Bridging the Gap for Patient Data Access and Integration

Naveen Gidwani, Ash Goel, Lacy Knight, Daniel Theleen, John Wong

ABSTRACT

"Like PC vs. Mac, but riskier" (Boston Globe, 2011), is the central theme behind the editorial to describe the lack of interoperability for a seamless integration that allows patients to access their medical records stored in a multitude of health care entities. The establishment of a cloud-based central repository data exchange system that serves both as an information switchboard and data consolidator among various health care entities will enable both the patients and their health care providers to better manage patients’ health.

With the Health Information Technology for Economic and Clinical Health (HITECH) provisions of the The American Recovery and Reinvestment Act of 2009, abbreviated ARRA 2009, (www.hhs.gov/recovery, accessed 2/23/2011), the push to integrate diverse Electronic Health Records (EHRs) has created a huge incentive for various stakeholders to explore different options for interoperability of these systems. A major objective of the HITECH Act required the government to develop standards by 2010 that allow for the nationwide electronic exchange and use of health information. The Office of the National Coordinator (ONC- www.healthit.hhs.gov, last accessed 2/25/2011) has championed the nationwide health information network (NHIN) as a set of standards, services and policies that enable secure health information exchange over the Internet. The network will provide a foundation for the exchange of health information across diverse entities, helping to achieve the goals of the HITECH Act. This critical part of the national health IT agenda will enable health information to follow the consumer, be available for clinical decision making, and support appropriate use of healthcare information beyond direct patient care so as to improve population health.

In this paper, we will explore how we can achieve this vision. Specifically, we will propose a system of a unified web-based Electronic Health Record that is accessed and updated by authorized providers and recipients of care and used as a communication portal between these stakeholders in a cloud-computing based platform. We expect that this method of storage and retrieval will help consolidate all health-related records of a patient’s care. In this model, patients will be provided with a unique smart card that identifies them to the system and grants access. Each practice will use its own practice management software that links to a web-based portal. An independent third party or multiple business entities (with databases connected together via secure internet gateways) can provide access through this secure portal to the cloud-computing platform database for a fee. The web portal will link to a database where patient data is stored. It will also enable a connected messaging system that allows for messaging across providers and between patients and providers.

ESTABLISHMENTS OF STANDARDS AND INTEROPERABILITY

As we mentioned in the introduction, interoperability poses a considerable obstacle for the integration of various systems. Few primary care physicians (PCPs) have EHRs, but many more are in the process of adopting this technology. As physicians adopt different EHR systems,
patient data typically becomes scattered over five or more sites: as a result, inefficiencies occur. Inconsistencies in what is recorded and how it is recorded create silos of data that cannot be merged for analysis or patient care. The HITECH Act encourages solutions to overcome these burdens and create a connected health system where data can flow seamlessly through the health care delivery system. Actualizing this goal requires attention to the concept of interoperability.

**INTEROPERABILITY** Interoperability means the “ability of health information systems to work together within and across organizational boundaries in order to advance the effective delivery of healthcare for individuals and communities” as defined by the Healthcare Information and Management Systems Society’s (HIMSS) Integration and Interoperability Steering Committee (I&I). HIMSS created I&I in September 2004 to provide oversight across many of its integration and interoperability-related activities (HIMSS Board of Directors Report, 06/09/05). I&I chose to refine the definition to tie interoperability to the context of the NHIN.

There are several dimensions of interoperability that all need to come together to create a seamless exchange of data: (a) uniform movement of healthcare data such that movement of data across systems does not alter the purpose and meaning of the data; (b) uniform presentation of data, enabling users of different underlying systems to have consistent presentation of data; (c) uniform user controls, to ensure that when the user is accessing a variety of underlying systems, and the contextual information and navigational controls are presented consistently and provide for similar actions in all relevant systems; (d) uniform safeguarding of data security and integrity as data moves from system to system and limiting access and edit abilities to authorized users only; (e) uniform protection of patient confidentiality even as users in different organizations access data that has been exchanged across systems; and (f) uniform assurance of a common degree of system service quality (e.g., reliability, performance, and dependability) that allows for each transaction to be processed effectively and accurately. An absolute necessity for achieving interoperability is the existence of standards, agreed upon ways in which these data will be presented, stored, and conveyed (Hammond, Bailey, Boucher, Spohr, & Whitaker, 2010).

