Security Issues in E-Healthcare

Flora S. Tsai*

School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798, Singapore

Received 1 Feb 2010; Accepted 18 Jun 2010

Abstract

Electronic healthcare, or e-healthcare, for paperless management of all activities within large healthcare establishments, promises much in speeding up the typical bureaucracy of healthcare in medical centers and hospitals. However, the realities that face the proper implementation of e-healthcare involve many security issues. For widespread adoption of e-healthcare by hospitals, it is essential to perform a detailed evaluation of security issues, to set the stage for standardization of various components for the proper implementation of e-healthcare. A typical e-healthcare system can consist of many components and subsystems, such as appointments and scheduling; admission, discharge, and transfer; prescription order entry; dietary planning; routine clinical notes; lab and radiology orders; picture archiving, and smart card sign-on. Each of these subsystems is vulnerable to security threats. This study examines the security issues for the implementation of e-healthcare using currently available healthcare standards, and proposes solutions and recommendations to secure the future of e-healthcare.

Keywords: E-healthcare, Electronic healthcare, Electronic medical record, Electronic health record, Security, Privacy

1. Introduction

With the development of Internet and information technology, lots of information sources are now available, such as blogs [1], social networks [2], mobile content [3], medical records, etc. The proliferation of wireless and mobile devices such as personal digital assistants and mobile phones has created a large demand for mobile information [4] as well as novel content that is personalized for the user [5]. The web is also changing its form from a data-centric web into web of semantic data and services [6]. The electronic patient record (EPR) system aims to make all of a patient’s medical reports, lab results, and images electronically available to clinicians, instantaneously, wherever they are. The EPR is the key in development of a truly digital hospital, where everyday operations and record-keeping are carried out and maintained almost exclusively with computers. Although EPRs have been healthcare priority for years in many countries, progress in implementing EPRs has lagged behind the latest information technologies available, and only a minority of hospitals and clinics actually use them [7].

Whereas EPR deals with patient records within a single healthcare organization, the electronic health record (EHR) is broader in that it refers to health records across multiple healthcare establishments (HCE) [8]. The EHR is a longitudinal collection of electronic healthcare information about individual patients as well as populations. EHR will be the primary mechanism for integrating healthcare information currently collected in both paper and electronic medical records (EMR) for the purpose of improving quality of care [9].

There are many issues that impede the widespread implementation of EHRs. Data sharing among autonomous departments that are slow to integrate with hospital-wide information systems is one barrier. In addition, issues of security, privacy, and confidentiality are examples of other hurdles to cross [10,11].

A typical EHR system (EHRS) consists of several subsystems, such as appointments and scheduling; admission, discharge, and transfer (ADT); prescription order entry; dietary planning; routine clinical notes; lab and radiology orders; picture archiving, and smart card sign-on. In this article, we examine the security and privacy issues in e-healthcare and propose possible solutions.

1.1 EHR architecture

The framework for the EHR architecture is based on the generic component model developed in the mid-nineties, which form the Reference Information Model (RIM) and agreed vocabularies enabling interoperability [12]. The EHR architecture supports electronic communication between all parties involved, documents any diagnostic measures in a standardized structure, and facilitates an unambiguous presentation of medical concepts, preserving the original context and enabling new ones [8]. For managing an EHRS, the architecture, along with its structure and behavior, must be designed appropriately.

There are basically two approaches in designing an EHRS. One approach focuses on the management of one
comprehensive model of all the structures, functions, and terminology known at development time. One example is the Comité Européen de Normalisation (CEN) “Electronic Healthcare Record Communication” standard. The other approach provides one generic and many specialized models reflecting organizational, functional, operational, contextual, and policy requirements [8]. Examples include the openEHR and Health Level Seven’s (HL7) Version 3 model.

1.2 CEN ENV 13606 architecture

Since 1990, CEN, the European standards body, has regarded the Electronic Healthcare Record (EHCR) as one of the most important areas for the establishment of European standards. It has so far published two generations of EHR standard, in 1995 and 1999.

ENV 12265 Electronic Healthcare Record Architecture (1995) was a foundation standard defining the basic principles upon which electronic healthcare records should be based. A four-part successor standard for Electronic Healthcare Record Communication, ENV 13606, was published in 1999 [13].

