, Health Information Technology (HIT) is viewed by many as an enabler of a revamped U.S. healthcare system (Institute of Medicine, 2001). HIT’s benefits are expected to further materialize into increased productivity and reduced costs through faster and more reliable information sharing and integration across healthcare professionals and healthcare institutions (Blumenthal, 2011). A 2006 study conducted at the University of Minnesota analyzed the costs and benefits of one such technology, telehealth that consists of remotely monitoring the well-being of patients using HIT. The study was conducted by creating three separate groups of patients. The first control group received traditional skilled nursing care at home. The second group received traditional skilled nursing care at home and virtual visits using videoconferencing technology. The third and last group received traditional skilled nursing care at home, virtual visits using videoconferencing technology, and physiologic monitoring for their underlying chronic condition. Within 6 months of study, no differences in mortality or morbidity were found between the groups. The average visit costs were $48.27 for face-to-face home visits, $22.11 for average virtual visits, and $32.06 and $38.62 for average monitoring group visits for congestive heart failure and chronic obstructive pulmonary disease subjects, respectively. The results of the study showed that virtual visits and monitoring by skilled healthcare practitioners of chronically ill patients can provide positive patient outcomes at a lower cost compared to traditional face-to-face meetings (Finkelstein et al., 2006).

Despite all of its potential, HIT has historically faced many barriers to acceptance and adoption by healthcare practitioners because of its high implementation and maintenance costs, difficulties of integration with legacy health infrastructures, the lack of standards that ensure interoperability between various HIT components, and the time and effort required for learning and training. In addition, patients have thus far shown meager interest in adopting pricey HIT products and services, and have expressed concerns about sharing their private information online. For example, the free Google Health service shutdown after only a few years of operation because of lack of adoption by patients (Google, 2011).

Organizations in the US that furnish, bill, or receive payment for healthcare, and transmit or perform transactions involving an individual’s protected health information (PHI) are required to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Title I of HIPAA is aimed at ensuring that no patient is denied insurance coverage based on health conditions, and at limiting coverage exclusions based on preexisting health conditions (U.S. Department of Labor, 2004). Title II of HIPAA has promoted the standardization of healthcare through using HIT in an effort to ensure that patients’ private information is protected and transferred securely (Centers for Medicare & Medicaid Services, 2012). The fundamental issues of privacy loss and excessive costs that permeate HIT were addressed in the American Recovery and Reinvestment Act (ARRA) that was signed into law by President Obama on February 17, 2009. ARRA allocated $300 million for improving health information exchanges, $20 million to the National Institute of Standards and Technology (NIST) to develop standards and enhance system interoperability, and $1.5 billion for health IT system upgrades in public health centers (Hoyt, 2009). Most importantly, ARRA included a provision stipulating over $19 billion in funding to establish a national electronic health record (EHR) system that enforces stringent security measures to protect patients’ private information (Khansa et al., 2012). This provision, called the Health Information Technology for Economic and Clinical Health (HITECH) act, was meant to “promote the adoption and meaningful use of health information technology” (U.S. Department of Health and Human Services, 2009a, p. 56124). Further, Title XIII of HITECH specifically encouraged healthcare institutions to adopt EHR systems.
by offering them a total compensation of over $17.2 billion (Hoyt, 2009).

The Healthcare Information and Management Systems Society (HIMSS) defines an EHR as “a longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting” that includes “patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports” (Healthcare Information and Management Systems Society, 2012). EHR systems have been considered the lynchpin that can pull together and integrate disparate healthcare systems, and are consequently expected to foster a community of collaboration. By offering a central repository where healthcare data is kept up-to-date and accurate, EHR systems reduce the reliance on patients to recall and constantly repeat their medical history. This is particularly important with elderly individuals and those on multiple medications that may have been prescribed by different physicians. It is not uncommon that different physicians prescribe to the same patient medications that negatively interact with each other. Additionally, without a fully integrated EHR system there will always be a certain level of manual intervention between various levels of care, which makes medical errors even more probable.