**STANDARD DEVELOPMENT ORGANIZATIONS (SDOs)** Standard Development Organizations (SDOs) were formed to address the exchange of clinical data among multiple Health IT systems. Presently, there are multiple SDOs: International Standards Organization (ISO), Technical Committee 215, Health Level Seven (HL7), Committee European de Normalisation, Digital Imaging and Communications in Medicine (DICOM), GSI, Clinical Data Interchange Standards Consortium (CDISC), and International Health Terminology Standards Developing Organization (IHTSDO) (Hammond, 2005). Table 1 is an analysis of several SDOs and their specific interests.

**Table 1: U.S. Standards-Development Organizations (SDOs)**

<table>
<thead>
<tr>
<th>Organization</th>
<th>Interests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accredited Standards Committee X12 (ACS X12)</td>
<td>Claims and reimbursement process (transactions)</td>
</tr>
<tr>
<td>American Dental Association (ADA)</td>
<td>Various dental standards</td>
</tr>
<tr>
<td>ASTM International (E31 for health data standards)</td>
<td>Clinical data standards; security and privacy</td>
</tr>
<tr>
<td>Digital Imaging and Communications in Medicine</td>
<td>Images, waveforms</td>
</tr>
</tbody>
</table>
### Health Level Seven (HL7)
- Reference information model, data types, clinical data architecture, clinical templates, data elements, terminology, V2 messages, V3 messages, CCOW, decision support

### IEEE 1073
- Medical devices

### Integrating the Healthcare Enterprise (IHE)
- Defines use of multiple standards at an enterprise or multi-enterprise level; not quite an SDO, organized by the Radiological Society of North America and Healthcare Information and Management Systems Society (HIMSS)

### Medbiquitious
- Distance learning, patient simulation

### National Council for Prescription Drug Programs (NCPDP)
- Third-party drug claims, prescription messaging

Source: Author's analysis. (Hammond, The Making And Adoption of Health Data Standards, 2005)

While many SDOs exist, none have achieved widespread adoption. This challenge, in many cases, is a matter of awareness of the existence of applicable standards. In other cases, the role of standards is unclear. Furthermore, overlapping and competing standards still exist (Hammond, 2005). Competition occurs because vendors stand to lose revenue if buyers are no longer forced to rely on custom integration and development processes. Establishing a standard requires significant cost, validation through successful implementation, and perseverance. In general, acceptance of a specific standard occurs gradually.

Aside from working to attain predominance of their standard, SDOs struggle to devise the standards themselves. The breadth and complexity of health information pose challenges in gaining consensus. Although the challenges are significant, the success of achieving interoperability would be remarkable, and perhaps life-saving. Clinicians would have the information they need at the point of care, consumers would have choice and portability, payers would save money, and researchers would have better data (Brailer, 2005). Without establishing interoperability standards, a nationwide health information network is impossible.

**Interoperability Standards** Interoperability standards in healthcare information technology are gradually becoming more robust as the myriad of healthcare IT SDOs scurry to put forward “the last word” on the subject, but with limited success. The only real results so far are the acronyms — HL7, HIE, CCR, CCHIT, RHIO, among many, many others — that point toward the goal, but don’t quite get there (Grace, 2008). W. Ed Hammond, PhD, Director of Duke (University) Center for Health Informatics, proposes the following be considered in any effort to create policies for data exchanged between Health IT systems:

1. Data should have to be entered only once; they should be “reusable.” Data that can be collected automatically is preferred.
2. Stakeholders must cooperate to ensure the application of consistent rules across technical domains.
3. Sensitivity to legal, ethical, and societal requirements must be applied, including security, privacy, and confidentiality.
4. A single global set of precisely defined data elements with attributes must become the building blocks of all such systems.

