J Med Syst (2012) 36:3019–3027
DOI 10.1007/s10916-011-9779-x

ORIGINAL PAPER

Advances and Current State of the Security and Privacy in Electronic Health Records: Survey from a Social Perspective

Antonio Tejero · Isabel de la Torre

Received: 20 July 2011 / Accepted: 9 September 2011 / Published online: 21 September 2011

Abstract E-Health systems are experiencing an impulse in these last years, when many medical agencies began to include digital solutions into their platforms. Electronic Health Records (EHRs) are one of the most important improvements, being in its most part a patient-oriented tool. To achieve a completely operational EHR platform, security and privacy problems have to be resolved, due to the importance of the data included within these records. But given all the different methods to address security and privacy, they still remain in most cases as an open issue. This paper studies existing and proposed solutions included in different scenarios, in order to offer an overview of the current state in EHR systems. Bibliographic material has been obtained mainly from MEDLINE and SCOPUS sources, and over 30 publications have been analyzed. Many EHR platforms are being developed, but most of them present weaknesses when they are opened to the public. These architectures gain significance when they cover all the requisites related to security and privacy.

Keywords E-health · EHR · Privacy · Security

Introduction

The evolution of the population has led to the changes in how the medical care is provided; nowadays, due to an increase in the older population (inverted pyramid effect), medical centers are packed of people and have less physical resources available. However, whereas the cost of treatments has increased, the implementation of digital solutions becomes less expensive. Therefore, since its appearance in the telematics technologies, E-Health has turned into a very powerful tool, being meaningful for both patients and medical professionals. Within this field, Electronic Health Records (EHRs) are remarkably useful to build a manageable and solid information system that, in accordance with current electronic services, offers a patient-focused care. These systems comprise information of many types and from many sources, as it is shown in [1]. The authors conclude this statement after performing a sytematic review about the content of EHRs. Records are accessed by multiple health workers, and compile data that ranges from past medical history to diagnoses, tests and treatments. It is also stated in this paper that this medical information has to be presented following a specific structure as well. Moreover, EHRs should follow a common standard to achieve interoperability, which would make them available in any context where patient information is needed by health professionals.

The motivations to implement this kind of systems in the medical area are reasonably clear; but just like any other technology that handles personal information, EHRs are subjected to security and privacy issues. This is crucial in EHRs since they involve very important private data, as important as banking information. These aspects of EHRs have motivated this paper, which presents an overview of the current state in security and privacy issues in the EHRs work field.

The remainder of this paper is in the following structure: "Advances in security and privacy in EHRs" reviews some of the last researches that address security and privacy in

A. Tejero · I. de la Torre (✉)
Department of Signal Theory and Communications,
University of Valladolid,
Paseo de Belén, 15,
47011 Valladolid, Spain
e-mail: isator@tel.uva.es

A. Tejero
e-mail: atejpab@ribera.tel.uva.es

EHRs, in order to obtain a general perspective on how these issues are being dealt nowadays. “Current state in EHRs” details a brief commentary on how security and privacy in EHRs are being implemented at the international level, not from the technical point of view, but from a social perspective. Section 4 offers a discussion on the different approaches introduced throughout the article, and to conclude, “Conclusion” summarizes the main conclusion of this paper.

Advances in security and privacy in EHRs

Portability in EHR systems

While social causes impulse the appearance of integrated e-Health solutions and EHRs, the blooming in information systems and Internet technologies has allowed developing more complex systems and infrastructures. Technology is more efficient and accessible, and those same characteristics are needed in EHRs. When the information is turned into bits it is more manageable, but it is still vulnerable as it happens with other digital media. Hardware is improved very fast, but attackers become more sophisticated at the same rate.

Therefore, as explained in [2], medical information is also subjected to piracy and EHR systems can be hacked if they are not properly protected. This situation involves a new paradigm related to security and privacy. This paper also defines security and piracy objectives that play an important role in the context of web-based EHRs. Considering that current deployed solutions present clear weaknesses in terms of security, it is concluded that a holistic approach, whose functionalities cover all the aspects of EHRs, can overcome the drawbacks of already existing systems.

Many studies, i.e. [3], conclude that in order to obtain the full potential of EHRs, patients should be able to access them anywhere and anytime. This can be achieved by making EHRs portable, turning them into Personal Health Records (PHRs); a solution is to keep PHRs in portable storage media, such as USB flash drives. This portability adds an additional mobility feature whose security needs to be covered; it is necessary to prevent the data from being exposed.

Portable EHRs are the option used when they cannot be transmitted via network. But when patients take care of their own health information, security and privacy can be violated. In [4], the authors propose a method to protect portable EHRs; to achieve this, three requirements have been identified to be met: measures protecting confidentiality, validity of the EHR to protect the patient’s rights, selective protection of privacy for consultations with a trusted third party.