Part 1, the Extended Architecture, was built on ENV 12265 and defined the Reference Architecture for communicating part or whole of an EHCR to allow the content of the health record to be constructed, used, shared and maintained. The subject of the record to be communicated is an individual person, and the communication is solely with respect to that person’s care.

Part 2, the Domain Termlist, defined a set of data objects that represent the rules for defining access privileges to partial or whole EHCRs, and the means by which security policies and attributes can be defined and implemented [13].

Part 3, the Distribution Rules, specified a set of data objects that describe selected, gross observations. The OBX segment is a standard, in 1995 and 1999.

Part 4 defined a set of messages to enable the communication of partial or whole EHCRs in response to a request message or a need to update a mirror repository of the EHCR to allow the content of the health record to be constructed, used, shared and maintained. The subject of the record to be communicated is an individual person, and the communication is solely with respect to that person’s care.

Part 2, the Domain Termlist, defined a set of data objects that represent the rules for defining access privileges to partial or whole EHCRs, and the means by which security policies and attributes can be defined and implemented [13].

Part 3, the Distribution Rules, specified a set of data objects that describe selected, gross observations. The OBX segment is a standard, in 1995 and 1999.

Part 4 defined a set of messages to enable the communication of partial or whole EHCRs in response to a request message or a need to update a mirror repository of a patient’s EHCR [13].

1.3 openEHR architecture

openEHR undertakes the collation of requirements for the design, implementation and deployment of interoperable EHRs to support the seamless sharing and continuity of healthcare and to enable EHR systems to interface with medical knowledge, evidence of best practice and other systems needed to deliver safe, secure and effective health services.

The openEHR Specification Project is a key project in the openEHR “technical space”. The project consists of requirements, architectural specifications, implementation technology specifications (ITTs), and conformance specifications. ITS is a specification that describes a method of encoding HL7 artifacts. The ITS specifies how abstract models should be transformed into on-the-wire objects that can be transmitted.

The architecture specifications consist of the Reference Model (RM), the Service Model (SM) and Archetype Model (AM). The first two correspond to the ISO RM/ODP information and computational viewpoints, respectively. All of the architecture specifications published by openEHR are defined as a set of abstract models, using the UML notation and formal textual class specifications. These models remain the primary references for all semantics, regardless of what is done in any implementation domain. The openEHR Modeling Guide describes the semantics of the models. The presentation style of these abstract specifications is deliberately intended to be clear, and semantically close to the ideas being communicated. Conversely, the abstract specifications do not follow idioms or limitations of particular programming languages, schema languages or other formalisms. All such expressions are treated as ITSs, for which explicit mappings generally have to be developed and described. There are numerous implementation technologies, ranging from programming languages, formalisms such as Extensible Markup Language (XML), to database and distributed object interfaces. Each of these has its own limits and strengths. The approach to implementing any of the openEHR abstract models in a given implementation technology is to firstly define an “implementation technology specification” (ITS) for the particular technology, then to use it to formally map the abstract models into expressions in that technology [14].

1.4 HL7 architecture

“Level Seven” refers to the highest level of the International Organization for Standardization (ISO) communications model for Open Systems Interconnection (OSI) – the application level. The application level addresses definition of the data to be exchanged, the timing of the interchange, and the communication of certain errors to the application. The seventh level supports such functions as security checks, participant identification, availability checks, exchange mechanism negotiations and, most importantly, data exchange structuring [15].

The RIM is the cornerstone of the HL7 Version 3 development process. An object model created as part of the Version 3 methodology, the RIM is a large pictorial representation of the clinical data (domains) and identifies the life cycle of events that a message or groups of related messages will carry. It is a shared model between all the domains and as such is the model from which all domains create their messages.

Explicitly representing the connections that exist between the information carried in the fields of HL7 messages, the RIM is essential to increasing precision and reducing implementation costs [15]. The RIM consists of templates, vocabulary, and XML standards as summarized in the next section.

HL7 templates are data structures based on the HL7 RIM which express the data content needed in a specific clinical or administrative context. They are prescribed patterns by which multiple observation result (OBX) segments may be combined to describe selected, gross observations. The OBX segment is primarily used to carry key clinical observation/results reporting information within report messages, which must be transmitted back to the requesting system. Some observations may be quite simple, such as the blood pressure concept in healthcare, which involves a set of expected observations (i.e., systolic, diastolic, patient position, method, etc.) Other more elaborate diagnostic
procedures may involve hundreds of related pieces of information, including anatomy, orientation, sequences of measurements, etc. Templates provide a means of coupling the multiple OBX segments needed to send the observation with separately encapsulated rules for combining/validating them for the particular observation. Based on user need and preference, the template offers the user the advantage of defining the collection of OBX segments needed and the corresponding set of validation rules once, and once, defined, the structure can be used again and again. Since they are based on a specific user’s needs/requirements, templates can be “plug and play” at a given user site [15].