5. It is critical to achieve interoperability among all of the diverse Health IT systems.

Table 2 below presents multiple examples of standards that have been developed in association with standards classes (Hammond, 2005).

Table 2: Category of Standards Required For Data-Sharing Interoperability

<table>
<thead>
<tr>
<th>Class of Standard</th>
<th>Example standards</th>
<th>SDOs creating the standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>General standards, broad use</td>
<td>XML, TCP/IP, 802.11, Web Services, security, wireless, GPS</td>
<td>W3C, IETF, IEEE, OMG, HL7</td>
</tr>
<tr>
<td>Data components</td>
<td>Reference Information Model (RIM), data elements, data types, terminology, templates, clinical statements, clinical document architecture</td>
<td>HL7, CEN, ISO, openEHR, SNOMED, LOINC, RxNorm, UMLS, others</td>
</tr>
<tr>
<td>Data Interchange</td>
<td>Structured and free-form documents, images</td>
<td>HL7, ASTM, DICOM, IEEE 1073, NCPDP, X12N, CEN, ISO</td>
</tr>
<tr>
<td>Knowledge representation</td>
<td>Guidelines and protocols, decision-support algorithms, Arden Syntax, GLIF, GEM, Prodigy, Portage, vMR, GELLO</td>
<td>HL7, ASTM, others</td>
</tr>
<tr>
<td>Electronic Health Record (EHR)</td>
<td>Functional requirements, EHR models, Continuity of Care Record (CCR), patient summary record, personal health record</td>
<td>HL7, ASTM, openEHR, CEN</td>
</tr>
<tr>
<td>Application level support</td>
<td>Identifiers, recourse registries, disease registries, tool sets, conformance requirements, implementation manuals</td>
<td>HIPAA, HL7, ASTM, ISO, CEN</td>
</tr>
</tbody>
</table>

Source: Author Analysis (Hammond, The Making And Adoption of Health Data Standards, 2005)

Considering the aforementioned axioms and standards, the challenge in defining a common language between systems is evident and few of these standards have the potential to support the framework to allow interoperability. Effective integration of clinical expertise into the process of making standards is crucial, in addition to collaboration with vendors to define the line between open standards and proprietary interests. A shared method of evolving standards promptly would permit vendors to get a return on software investments for implementing standards while taking advantage of new technologies and meeting future needs. At the moment, an effort is under way to create the Continuity of Care Record; an XML-based standard intended
to become the equivalent of a Resource Description Framework (RDF) or Open Document Format (ODF) file that lets the various EHR vendors read and write to the same file format.

For purposes of data exchange between our proposed cloud-based EHR solution and a provider’s practice EHR, our recommended data standard is the Continuity of Care Record (CCR). Of the current available standards, the CCR best manages to provide reuse and automated collection of data, support interoperability, and meet privacy, security, and legal requirements. According to the Standard Development Organization that developed the CCR format, ASTM International, the standard abstract states:

The Continuity of Care Record (CCR) is a core data set of the most relevant administrative, demographic, and clinical information facts about a patient's healthcare, covering one or more healthcare encounters. It provides a means for one healthcare practitioner, system, or setting to aggregate all of the pertinent data about a patient and forward it to another practitioner, system, or setting to support the continuity of care.

For successful exchange using CCR, the EHR solutions need to be able to export and import the complete document. The following elements of the CCR are the leading reasons we believe that this is the most appropriate data exchange standard in the presented solution:

1. **Document structure is specified** – Header, Body, and Footer.
2. **Document format is specified** – XML coding
3. **Format provides flexibility** to prepare, transmit, view, and display the CCR in multiple ways; for example, in a browser, as an element in a HL7 message, in a secure email, as a PDF file, as an HTML file, or as a word processing document.
4. **Format and structure of CCR** enable automated healthcare information transmission with minimal workflow disruption for practitioners. Equally important, it will allow the interchange of the CCR data between otherwise incompatible EHR systems.
5. **Structure of CCR** instance supports self-protection, privacy, and authentication and authorization controls.