In this paper, we propose an intelligent cloud-based EHR system (ICEHR) that streamlines healthcare services and leverages cloud computing to lower the costs of EHR development, testing, and delivery to healthcare institutions and patients. Cloud computing has been used to describe a wide variety of technical capabilities and delivery models in the past several years. Typically these definitions fall within the broad categories of Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) (Grossman, 2009) where each of these terms refers to a progression of managed capabilities from basic technical infrastructure building blocks (e.g., compute, storage, and networking) through feature rich, industry-specific, fully managed applications. Complex issues regarding data protection and breach notification regulations, compliance with privacy laws, and storing data on sensitive information such as mental health or substance abuse problems would accompany migrating EHR systems to the cloud (Choo, 2011; Chaudhuri et al., 2011). To address these issues, we further develop a set of best practices.

The proposed ICEHR is designed to assist healthcare professionals in mining the past health history data of multiple patients and recommending/suggesting medications and/or treatments. The ability to make the right decisions faster is expected to save patients’ lives. It can also be used to considerably reduce costs across the board to patients, healthcare institutions, and insurance companies by assisting doctors in providing effective telehealth to remotely-located patients. The predictive capability of the proposed ICEHR can also support medical research and help detect national or worldwide disease outbreaks.

The rest of this paper is organized as follows. In the following section, we present current examples of completed or nearly completed implementations of EHR systems, and highlight their shortcomings. We then present our proposed ICEHR system that addresses most of these shortcomings. We complement the design of the ICEHR with a set of best practices that strengthen its security and privacy characteristics, and its analytical capabilities. Finally, we conclude by summarizing our contributions and setting avenues for future research.

CURRENT EHR SYSTEMS AND SHORTCOMINGS

EHRs in the Military

The Armed Forces Health Longitudinal Technology Application (AHLTA) is a U.S. Army electronic medical record (EMR) that can be used to track the health and well-being of soldiers while at home and in combat. Note that EMRs are usually housed within the confines of a specific healthcare organization or network, whereas EHRs refer to the larger nationwide system that encompasses and connects EMRs.
AHLTA connects to the U.S. military’s central health database, called the clinical data repository (Buxbaum, 2010), and can be remotely accessed via a Web-based interface called the Theater Medical Data Store (Buxbaum, 2010), as well as via the AHLTA-Mobile application that runs on smart phones. AHLTA-Mobile provides real-time access to army personnel’s health history information, medical reference material, and point of injury clinical documentation (Geesey, 2012).

Despite its ability to provide up-to-date health information in real-time, the AHLTA EMR system has been criticized for its complexity and user unfriendliness (Versel, 2010). A variant of this EMR system is the Virtual Lifetime Electronic Record (VLER) system that integrates the AHLTA infrastructure with the Veterans Health Information Systems and Technology Architecture (VistA) EHR system (http://www.ehealth.va.gov/VistA.asp). The goal of this integration is to provide secure access to a common centralized repository. Once completed, the VLER initiative will be the first embodiment of a complete EHR system that allows for reduced duplication of data, improved ease of integration into civilian society for a soldier, and time saved across the board by having patients’ full history available regardless of the clinical setting.

**National Health Information Network and Infrastructure**

The U.S. Federal government is developing a Nationwide Health Information Network (NHIN) via the U.S. Department of Health and Human Services (HHS). The NHIN is as a “network of networks” (Nationwide Health Information Network Exchange, 2010, p. 4) whose primary purpose is to “enable health information to follow the consumer” (Nationwide Health Information Network Exchange, 2010, p. 4). HHS specifically states that the “NHIN will not include a national data store or centralized systems at the national level” (Gartner, 2007, p. 2). Instead, it seeks to interconnect health information exchanges maintained by providers.