1.5 Eclipse open healthcare framework (OHF)

The Eclipse OHF is a project under Eclipse aimed at improving the need to improve the levels of interoperability between applications and systems within and across healthcare organizations. This project implements extensible frameworks, tools and key health informatics standards wrapped as plug-ins. While the Eclipse platform is designed to serve as an open tools platform, it is architected so that its components can be used to build just about any client application. The minimal set of plug-ins needed to build a rich client application is collectively known as the Rich Client Platform (RCP). The Eclipse RCP application with user interface and workflow logic can be created using the OHF components. The National Health Information Infrastructure (NHII) was connected to the interoperability stack of the repository database. They can be accessed by the OHF plug-ins using two different types of protocols, namely, cross-enterprise document sharing (XDS) and patient identifier cross-referencing.

However, this way of implementation would eventually pose certain problems. Developers could already foresee some of the problems that would arise due to this method of implementation. But perhaps the most major problem arose due to the need to interconnect. With advancements in information technology such as the internet and other mobile communication devices, as soon as the application targets more than one user, the market demands a client/server solution. Implementing applications using the traditional method of Eclipse RCP applications with the plug-ins based on the client side would cause enormous problems in future as applications go client/server. The need to adopt a better framework right from the start was of utmost importance. If this was not carried out, huge amounts of time, money and effort would be invested in projects and applications which, at the end of the day, would be abandoned.

With that enormous issue in mind, a team of software developers from IBM set out to resolve this issue. They eventually developed a solution they call the OHF Bridge. The OHF Bridge is a sub project of the OHF. OHF Bridge uses Server-side Eclipse and Axis to expose the functionalities of OHF components via web services. The OHF bridge is an “Open Services Gateway initiative (OSGi) on Server” runtime that embeds OHF Plug-ins and exposes a subset of their functionalities as web services. Thus any application which uses Simple Object Access Protocol (SOAP) can invoke the functions made available via web services by the OHF Bridge.

2. Methods

2.1 EHRS security

The significance of EHRS to the society is paramount as it utilizes technology to provide added convenience to our daily lives. In the past, a patient would have to wait as doctors and nurses retrieved their paper medical records. Now, doctors have instant access to our medical records with just a click of the mouse. However, the challenge of implementing EHRS is protecting the patient’s privacy and the confidentiality of the medical records. The consequences are great if the medical record is leaked to outsiders. The record might be used against the patient when looking for employment or securing an insurance deal, or leaked to the public, through newsgroups, for example. Hence, information security is vital in protecting the records. All security systems are built on three bases: managerial policies, technology and legal and ethical issues. This article will look into how those three bases are implemented to protect our digitalized health records.

Since the start of the global widespread usage of EHRS, there have been increasing concerns regarding security issues of protecting EHRS. Several government bodies, non-government organizations, public hospitals and private clinics have joined forces to implement numerous security measures ranging from regulatory control to security process and technologies.

2.2 Implementation of EHR

The security management in the implementation of EHR exists through regulations from governing bodies around the world. To implement the use of EHR in a country, appropriate security measures have to be designed by the relevant organizations. In order to ensure that the relevant organizations will undertake the necessary security procedures, government and regulatory bodies must play a part.

Since the introduction of EHR, health ministries of different countries have set up separate entities to govern the security aspects of EHR through the implementation of various acts and policies. These governing bodies actively participate in maintaining security and digital risk management throughout the usage of EHR.

Table 1 shows a summary of the Governing Bodies for EHR around the world. The implementation of policies and acts that manages the security of EHRS globally is summarized in Table 2.

2.3 Health insurance portability and accountability act (HIPAA)

The HIPAA of the United States addresses several issues regarding the implementation and the maintenance of the EHR in the country. As summarized from [16], HIPAA ensures that health organizations implementing EHR have security standards that take into account the technical capabilities of recording systems used to maintain health information and the need to train people who have access to the health information. In addition, it requires large organizations to have policies and security procedures, which isolates the activities of EHR usage
Table 1. Governing bodies for electronic health records.