Agreeing upon an interoperable framework doesn't address another key issue: the creation of a unique glossary of terms to describe both medical procedures done to a patient as well as to describe a diagnosis. The upcoming transition from International Statistical Classification of Diseases and Related Health Problems (ICD) version ICD-9 to ICD-10 will not make this any easier. Maintaining privacy of data is another area of concern, particularly when most states have added their own requirements to the Health Insurance Portability and Accountability Act’s (HIPAA) privacy standards (1996) (Thompson & Brailer, 2004). Thus, for the most part, a hospital in one state trying to send patient data to a hospital in another state can only do this on a one-to-one basis, typically with a phone call and proper identification. However, in a scenario where a patient has the ability to securely transfer essential medical data through the use of a smart card or a cloud-based central repository data exchange system; one can envision how this roadblock might be passed.
DETAILED PROPOSAL

USE CASE SCENARIO With the groundwork for standards and interoperability defined, we can apply it to our proposal to establish a web-based electronic health record on a cloud-computing platform. The system will assure privacy and security, provider and patient access, integrated communication, and create a unified database for patient health information. The framework for this system is as follows. Each provider has their practice electronic medical record that has the capability of importing and exporting information in the CCR format. For an annual fee, the practice EMR links through a secure portal to a cloud-based EHR database with at least 99.9% uptime (e.g. http://www.google.com/apps/intl/en/business/index.html), in contrast to the average uptime for health records networked in traditional fashion – 96% (Anderson 2011). A patient’s health information is now accessible by any authorized provider through this portal. The patient may access their own health information through the same portal using a personal identification number (PIN) and a smart card issued by their PCP when becoming a patient of the practice. The patient (or insurer) pays for the smartcard, and its signed acceptance by the patient authorizes the sharing of health information through this network and consents to e-mail communication from any established provider. The patient is capable of adding provider relationships to their profile to facilitate syncing of health data. The smart card is another means of establishing a relationship by “swiping in” to an office. Providers purchase a smartcard reader for their office. The patient must enter their PIN after swiping to transfer information from the card. Once the patient has registered with practice, the provider can use the patient’s MPI number, practice name, and password to review records through the portal. In the case of an emergency, the Emergency Department is able to override the PIN to access health data with a verified and secured reader.

When a PCP accepts a new patient into the practice, they discuss the benefits and mechanism for exchanging health information between providers. The patient is built into the practice’s Master Patient Index (MPI), the index of unique identifiers that integrates patient data from a practice’s disparate systems (billing, scheduling) via their respective identifiers. The provider explains that a smart card is used to assist in health data transfer and its purchase provides consent to share health records and communicate electronically through the portal. The patient is provided a unique PIN, and instructed how it may be used to grant access, by swiping the card through a provider’s authorized card reader or entering the web portal. After the medical evaluation by the PCP, a document is created in the practice’s EHR and a CCR is exported to the cloud EHR and also placed on the patient’s smart card by scanning. When the patient is referred to a specialist, they have the option of authorizing the practitioner in advance via web portal or by “swiping in.” The PCP may also send a secure e-mail to this consultant regarding the patient, and the patient may send a secure e-mail to the provider in anticipation of consultation. In a similar fashion to the PCP, the specialist documents in their own EHR and a CCR exports and updates the cloud database as well as the patient’s smart card. The cloud-based EHR is updated with each episode of care and pushes messages and updates to the patient’s record to all registered provider EHRs. Each day when the practice opens for business and connects to the database, messages specific for the MPI will be downloaded. This enables it to communicate with other providers in an efficient manner. We will attempt to demonstrate that, with certain assumptions, this model will resolve the limitations and problems highlighted above and explore further into the mechanisms of the various components mentioned.