The business problem that the NHIN attempts to solve is that of enabling data communication between related entities that are part of the healthcare experience for the customer. By enabling this communication, entities are assured to reach any other participating entity through a secure network sponsored by the Federal government. Organizations have begun to adopt the NHIN and, in particular, are leveraging it in order to transfer data to the government. In June of 2012, Kaiser Permanente announced that it was utilizing the NHIN in order to file disability claims with the Social Security Administration (Poorsina, 2012).

The National Committee on Vital and Health Statistics (2001a) created a report outlining a vision and process for “a comprehensive, knowledge-based system capable of providing information to all who need it to make sound decisions about health” (p. 1) that they call a National Health Information Infrastructure (NHII). Comprised of “values, practices, relationships, laws, standards, systems, and applications that support all facets of individual health, healthcare, and public health” (National Committee on Vital and Health Statistics, 2001b, p. 17), the NHII is akin to the NHIN but further introduces the idea of patient access to various sources of information, such as healthcare providers and insurance companies. The NHII frequently asked questions (FAQ) site (http://aspe.hhs.gov/sp/NHII/PrintableFAQ.html) specifically points out that the NHII is “NOT a centralized database of medical records or a government regulation.”

**Shortcomings of Current EMR Implementations**

One of the greatest challenges of data reconciliation exists when disparate data islands are formed by disconnected information systems. An example of this would be when a patient checks into one health organization and identifies that he or she has had surgery a few years back. Because he or she cannot remember the specifics, the individual approximates the date of the surgery during admission. The actual date
of the surgery is known to the provider who conducted the surgery and exists within their database. However, once the patient registers the incorrect date at the new provider, a data disparity is created with respect to when the actual surgery took place. One possible means for mitigation would be for the new provider to pull that information from the previous provider so that it minimizes the chance for error. However, this assumes that the new provider has an interconnection agreement with the old provider and can access the relevant information. Additionally, once the new provider is aware of the information, they create another instance of the data, possibly without a dependency upon the original source. Because of these disconnected islands of data, there is no referential integrity that would ensure that updates cascade through to dependent data sets.

Any organization that maintains sensitive data strives to create a security boundary that protects their private information from external access. Since there are a lot of external entities that need access to the data, the organization has to establish technical, administrative, and operational controls to permit access to their data. Outside organizations that access the information should formally agree to an interconnection agreement that identifies the type of access and how accessed data should be handled. The NHIN creates a pathway for multiple entities to access the provider’s network. Although controls would likely be installed by the provider to limit security exposure, the burden would essentially be the same as in the case of an organization who hosts a Web site on the Internet. Although the partners on the NHIN are “more trusted” they can still suffer from malware outbreaks and insider threats.

Administratively, the NHIN will not alleviate the burden of managing interconnection agreements with partner entities. HIPAA requires that partners agree to a chain of custody associated with patient records and that proper safeguards meeting these requirements are leveraged in order to ensure continuity of patient data security. Essentially, the NHIN builds a government version of what healthcare entities do today over the Internet or through private connections. The NHII identifies a set of standards that can be leveraged for a healthcare information exchange with Orion Health (http://www.orionhealth.com/) being an example of a private version that they offer to healthcare providers.

In summary, the primary missions of the NHII and NHIN miss the mark in a number of areas that include: exacerbating the disparate data island phenomenon, not offering an infrastructure that safeguards patient data, and creating yet another pathway for external parties to reach into an organization’s sensitive patient infrastructure. Safeguarding patient data goes beyond ensuring that it is secure during transit. The NHIN offers assurance that communication will be protected; however, the “network of networks” that it offers is really another form of Internet. Granted, there will be more checks and balances around members registering prior to joining this network, NHIN does not attempt to control access to patient information explicitly. However, the NHII raises the bar by asserting that it offers more prescriptive guidance on how to use their infrastructure.