<table>
<thead>
<tr>
<th>No.</th>
<th>Country</th>
<th>Governing body; working systems, if any</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>International</td>
<td>World Health Organization International Federation of Health Records (IFHRO)</td>
</tr>
<tr>
<td>2.</td>
<td>United States of America</td>
<td>Office of National Coordinator (ONC) Ministry of Health (MOH); Electronic Medical Record Xchange (EMRX) National Healthcare Group (NHG)</td>
</tr>
<tr>
<td>3.</td>
<td>Singapore</td>
<td>SingHealth National Medical Ethics Committee (NMEC)</td>
</tr>
<tr>
<td>4.</td>
<td>European Union</td>
<td>Comite Europe de Normalisation (CEN) Technical Committee 251 (Medical Information)</td>
</tr>
<tr>
<td>5.</td>
<td>Switzerland</td>
<td>International Medical Informatics Association (IMIA)</td>
</tr>
<tr>
<td>6.</td>
<td>Canada</td>
<td>Health Canada, Committee on Information and Emerging Technologies</td>
</tr>
<tr>
<td>7.</td>
<td>Australia</td>
<td>National E-Health Transition Authority (NEHTA)</td>
</tr>
<tr>
<td>8.</td>
<td>Hong Kong</td>
<td>Department of Health, Food and Health Bureau; Smart ID Cards</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Hong Kong Medical Association; Patient-held Record</td>
</tr>
<tr>
<td>9.</td>
<td>Japan</td>
<td>Ministry of Health, Labour, and Welfare; Computerised Patient Medical Records (CPMR)</td>
</tr>
<tr>
<td>10.</td>
<td>Malaysia</td>
<td>Ministry of Health Malaysia and Department of Public Health; Lifetime Health Record (LHR)</td>
</tr>
<tr>
<td>11.</td>
<td>Taiwan</td>
<td>Department of Health, Taiwan, ROC; National Health Insurance-Identity Cards (NIH-IC)</td>
</tr>
</tbody>
</table>

Table 2. Implementation of EHR policies and acts for various countries.

<table>
<thead>
<tr>
<th>Country</th>
<th>Implementation of EHR policies and acts</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States of America</td>
<td>Health Insurance Portability and Accountability Act (HIPAA)</td>
</tr>
<tr>
<td></td>
<td>Certification Commission for Healthcare Information</td>
</tr>
<tr>
<td></td>
<td>(a) Privacy and Compliance Work Group</td>
</tr>
<tr>
<td></td>
<td>(b) Security Work Group</td>
</tr>
<tr>
<td></td>
<td>Health Information Security and Privacy Collaboration (HISPC)</td>
</tr>
<tr>
<td></td>
<td>Health Information Technology for Economic and Clinical Health Act (HITECH)</td>
</tr>
<tr>
<td></td>
<td>American Health Information Community (AHIC)’s Confidentiality and Privacy</td>
</tr>
<tr>
<td>Canada</td>
<td>Personal Information Protection and Electronic Documents Act (PIPEDA)</td>
</tr>
<tr>
<td></td>
<td>Privacy Working Group of the F/P/T Advisory committee on Health Information (ACHI)</td>
</tr>
<tr>
<td>Australia</td>
<td>NETHA Privacy Blue Print</td>
</tr>
<tr>
<td></td>
<td>Australian Law Reform Commission (ALRC) review of the Privacy Act</td>
</tr>
<tr>
<td>New Zealand</td>
<td>Privacy Act</td>
</tr>
<tr>
<td></td>
<td>Health Information Privacy Code (HIPC)</td>
</tr>
<tr>
<td>European Union (EU)</td>
<td>Implementing Secure Healthcare Telematics Applications in Europe (ISHTAR)</td>
</tr>
<tr>
<td>Singapore</td>
<td>National Medical Ethics Committee</td>
</tr>
<tr>
<td>Malaysia</td>
<td>Private Healthcare Facilities and Services Act 1998</td>
</tr>
</tbody>
</table>

so as to prevent unauthorized access to EHR. Lastly, it states that appropriate administrative, technical and physical safeguards have to be maintained during the process of transmitting EHR so as to ensure the integrity and confidentiality of the information.