WEB BASED EHR The web-based EHR is an established concept since the proliferation of Integrated Delivery Networks (IDN) across the nation in the 1990’s. For nations with an integrated health network system, such as Taiwan, it has been a long accepted practice of exchanging health data between health care entities by “using streaming media and web technologies, [whereby] the system maintains medical record integrity, resulting in improved clinical outcomes, and reduced time in administering prescriptions” (Chen W & Shih, 2010).
Within organized healthcare delivery systems, such as managed care organizations, several distinct institutions may participate in the care of the patient. “Safe, comprehensive and cost-effective patient care depends on the ability to obtain an accurate history of the patient’s health care” (Kohane et al., 1996).

We propose a web-based solution because of its wide availability for access, scalability, EMR vendor neutrality, and ability to participate in this format with limited up-front costs (e.g. new hardware, software).

Needless to say, data security and privacy is one of the main concerns of an EHR. Approaches such as the use of public and private key encryption to ensure the proper security transmission of the information over the internet (Halamka, Osterland, & Safran, 1999), systems that seek appropriate protocols or templates automatically by the file’s XML content (Hu, Jain, Chang, & Hsu, 2005), and the use of policy-compiler-like implementation scheme to provide adaptable access control for EHR such as the use of aspect-oriented programming (AOP) (Chen K, Chang, & Wang, 2010), are examples of security measures for EHR.

More specifically, a well-defined web based EHR should not only provide the ability to store a patient’s medical records, but also provide “a set of services for creating an application ecosystem that lets consumers collect, store, and share health information online” (Liao, Chen M, Rodrigues, Lai, & Vuong, 2010). The format would provide a “well organized and maintained platform (that) provides a privacy-enhanced and security-enhanced foundation that can be used to store and transfer information between a variety of e-healthcare customer’s applications, hospital applications and healthcare devices”.

**Electronic Messaging** It is apparent that the sharing of health information among providers is the cornerstone of the system. However, pure data transfer is meaningless without corresponding communication and messages among the entities. Therefore, secure and HIPAA compliant messaging between different EHRs to provide messages from one provider to another (including patient referrals, consultation and scheduling of appointments) would certainly help in providing more effective and timely care to patients (Gandhi et al., 2000). In addition, as competition between health care delivery systems increases, the need to provide superior customer service (i.e., in terms of prompt, polite, and informative communication) to referring physicians has become a priority (Montalto, 1995).

Some early work in computer-based systems was done in Boston at the Partners HealthCare System (Sittig et al., 1999). This integrated health care delivery network serving large part of eastern Massachusetts, includes the Massachusetts General and Brigham & Women’s/Faulkner Hospitals, Dana-Farber/Partners Cancer Care, Newton-Wellesley Hospital, and North Shore Medical Center. In addition, Partners is affiliated with over 900 primary care physicians in the Boston area. All together, Partners provides care for over 1,000,000 patients in the greater Boston area. Results from the use of the new "email-based" referral system were very encouraging.

The National Health Service (NHS, UK) has implemented a very large project with multiple technologies that support communication (NHS Connecting for Health Implementation Guide, 2007). The key deliverables for the project involve: a National Care Record Service that would contain all clinical data for all NHS patients; ‘Choose and Book’ for scheduling appointments, electronic transmission of prescriptions, national Information Technology (IT) broadband IT network (N3), picture archiving and communications system; central email called NHS mail; GP2GP information transfer between physicians allowing secure transfer of records, and a portal (secure) website called “Healthspace” that stores and allows access to a summary care record. The data warehouse known as the “Spine” is the set of services used by the Care Record Service. The NHS Spine is a care record repository, deposited into and accessed by
electronic health record (EHR) systems - it is not itself an EHR system. The Care Record has a
detailed record held locally and the summary record held nationally. The security model utilizes a
Role Based Access Control (RBAC) that requires the maintenance of people, roles, and system
capabilities. The adoption has been phenomenal. Over eight million appointments have been
made on 'Choose and Book'; Over 87 million prescriptions have been transmitted; Over 162,000
care records have been uploaded to the SPINE; there are 486,498 Smartcard holders who are
registered and approved for access to the Spine. Approximately 1.2 million NHS employees have
access to the N3 broadband network (NHS Connecting for Health Latest deployment statistics
and information, May 16, 2008).