PRIOR LITERATURE ON CLOUD-BASED EHR DESIGNS

Schweitzer (2011) argued that cloud computing is effective as it provides various EHR system functionality in the form of modules to small health practices that seek rapid compliance with the HITECH meaningful use requirements. Haughton (2011) and Kabachinski (2011) also argued that cloud computing can reduce EHR systems’ initial implementation costs that result from the need for extra firmware, trained personnel, and licensing fees. Rosenthal et al. (2010) advocated cloud computing as a new computing paradigm that can be used to further innovation in biomedical informatics through data and applications sharing. It has also been shown that cloud computing offers an inexpensive computational solution that addresses the complexity and data handling problems
surrounding biomedical informatics (Anderson et al., 2007; Bateman & Wood, 2009; Dudley et al., 2010; Kudtarkar et al., 2010; Schatz et al., 2010; Wall et al., 2010). Steele et al. (2012) focused on cloud-based personal health records (PHRs) and cited their advantages as “greater fault-tolerance and resiliency, interoperability, flexibility of data access and sharing, data integration, and trusted collaboration” (p. 1084).

Several designs of cloud-based EHR systems have thus far been proposed. For instance, Rolim et al. (2010) proposed real-time collection and processing of patients’ vital information, such as glucose levels for diabetics, using a network of sensors connected to the cloud. Such a system would eliminate the need for manual collection and the possibility of human error, and ultimately saves human lives. Similarly, Nkosi and Mekuria (2010) proposed adding a cloud-based security as a service system to mobile devices to improve their usability in healthcare delivery to rural communities. Rao et al. (2010) and Koufi et al. (2010) discussed two cloud computing initiatives that leverage wireless technologies to provide healthcare professionals with anytime-anywhere access to their patients’ vital information.

These designs, while attempting to leverage cloud computing for better healthcare, lack two important ingredients. First, they do not specify who will manage patients’ private information, nor do they suggest effective ways to ensure that this private information is kept safe and secure. Second, they do not show how patients’ information on the cloud can be intelligently mined to provide healthcare professionals with better decision making capabilities that improve patients’ lives.

**INTELLIGENT CLOUD-BASED EHR SYSTEM**

Establishing an intelligent cloud-based nationwide EHR system is value-generating for patients, healthcare professionals, and healthcare governmental institutions for the following reasons. First, standardized cloud computing services offer a common platform to healthcare providers and patients that allows circumventing issues related to system interoperability and inefficiencies, and facilitate health information exchange between healthcare partners. Second, the self-service deployment and metered consumption that characterize cloud computing allow healthcare institutions to tailor-make their cloud usage by scaling up or down based on their workloads and number of patients, and to only pay for the services that are actually used. Third, the ubiquitous accessibility of the cloud allows for real-time access to vital patient information and, in turn, timely response to save patients’ lives, fewer medical errors and better quality of life, and fewer redundancies and lower healthcare costs. Fourth, advancements in cloud security innovations by industry leaders such as Amazon, Google, Microsoft, etc… makes cloud computing the best conduit to drive the EHR revolution. Last but not least, the cloud can provide a common platform for collaboration and knowledge-sharing in the healthcare industry. One example would be that of public health departments uploading health data in a timely manner to assist state and national health officials in identifying and tracking disease outbreaks and environment-related health hazards (McGee, 2008).

The Amazon Web Service (AWS) is widely recognized as one of the world’s largest cloud computing services that has been certified as compliant to most information security regulations, including HIPAA, and has been leveraged in a multitude of research efforts. Bateman and Wood (2010), for example, proposed using AWS to assemble a full human genome. Kudtarkar et al. (2010) also used the computational power of AWS to conduct genome-to-genome comparisons at a cost 40% less than that of other techniques. Additionally, the AWS has for instance made publicly available a large set of human genetic data that could be used for free public medical research (National Institutes of Health, 2012). Other cloud computing services include Microsoft’s HealthVault and Oracle’s Exalogic Elastic Cloud.
Figure 1 gives a graphical representation of the general functionality of the proposed ICEHR, and Figure 2 is a detailed view of the ICEHR’s clinical decision support system (CDSS) unit that provides healthcare providers with intelligent clinical and analytical capabilities. Hunt et al. (1998, pp. 1339-1340) define CDSS units as systems running “software designed to directly aid in clinical decision making in which characteristics of individual patients are matched to a computerized knowledge base for the purpose of generating patient-specific assessments or recommendations that are then presented to clinicians for consideration.” The proposed ICEHR’s CDSS allows quickly cross-referencing available prescription drugs against known side-effects and a patient’s history, thus cutting down on potential complications and the need for follow-up visits.