The method was designed following HIPAA guidelines. It is a secure process that assures anonymity in secondary uses, for example: de-identification, pseudonymity, patient selection and encryption. It includes a recovery process (decryption, verification) to protect EHRs when they are being held that can be used by patients themselves. The solution is a method that applies cryptography such as the application of digital signatures, encryption algorithms and digital certificates. Besides security protection with smart-card by applying cryptography such as protecting under PKI, the solution also provides privacy preservation of EHRs. The study is also aimed at identifying different data types (text, images) of an EHR.

The results of this study show that the methods that have been put into practice are effective in ensuring both information security and privacy preservation through portable storage medium when it is used by patients or carried outside the hospital.

Access control in EHR systems

When a Health Record is turned into an electronic format, it acquires the capability of being ubiquitous; but for this, it needs to collect information from a wide variety of medical sources. This type of shared EHRs deals with sensitive information that needs to be accessible only to those entities allowed by patients. These constraints are translated into access control requirements.

Traditionally, Role Based Access Control was the predominant method in the EHR area, as explained in [5]. But according to this paper, recently appeared standards find its way to replace previous methods of access control. eXtensible Access Control Markup Language (XACML) is an example of this. XACML is not technology related, and IT leaders such as Sun have published their own implementations. XACML consists of attributes values of defined type and name that is to be attached to a subject, a resource, an action and an environment in which a subject request action on resource.

The paper works with the aforementioned Sun’s version. As a related work on hierarchy access control policies, the European system ARTEMIS is described. In ARTEMIS, healthcare providers can define privacy policies that indicate which professional has the rights to access certain medical data.

Then, the paper examines performances in CEN 13 606 and ISO 22 600 based healthcare system which uses XACML for access control. XACML is applied in the MEDIS system for access control. MEDIS is a multidomain EHR system. The scenario presented provides master access control policies on the central server and local policies on clinical servers. Following ISO 22 600, access control policies are attached to the resources. Besides, attributes in policies have a hierarchical organization as in ARTEMIS.

The results of this research show that performance does not worsen, independently of the type of architecture utilized (tree or forest) and in the case of writing a policy with several attributes in hierarchy.

In [6], the authors propose an access control model for selectively sharing EHRs. Their model represents the internal structure of a health record in a hierarchy where data objects are associated in terms of properties. This allows addressing important criteria for medical data sharing, which is used to give authorization to specific parts of the EHR. Besides, to regulate this system it is needed a unified policy scheme; but when distributed EHRs have to be dynamically aggregated, integration of access control policies is needed. For this purpose, another contribution of this paper is a mechanism to solve policy inconsistencies, independently of the data source; this mechanism is divided into two parts: anomaly classification and anomaly detection. Finally, the paper explains the design and implementation of a composite EHR sharing system for integrated and federated healthcare networks; the patient is able to control the authorization for consulting medical information.

The results of this work are positive for the implementation of the prototype, but its efficiency in performance is still to be evaluated.

Another common scenario is a hospital where staff access to patient data. The different health workers should have different permissions with respect to the patients' information. A powerful tool is to create roles within a system so all the information cannot be accessed without permission. In [7], a health information system that uses an extended digital certificate to support high privacy levels natively is proposed. This system is based in an EHR stored in patients' mobile device so they can have more control over it; therefore, this approach allows performing authentication and access control. There are also given some examples in which a person exchanges medical information with different health specialists by means of a certificate issued by a health authority. In conclusion, this system achieves flexible interactions, which can vary depending on the information flow. However, special measures that need to be considered if the device gets lost are not discussed.

Transmission of EHRs

If the use of a portable system implies using additional security methods, when a distributed e-Health system is designed, these measures have to be taken into account as well. Internet accesses can expose personal information to the public if it is not well protected; this is especially delicate when an unsecured communication network is used.

When it comes to security in EHRs, it does not involve only patient's data in text format. Medical images are also subjected to protection, and due to their digital characteristics, special measures have to be taken into account. They can be compressed and transmitted easily, but they can be intercepted as well.

In [8] the authors explain how to use a watermarked image to protect this type of medical data. The watermarking technique embeds information within a multimedia signal, being imperceptible for attackers. Besides, when an image is watermarked, it still complies with the Digital Imaging and Communications in Medicine (DICOM) format.

They explain how previous studies that apply watermarking cause non-reversible distortion in the original image, being impossible to recover it. On the other hand, recent reversible watermarking works do not take into account the Region Of Interest (ROI) of the image; so, in order to avoid wrong diagnostics, watermark extraction and the original image restoration must be performed every time. The paper presents a region-based lossless watermarking scheme for medical images to check authenticity and integrity, since any modification in the watermarked image can be detected. The embedding regions can hide large amounts of data and can be chosen so as not to interfere with the ROI, although the ROI has to be identified manually. This way, the exact recovery of the original image is only necessary when the integrity of the image wants to be checked.