SMART CARD TECHNOLOGY Smart card technology augments the security, privacy, and
confidentiality of our web-based EHR. As we mentioned in the previous section, an important tool
in the authentication of a patient’s identity is the use of a personalized health identification smart
card. A smart card, that contains the relevant information, may “avoid circumstances where
management decisions are made in a “vacuum” — that is, without relevant information at hand”

Smart card is a plastic card containing a microchip that has a memory capacity superior
to magnetic stripes and that can be updated readily. The card can be equipped with a personal
identification number (PIN), can require an authorized card reader system and can be configured
to reveal certain information depending on the person seeking access (Ward, 2003).

Traditionally, the medical history, drug information, allergy, and other relevant
information are being kept in the local doctor’s or clinic’s office. The information became a
valuable tool to the local doctor, as they are vital clues for the diagnosis of a disease. However,
when a patient is away from his local doctor’s office, the information may not be available for
other health professionals. This is especially true in emergency departments that may be distant
and have no connection with the local doctor’s office. The use of smart card technology would
allow proper authentication and access of a patient’s health record from anywhere.

Technology has come to a point whereby we can contain sophisticated programs in the
card, such as the inclusion a smart magnetic strip technology (Bernard, 2010), in which the
magnetic strip is decrypted, only when the user enters the correct PIN or password onto the card.
This feature will ensure that if the card was lost, the information inside the card could not be
read or accessed by other people.

The use of smart cards can have tremendous potential. When a patient first checks in to
the emergency room, the nurse can immediately insert the smart card into the official smart card
reader. As the list of procedures, tests, results, and medications are added; the information can
be immediately be exported to our cloud-based HER and entered onto the smart card as backup.

ENHANCED HER ON CLOUD-COMPUTING PLATFORM While a web based EHR can expand the
availability of medical information, it is still limited by other factors such as display of data
obtained from different institutions, selection of patients in the absence of a national
identification system, vocabulary translation, and authorization of access to records outside an
institution (Kohane et al., 1996). Therefore, we can add, on top of a web based EHR system, an
integrated cloud-based solution that can help minimize the need to transfer information from one
system to another.

Cloud computing is the concept in which, “the computational part (hardware and
software) is at a central facility, now called “cloud” which does the data processing and provides
the most advanced computational service, at any time, to an unlimited number of users,
connected through telecommunication to the central processing facility” (Meir & Rubinsky, 2009).
In a typical cloud scenario, the cloud vendor would control the operation and maintenance of the essential hardware and storage. User would access the information by a local terminal, which is responsible for the acquisition of raw materials and data from local facilities, the transmission of the information to the central cloud unit, and the receiving of the processed information from the central cloud repository.

A “cloud” could be “built to provide a way to input, store, and access information without the need to build complex infrastructures to support outside medical record numbers or patient identifiers, dictionaries and user accounts, different databases and archive protocols, and so on” (Andriole & Khorasani, 2010).

Other qualitative benefits include less resource to manage, superior resiliency, homogeneity, fewer issues to negotiate with institutional authorities, archiving, archiving, backup, and fault tolerance, sharing data and tools across a consortium, and high performance computing (Rosenthal et al., 2010).

Since the main concern of any EHR is to ensure the security and privacy of patient’s data, the utilization of a cloud computing system would improve data security by focusing the security safe guards into one central location. Administrator would no longer have to worry about data being stored in each individual’s local computer. Administrator would be focusing on other aspects, such as the transmission of data and the presentation of images across the Internet.

Specifically, in terms of data transmission, one can build on top of the encryption key technology as described in the EHR section. Other technologies, including transport layer security encryption technology, would allow HIPAA-covered data to be transmitted securely through the Internet (Philbin, 2010). In terms of transmission of medical images, techniques such as remote rendering or server-side rendering, can allow images to be rendered on a server in a data center that then streams only the bits necessary to represent the current 2D image on the user’s display using techniques similar to those that allow a Netflix movie streaming (Philbin, 2010).