When a healthcare provider queries a specific patient’s information using the ICEHR’s user interface, the CDSS unit initiates a request to the ICEHR’s database on the cloud for that patient’s information. The doctor then enters the patient’s symptoms and other information such as age, existing health conditions, and family health history, among others. The CDSS unit then looks for all past comparable cases that best match the combination of symptoms, diseases, and other health conditions. The results are then filtered by the CDSS and only the top ten comparable cases and treatments are kept. The system makes a prediction on the patient’s diagnosis, and recommends a list of...
“best actions” including medications and other medical interventions after consulting the most up-to-date database of pharmaceutical database. Finally, the CDSS recommendations are displayed on the ICEHR interface for the doctor to use.

ICEHR BEST PRACTICES

One of the most important features of EHR systems is their ability to enforce healthcare institutions’ ownership of patients’ electronic PHI (ePHI) and enable healthcare providers to encrypt patients’ data and render it unreadable to humans. To achieve the flexibility and control that allow healthcare institutions to deploy HIPAA-compliant applications, there needs to be a shared-responsibility security model between healthcare providers and their cloud providers. In particular, several layers of physical, administrative, and technical controls are required on the cloud to ensure cloud resiliency and achieve compliance with HIPAA. First, healthcare organizations remain responsible for installing physical security safeguards including workstation and media security (U.S. Department of Health and Human Services, 2007a). Cloud providers need to enforce physical security at their end by making sure their data centers are highly-secure and resilient. Second, administrative safeguards comprise over half of the HIPAA security requirements. To comply with HIPAA’s administrative requirements, healthcare organizations are responsible for putting in place security management processes; security awareness and training; and security incident response procedures and contingency planning (U.S. Department of Health and Human Services, 2007b). Third, it is important that cloud providers abide by industry standards by offering HIPAA-compliant tools for accessing service endpoints, such as cryptography and authentication technologies, and access control, audit, and tokenization services.

The NIST report, “Guidelines of Security and Privacy in Public Cloud Computing” (Jansen & Grance, 2011), enumerated security and privacy challenges on the cloud as governance, compliance, data ownership and risk management, architecture, identity and access management (IAM), availability, and incident response. We built on the NIST categorization to develop a reference architecture that goes beyond the existing NHIN’s “network of networks” approach, offering a cloud-based data warehouse of patients’ ePHI and serving as the information nexus of health records. Instead of attempting to have every healthcare provider figure out how to establish communication protocols and interconnection agreements with every other potential partner, the proposed framework offers a single interconnection agreement for an entity with the cloud host (the Federal government, or a private company such as Amazon, Microsoft, Oracle, etc…). Access to patient data is controlled based on a unified set of access principles that every entity has to adhere to.

Given that technology continues to evolve at an increasing pace year after year, the concepts presented in this paper serve as a best practices’ architecture, rather than as a specific design. The architecture should remain fairly constant over time with details of implementation evolving to keep pace with technology and the security landscape. Implementation at any layer needs to be considerate of the relative burden placed on a participant or organization. The implementation costs need to scale appropriately, i.e., it would not be appropriate for a patient to have to purchase expensive equipment, applications, and communications in order to look at the history of their medical treatment. However, it might be reasonable to expect the patient to have access to an Internet-connected computer with a Web browser. Essential elements of the architecture are grouped within layers to offer an abstracted reference framework helping to conceptualize the architecture. These best practices, presented in Figure 3, encompass end-user policies and regulations, IAM, network resilience, service level agreements (SLAs), advanced computational power, “Big Data” mining abilities, and other operational/management controls. While the architecture could certainly be expanded to include more layers, our intent is to provide
enough detail to offer a working architecture and a set of principles without locking in on any particular technology.