2.4 Extraordinary procedures

Emergency access procedure (EAP) is a required implementation specification defined within the access control standard in the technical safeguards section of the HIPAA security rule. The objective of the emergency access procedure implementation specification is to establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. Emergency access is a necessary part of access control and will be necessary under emergency conditions, although these may be very different from those used in normal operational circumstances. EAP are procedures for obtaining necessary electronic protected health information during an emergency [18].

These procedures are written instructions and operational practices for gaining access to necessary EHR during an emergency. Access controls are required during an emergency. Beforehand, organizations must decide what circumstances would warrant emergency access to EHR information.

An example would be the break-the-glass (BTG) capability. Medical personnel can invoke the BTG capability if they require urgent access to the EHR, but do not have sufficient rights. A special audit trail is created when the capability is used. This provides a strong deterrent to unauthorized access or misuse of the function [20].

3. Results and discussion

3.1 Case study of electronic medical record Xchange (EMRX)

In 2004, Singapore’s Ministry of Health (MOH) and the two public health clusters – Singapore Health Services and the National Healthcare Group – initiated EMRX to allow sharing of electronic medical records between the two clusters. MOH envisions EMRX as the first step to the creation of a genuine National Medical Records System for Singaporeans. Today, EMRX extends its reach to public hospitals, polyclinics, specialist centers and community hospitals.

Currently, only the two public health clusters and community hospitals are allowed to share their patients’ electronic medical records. However, the situation is about to change soon. In line with the Ministry of Health’s vision of “One Patient, One EMR” and Singapore’s Intelligent Nation
Security Issues in E-Healthcare

2015, EMRX will be extended to the private hospitals and clinics and eventually, the whole health sector in Singapore. The purpose is to allow seamless integration and enable true interoperability.

EMRX is a computer platform that connects the EMR systems of the two clusters and community hospitals. This allows the doctor treating a patient at a particular hospital or polyclinic to view the EMR of the patient that was created in the hospitals of the other cluster. To access the EMR of the patient, the doctors will need the National Registration Identity Card (NRIC) number of the patient. This is because the NRIC number is mapped to the patient’s record. According to the EMRX documentation, the following medical information is shared: (1) discharge summaries, (2) laboratory test results, (3) X-ray and other radiological test results, (4) medical operation reports, (5) drug allergies, (6) medicine prescribed, (7) cardiac reports and (8) emergency department reports.

3.2 Discussion

As mentioned above, privacy is one of the main concerns when implementing EMRX. Privacy is a duty of care. The hospital, being the custodian of the confidential information, owes a duty of care to the patients as there will be serious implications when the information is not secure, whether misused or simply leaked. A wide range of people both in and out of the healthcare industry share our medical information. Generally, access to an individual's records is obtained when that individual/person agrees to let others see them. In reality, one may have no choice but to agree to the sharing of his health information if he is to receive healthcare and qualify for insurance. There are many questions concerning privacy, including where the safeguard of privacy should come from and where it extends. Some issues of privacy:

(1) No explicit right to control access to and dissemination of information about oneself. This means one cannot sue successfully for invasion of privacy when he feels that his personal health information has been disclosed without consent.

(2) EMRX captures the full data complement, including sensitive medical information: sexually transmitted diseases and mental health indications.

(3) The Ministry of Health has fewer controls over private-sector and voluntary welfare organizations.

(4) The policy preference for many health organizations is self-regulation, where they establish their own code of practices. However, compared to statutes, codes tend to be weak and hence, enforcement is difficult.

(5) Privacy regulations are lacking in technological specifications.

The confidentiality of the patient’s medical record is important. If the privacy is breached, it can affect different parts of the EMRX application, such as the hospital information service (HIS), clinical information systems, radiology information systems (RIS) and pharmacy information systems (PHIS) [21].

The Computer Misuse Act current governs the use of EMRX. Because electronic health records are computer records, unauthorized access is an offence under Section 3.1 of the Computer Misuse Act, Cap 50A. Under this act, both health clusters are treated as “protected computer” installations. The enhanced punishment for offences covered under Section 9 of the act attracts a fine not exceeding $100,000 and/or jail up to 20 years for unauthorized access or infringement of the act.