LIMITATIONS AND CHALLENGES OF CLOUD COMPUTING

Even though cloud computing provides a great promising potential for the accessibility and availability of a patient’s medical information, anywhere, anytime, and anyhow, there are issues and limitations that must be considered. In particular, data latency, data ownership, cost effectiveness, data security issues all must be taken into account (Philbin et al., 2010). Furthermore, interoperability, open standards, and open-source issues (Androile & Khorasani, 2010) would limit the utilization of cloud computing.

First, as we alluded to earlier, latency and connectivity issues would hamper the retrieval of time critical information, especially in a stressful environment such as the emergency department. The Gmail outage that occurred in late February 2011 caused major productivity problems for some companies who have migrated to use Google mail. A similar outage affecting critical medical data would make a significant impact if unavailable for life saving operations.

Second, in terms of data privacy and confidentiality, individuals are at the mercy of the cloud provider, to ensure that the systems and data transmissions are secure. It is possible that the cloud provider is hosting several virtual cloud environments on a single physical server. Therefore, the cloud provider must ensure additional data contamination safeguards, especially during times of data replication and backups. In addition, as the cloud is essentially serving as a data consolidator across multiple content entities, not only must the cloud provider ensure security in its central repository, but that it must also ensure that both the content providers, and the data recipients, would adhere to comparable privacy and confidentiality standards.
Third, since multiple content providers are contributing to the content of the cloud repository, the issue of data ownership could cause a problem: for example, a certain entity may refuse to collaborate or share its information. Furthermore, if and when one party decided to terminate its relationship with the cloud provider, it may want to ensure that all data to be removed from the cloud repository (Rosenthal et al, 2010). However, it is debatable whether the data residing in the cloud, belongs to the content entity, the cloud provider, or the particular patient.

Fourth, as more and more information are being stored in the cloud environment, we may reach a point whereby, too much information are contained in one location.

Lastly, as echoed in the recent Mobile World Congress, the lack of standards (or more precisely, the myriad of competing standards) would mean that interoperability among different content entities and cloud providers would remain an issue (Hill, 2011). Furthermore, the question of who should pay for the implementation and maintenance of such a comprehensive infrastructure would create additional challenge and limitation to the use of cloud computing (e.g. should patients pay extra for the convenience of having their medical records being accessed anywhere?)

Despite of some of the drawbacks and considerations, there seems to be tremendous potential for cloud computing. In a sense, the several dimensions of interoperability mentioned in the introduction can be resolved by the introduction of a patient identification smart card with authentication entry to a web based EHR system on top of a cloud based computing infrastructure.

Clearly such a system would go a long way in providing for some of the answers to the problems traditionally faced in communication between isolated EHRs. However this cannot be replicated as easily in the United States’ private sector market. Physicians are contracted to the NHS so adoption can be required. The United States has struggled with ways to increase and require adoption by physicians, hospitals, and payers. The President has set a mandate for most Americans to have electronic health records by 2015. However, many agree that the deadline is arbitrary and will not be met (HIMSS HIE Technology Guide White Paper, 2009).

**EXAMPLE OF A WEB BASED EHR ON CLOUD BASED COMPUTING ENVIRONMENT**

To provide a more detail description of the concept and technology behind cloud computing, we can borrow a real life example by one of the said authors of this document, who is managing the implementation of such an application that access a patient’s EHR on a cloud based platform. An example of the basic architecture and process flow behind the technology can be found in Table 3. An example of the underlying schema diagram can be found in Figure 1.