**End User Policies & Regulations**

Fundamental to the success of any means to safeguard sensitive information is the idea that there are consequences to not adhering to the rules of accessing the data. That being said, existing laws will need to be expanded to ensure that providers who access patient information understand that they are responsible for ensuring the information they provide is accurate and timely, to the best of their knowledge. In addition, the laws need to ensure that everyone who has access to health information understands that they are not permitted to share or disclose the information outside of working with the patient or designated guardian and/or family.

Currently, patient privacy and data security requirements are defined by the HIPAA Privacy and Security Rules. The HIPAA Privacy Rule (U.S. Department of Health and Human services, 2002) establishes national standards for, among other things, defining who may access an individual’s medical records and other PHI, regardless of whether the information is in electronic or paper form. The HIPAA Security Rule (U.S. Department of Health and Human services, 2003) sets standards for ensuring that only those who should have access to PHI have access to it. The Privacy and Security Rules only apply to covered entities (CEs). At a high level, a CE is a healthcare provider, health plan, or healthcare clearinghouse. However, most CEs do not carry out all of their healthcare activities and functions by themselves. Instead, they sometimes leverage business associates for functions and activities including, claims processing or administration; data analysis, utilization review; quality assurance; billing; benefit management; practice management; and re-pricing (U.S. Department of Health and Human Services, 2009b). Recognizing that EHR systems would introduce new security and privacy challenges, the U.S. Congress included provisions in HITECH that expand HIPAA’s reach to business associates who can “access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured protected health information” (U.S. Congress, 2009, p. 1). The relationship between a cloud provider and a CE is currently under debate because it is unclear whether or not cloud providers qualify as business associates. According to the HHS, organizations who merely act as a conduit for PHI are not business associates (U.S. Department of Health and Human Services, 2009b).

Policies, standards, and guidelines need to be strengthened to educate participants about their rights and responsibilities as required by
the corresponding laws and regulations. This will require the drafting and adoption of a significant amount of documentation that needs to address a number of stakeholder groups including: patients, healthcare providers, insurance providers, legal representatives, and technical experts. This is important in that it spells out the expectations that ICEHR has towards entities that utilize its resources, as well as what entities expect from the ICEHR in return. Ideally, such policies, standards, and guidelines need to be structured so that the consequences are reasonable to the intent, and the punishment of any disclosure or violation is stringent enough to increase the likelihood of compliance. This is probably the most difficult layer that will very likely take the longest time to achieve within the architecture. It requires executive backing within the Federal government and the cooperation of many aspects of the various branches of government, private cloud providers, if any, and healthcare providers. An extra dimension to this layer is the impact that international entities have on being compliant with and held accountable for enforcing the laws enacted. It may be necessary for participating partner countries to enact similar laws to help ensure reciprocity; otherwise they will need to be excluded from accessing the information.

Identity & Access Management

The ICEHR should be designed in such a way to facilitate access to ePHI by authorized individuals and organizations that are either attempting to render healthcare-related services or providing payment for services that are rendered. The ICEHR interface has to be designed so as to adhere to the contextual presence of each user in a way that literally adjusts the features available to the user based on their authorized role. This layer has to enforce data protection and ensure that users accessing private data cannot "harvest" it for their own use. Additionally, it has to act as a universal interface for organizations that wish to use their own applications to transfer data updates to the ICEHR.