However, we shall look at what the Ministry of Health Holdings (MOHH) [22] in Singapore is implementing so as to secure the use of EMRX. The MOHH (previously known as the Health Corporation of Singapore) is the holding company of Singapore’s public healthcare assets [22]. The MOHH provides systems-level coordination and facilitates collaboration across healthcare establishments, and seeks to leverage on synergies and economies of scale across the entire healthcare spectrum, thereby enhancing operational efficiency of the public healthcare sector in the long run [22]. These are the three approaches the MOHH is taking:

(1) Clinically driven: it states clearly who is in charge of each function of EMRX and hence, improves the efficiency and functionality of EMRX.

(2) Guided by an enterprise architecture framework: it draws on the strengths of a method-based, recognized and tested framework.

(3) Synthesizing ideas over the globe: it brings in a useful array of experiences and approaches, e.g., Information model-HL7v3, HL7v2 and NHIN, Spine, Infrastructure.

To safeguard the privacy of the patient’s records, a defensive technological infrastructure must be in place to protect them. The Ministry of Health Holdings (MOHH) and National Computer Systems Pte. Ltd. (NCS) review the EMRX’s infrastructure constantly to ensure its confidentiality and availability.

Firstly, identification is required before using EMRX. For any security system, there are two basic types of identification: password and access token. EMRX utilizes both to provide a better authentication. Every medical personnel is given a password and an access token in the form of a smart card, which is embedded with a chip that stores important information. In the case of EMRX, the chip contains authentication information for use to log in to EMRX. The benefit of using a password and a smart card together is that it can prevent medical identity theft and fraud. When a medical staff loses the smart card, the intruder cannot log into the system because he does not have the password and vice versa. Hence, this form of authentication is very secure.

Secondly, an intrusion detection system (IDS) is used within EMRX. IDS refers to a category of defensive tools that are used to provide warnings indicating that the system is under attack or intrusion. The purpose of IDS is to help identify an attack against information systems. EMRX uses a host IDS (HIDS) as it provides a better overall protection compared to network IDS (NIDS). According to Internet Security Services (ISS), one of the strengths of HIDS is the ability to monitor specific system activities. HIDS can monitor the user’s activities when he is logged on to EMRX. If HIDS identifies suspicious activity from the user, it will log off automatically, and a warning is set off to inform the relevant authorities.
However, IDS only acts as a complementary security feature. The most important feature of EMRX is its firewall. A firewall is a security system that acts as a protective boundary between your computer and the outside world. It helps make your computer invisible to online attackers and some malicious software such as viruses, worms, and Trojan horses.

Regarding the evaluation of EMRX in practice, as EMRX was designed as a document-level exchange, with no standardized or structured data, difficulties arose when medical practitioners wanted to seamlessly share data beyond the document-level [23]. Sharing of diagnostic images such as X-rays could not be exchanged over EMRX because various institutions use different vendors and their current viewers use different versions of image protocols. SingHealth and National Healthcare Group (NHG) also operated their electronic medical records independently, which further impeded the sharing of medical records between different healthcare providers. Because of the limitations of EMRX, the Singapore government is replacing EMRX by the next phase of the National Electronic Health Record (NEHR), which will cost $176 million and is scheduled to be implemented by April 2011 [23]. The new system will be expanded to include a number of healthcare providers, including general practitioners (GPs), polyclinics and hospitals. The Health Ministry stated that the next phase will aim to achieve the goal of creating a truly personalized and ubiquitous national health record [23]. Important information such as a patient’s demographics, allergies, clinical diagnoses, medication history, X-rays, laboratory investigations and discharge summaries will be fully exchangeable between various healthcare providers.

4. Conclusions

The EHRS is the key to developing truly digital healthcare, where everyday operations and record-keeping are carried out and maintained almost exclusively with computers. Although EHRS is a healthcare priority in many countries, progress in implementing EHRS has lagged behind the latest information technologies available. Furthermore, the diverse heterogeneous environments of many EHRS make maintaining the systems very difficult.

The development and implementation of EHRS is by no means an easy task, and requires the collaborative support of HCEs and governments to truly succeed. This paper has explored the architecture and design of the EHRS for increased security, privacy, and mobility by examining the policies, regulations and technologies for EHRS security. However a standardized approach to the development of EHRS is still lacking in the medical world today, although several models of standardization for electronic medical records exchange are currently being designed and evaluated. Ultimately, the success of EHRS will depend on the standardization of a common health information infrastructure, initially at the national level, so that the goal of a truly global EHRS can be realized.

References