<table>
<thead>
<tr>
<th>Table 3: Basic Architecture and Process Flow Behind Cloud Computing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Client application displays <em>Sign In</em> page to user on remote desktop, tablets, or terminal</td>
</tr>
<tr>
<td>2. User uses smart card to provide authentication</td>
</tr>
<tr>
<td>3. Client application sends HTTPS request to middleware with the authentication</td>
</tr>
<tr>
<td>4. Servlet receives the information and authenticate it against the records in cloud data store</td>
</tr>
<tr>
<td>5. If authorized, servlet sends HTTPS response back with successful message</td>
</tr>
<tr>
<td>6. Client application receives the successful HTTPS response, and sends another HTTPS request for the retrieval of the electronic medical records (EMR) pertaining to the user</td>
</tr>
</tbody>
</table>
7. Servlet sends a HTTPS request to the central repository web service for the EMR of the patient
8. Central repository authenticates the HTTPS request against secure data connector through a designated port number
9. If authenticated, the HTTPS is allowed to go through the firewall and hit the requested web service
10. Web service issues appropriate SQL commands to the data repository, to get the EMR of the patient
11. Web Service sends back HTTPS response with requested data in XML format
12. Servlet receives the HTTPS request with XML data
13. Servlet sends the HTTPS response back to the client application with the XML data
14. Client application decrypt and parses the XML data and display the information on the client remote desktop, tablets, or terminal

**CONCLUSION**

Based on the analysis of multiple technologies and current state of interoperability standards deployment, several common themes emerge. At a minimum, the future state of national medical information sharing systems needs to be:
• Based on a detailed set of agreed upon standards
• Web based to help ease of access, redundancy, and manage costs (esp. of integration, exchange interfaces).
• Able to support a robust security, privacy and audit methodology.
• Real time data exchange and update enabled technology with scalability to needs of each entity.
• Achieve a uniform data presentation and manipulation interface.

Several international models of similar nature have been deployed with varying degrees of success (HIMSS HIE Technology Guide White Paper, 2009). There were limitations with each in terms of available technology, resources, and uniformity of applications as detailed in this paper. The applicability of these models to the US healthcare environment is also limited by lack of a clear source of funding (as it is left to individual vendors to develop sets of competing and loosely interactive technologies) and minimal impetus for mandated implementation and governance to ensure uniformity of such products.

The proposed model of a central data repository with a strong standards based information exchange methodology which is secured by ‘smart cards” for user access addresses these concerns to a certain extent. The model has some unique features that are highlighted here. The “cloud model” provides for scalability and subscription based service allows for managing local costs for a practice. Such data storage also creates uniformity of data storage and instant access with real time data upload and download. Integration of data into one structure removes redundancy except as required for data back up and availability. User access control based on “smart cards” with secure messaging and sharing of information with continuous audit capabilities in a HIPAA compliant system is a strong attribute of this proposal. This model also allows for different application interfaces (each entity’s EHR) to be customized to individual preferences thus managing to provide a good balance between uniformity of data availability and content; and flexibility of data presentation tailored to individual’s needs. Ability to store data on smart cards provides an added layer of redundant data storage for use when needed.

The limitations of this model are primarily related to the inability to enforce a uniform standard of interoperability as was highlighted above. Application of such technology is also restricted by the adoption by both patients and providers. Building a business case for such technology is based on the assumption that every entity or provider of health care services adopts this as the modality of choice for storage, exchange and securing medical data. The full benefits of such a system can only be realized then. The total cost of ownership over a period of time will certainly turn out to be cheaper as is highlighted by a study in Auckland, NZ (HIMSS proceedings 4/8/2003). The technology solution incorporated a server supporting multiple clinical programs with a thin client, web enabled interface, HL7 messaging and a total security and privacy solution. The financial results were very impressive - $9m NPV, 164% internal rate of return, $3.88 return for each NZ dollar spent and self-funding status after year one.

The future application of our suggested model may also need to address the political issues around having a central data repository with all health information for the nation along with perception of control. The ability (or inability) to restrict some part of personal health information e.g. with certain insurance payers will have to be addressed. The benefits of cost savings, provision of better care and better outcomes however may far outweigh the social concerns enough to get past these barriers.
REFERENCES


(06/09/05). *HIMMS Interoperability Definition and Background*. Approved by HIMSS Board of Directors.