IAM technologies need to be woven into the various layers of the best practices architecture to help understand contextually the role that an individual or organization is performing when he or she accesses patient data. IAM encompasses authentication, authorization, access control, and role management, among other functions. Authentication consists of establishing confidence in the claims made by the user or the organization attempting to access the cloud. This is followed by authorization that maps particular users or organizations to privileges or roles, and access control, a step that ensures that the user or organization has the right entitlements to access the resources that are sought. Role management is responsible for assigning levels of access to the ePHI and ensuring that access is on a “need to know” or “right to know” basis. In other words, not only is it important to verify “who” an entity is, but, equally important, the context in which this entity is attempting to access data. Patients have the right to see their own medical information for treatment recommendations, diagnoses, prescriptions, and billing. A doctor also has the right to see the same information for a patient they are treating. However, a doctor who usually practices healthcare in New York should not be accessing patient data from an unknown location in another country. Similarly, an insurance provider might need to know that a patient received certain diagnostic services, but does not need to know that the patient increased his or her weight by 10 pounds since the last visit. Additionally, IAM tools need to be able to track information access so that it is possible to provide auditing and oversight on how the information is being used within the system. Without this contextual sensitivity, the data will be exposed to increased levels of risks that commonly plague e-business organizations today.
Network Resilience & Service Level Agreements

A resilient network is necessary in order to handle the incredible demand for ubiquitous access to information that has been centralized in the ICEHR. The network is more than just a bundle of wires providing a pathway for 1’s and 0’s. It needs to be designed as a context sensitive railway capable of switching trains off of the network if they are not compliant with the policies and standards of the ICEHR. Although it can leverage existing technologies like secure sockets layer (SSL), the Internet, clouds, and private lines, a resilient network needs to separate the ICEHR’s information flow from general data flows. It also needs to support appropriate levels of availability and fault tolerance for the ePHI that is leveraged for life or death scenarios. The rapidity of cloud recovery following downtime, and appropriate levels of redundancy are important for maintaining normal operations on the cloud, and the issue of availability is relevant at all cloud levels. It is essential that patient information is not lost and as such, this best practice needs to address how resources are properly replicated in alternate facilities for continued operations or failover. The ICEHR will also need to establish an SLA between the various entities that ensures the confidentiality, integrity, and availability of private patient data, commonly referred to as the CIA triad (Dhillon, 2007; Stallings, 2011).

Advanced Computational Power

This layer is responsible for processing patient information. Although the architecture does not specify the details of the processing platform or the components, it is the expectation that this layer is implemented in a fashion that handles the current demand requirements and has the flexibility to grow with additional future demand. Since the availability requirements are high for the data that is supported by this layer, actual implementation will need to ensure that this computational layer possesses infrastructure survivability and resilience to address failures.

Data Mining of HIT “Big Data”

Using HIT produces an enormous amounts of data that can be divided into the following four main categories (McKinsey Global Institute, 2011, p. 42): (1) clinical data, (2) insurance claims and cost data, (3) pharmaceutical and medical research and development (R&D) data, and (4) patient behavior and sentiment data. It has been estimated that “Big Data” related to healthcare stood roughly at 150 Exabytes in 2011, and is expected to increase at a rate of 1.2 to 2.4 Exabytes per year. Overall, there exists roughly 235 Terabytes of health data stored in the Library of Congress. Extrapolating these numbers worldwide gives roughly 630,000 times the amount of data stored in the Library of Congress. ARRA calling for a common standard for healthcare data is an effective first step to mine “Big Data” used or generated by the proposed ICEHR. There are several methods that “Big Data” can be leveraged and used to improve healthcare delivery. In particular, CDSS units can be designed to enable physicians in diagnosing and treating patients in a safer and more cost effective manner. Also, having access to a vast repository of treatment outcomes enables the physician to use a more empirical approach when treating patients. CDSS units can also help deliver personalized care to patients based on their genetics and other personal characteristics.

Other Operational/Managerial Controls

The Federal government needs to have operational responsibility and oversight over the ICEHR, in order to ensure that it delivers on its mission for the healthcare community. The Operational/Managerial layer focuses on providing the necessary administrative and monitoring tools and controls for the government to properly support the ICEHR infrastructure.
CONCLUSION, CONTRIBUTIONS, AND FUTURE RESEARCH

This paper has explored the tremendous potential that cloud computing offers healthcare organizations to help them jump on the EHR bandwagon. The proposed ICEHR’s functionality is expected to assist healthcare professionals in their diagnoses and patient treatments by suggesting medications based on a set of symptoms and patient characteristics. The ICEHR’s design is an easily expandable concept and can be extended much beyond a single healthcare provider. It can be built on top of existing cloud infrastructures, such as AWS, and can ensure better quality healthcare through reduced medical errors and readily access to real-time patient health information. It also offers cost savings and higher operational efficiency to healthcare organizations.

To address privacy and security issues that cloud computing generates, we proposed a comprehensive set of architectural best practices that encompass end-user policies and regulations, identity and access management, network resilience and SLAs, advanced computational power, “Big Data” mining abilities, and other operational/management controls. These best practices help solve a number of issues that arise from the NHIN, NHII, and private information exchanges. The ICEHR best practices framework is transformative in that it acts as the authoritative record on patient health data and ensures that ultimately the patient receives the best care. While NHIN may be the current step in the Federal government’s participation in healthcare, the ICEHR best practices framework marks the beginning of better healthcare prospects. The identified best practices also define lucrative areas of HIT research that will gain from further elucidating in the future.

The scope of the best practices framework idea easily extends beyond the content of this paper with additional developments in each of the architectural layers. Once the overall architecture is established, an initial plan would be necessary to help provide adequate

scope around the level of budget and effort necessary to design and deliver this as a first revision solution. In addition, effort would need to begin with law makers in order to obtain an executive sponsor who could help drive the legislative process necessary to instantiate this system. NHII already proposes the instantiation of a position within HHS. The expectations of that role could be expanded to include the best practices framework of the proposed ICEHR.

REFERENCES


Lara Khansa is an Assistant Professor in the Business Information Technology Department at Virginia Tech. She received her PhD in Information Systems, MS in Computer Engineering, and MBA in Finance and Investment Banking from the University of Wisconsin, Madison. Dr. Khansa has published in leading journals including Decision Sciences, Decision Support Systems, Computers & Operations Research, European Journal of Operational Research, Communications of the ACM, International Journal of Electronic Commerce, Computers and Security, and IEEE Technology and Society, among others. She is a member of the Association for Information Systems (AIS), IEEE, and the Beta Gamma Sigma National Honor Society.

Jonathan Forcade received his MBA with concentration in IT from Virginia Tech, Graduate Certificate in Information Security Management from the University of Virginia SCPS, and BS in Computer Science from Western Michigan University. Mr. Forcade has extensive experience in making design recommendations for secure mission critical computing architectures across various industries, including utility and healthcare. He has been cited in several articles relating to topics in Information Security and outsourced IT services and is a Certified Information Systems Security Professional.

Girivaraprasad Nambari is a senior software developer and architect. He holds a BS in Computer Sciences from JNTU, India and is currently pursuing a Masters in Information Technology degree at Virginia Tech. Giri has 10 years of experience in product development in various business domains. His interests are in integrating technology with business to simplify business processes and increase business success. Giri also contributes to different open source projects.

Saravanan Parasuraman is a lead systems administrator. He earned a diploma in Electrical and Electronics Engineering, a BS and MS in Business Administration, and is currently working towards a Masters in Information Technology degree at Virginia Tech. Saran has over 15 years of experience as a Unix Systems Administrator and is an expert in IBM AIX, Oracle Solaris, Redhat Linux, Tru64, and HP-UX. Prior to his current position, he worked for IBM, HP and CSC in various capacities.

Patrick Cox is a Sun-certified Java programmer and Web component developer. He has twelve years of experience working in Information Technology in various industries such as banking, wholesale distribution, state government, and energy. Patrick completed his undergraduate degrees in Management Information Systems and Business Administration in 2000 from Winona State University in Winona, Minnesota, and is currently pursuing a Masters in Information Technology at Virginia Tech. Patrick has worked in data processing, quality assurance, and as an IT consultant.