This embedding mechanism allows:

- Verifying the integrity of the images embedding a digital signature.
- Verifying the authenticity of the images processing the watermark and its respective EHR at the same time. To improve this feature, the patient's fingerprint information can be included.
- Detecting unauthorized accesses.
- Multilayer embedding.
- Hiding patient's confidential information.

To conclude, it is shown that, experimentally, this scheme achieves high embedding capacity with a low level of distortion.

As important as protecting the data contained in EHRs is to make transactions over a secure architecture. Alanazi et al. (2010) offer an overview of different architectures and systems to record patient related information [9], putting special emphasis on the patients' rights. As they explain, it seems hard for developers to provide security and privacy to an e-Health platform, characteristics that are required even before the system is utilized. These systems need to provide security and privacy in transactions, and reliability in the information they handle. In this paper, main security features are analysed: authentication, authorization, privacy, confidentiality, integrity and non-repudiation. Although the literature the authors revised to write the article was based on recent filters, a system that met all those security requirements at the same time could not be found. Besides, it was determined that old algorithms such as RSA, which is currently used in cryptographic operations with EHRs, present a poor level of efficiency. A new PKI standard called NTRU was approved in 2009 and allows much faster crypto-operations (up to 200 times) with the same level of security. To conclude, it is stated that Electronic Medical Record systems have to take into account not only patients' privacy, but also their legal state in order to be protected.

A quite interesting point in the study carried out in [10] is that most EHR architectures perform only local operations, and when it comes to communicate with each other, very specific data exchanges are implemented. However, when clinical information is requested by many different external parties, the organization of this content needs to be adapted. Ensuring secure health information exchange across organizations requires a global standardization, such as HL7v3.

This paper explains how health information is exchanged between health care organizations, studying a typical scenario. The scenario consists of a set of organizations connected transparently through a central service. This setting has been chosen because it represents a generic networked environment. The central service provides a repository and an index service to access information.

The method utilized is practical; based on that, generic realistic scenario questions were formulated following a series of steps and divided in different themes. Twenty-six questions are raised and answered using relevant reference material. The addressed issues are showed and described in Table 1.

The paper concludes that the current tendency to retrieve information involves a one-to-many exchange and a search-and-retrieve paradigm. In order to create a robust EHR system, authorization, restrictions and consent have to be implemented, as well as confidentiality and relevancy. Archiving information for its future use is also a topic that needs more clarity.

A lot of other different architectures are being proposed in order to offer strong security features. As it is mentioned before, these systems should be patient-oriented so that a person can interact easily with specific information among the amount of data collected in an EHR, but always protecting the user's privacy. It is necessary to allow reliable secure interactions in EHRs systems, especially in cases of emergency when a health record has to be consulted immediately. To really achieve a robust system, it is necessary to guarantee interoperability among other platforms by adopting a common standard. All these issues are discussed in [11], where studies about how patients adopting an EHR system show positive results are referenced. The main problem found was the fact that once an EHR system is adopted, people are generally not likely to maintain it.

Given this background, [11] makes a revision of the literature from the security and privacy points of view. A discussion of possible EHR architectures is presented and then three different EHR structures are proposed and compared to analyze their benefits; tethered, integrated and standalone architectures are discussed. To summarize, tethered systems are the simplest, being the primary care center responsible for the management of EHRs, including security, privacy and data integration. On the contrary, integrated architectures are the most complex, collecting information amongst different sources and managing security and privacy issues in a centralized way. On the other hand, standalone platforms not only offer direct access to health data via Internet, but also propose the use of a portable smartcard. Although this last system allows patients to have more control of their data, the use of a smartcard presents problems such as loss or theft, so security issues have to be addressed in terms of encryption

Table 1 Issues in the study [10]

Issues	Description
Authorized access	Define how to implement identification, authentication, and authorization across organizational boundaries.
Confidentiality	Define how can be determined that no confidentiality breach has occurred when a copy of the information resides in another system.
Patient consent	Aspects about how patient's restrictions need to be managed.
Relevancy	How to define what information is relevant enough to make it available.
Ownership of information	Defining ownership and its implications.
Infrastructure	Version management, sending notifications on data.
Audit log	Storing information for review purposes, content and function.
Archiving	Legal retention time of data and its implications.

as well. As it has been mentioned before, it is also concluded that the main barriers are interoperability and the adoption of EHRs by family physicians.

Current state in EHRs

Observing the international scenario, it can be determined that EHRs are not adopted in the same way in all countries. Whereas the United States and Canada are the most advanced countries in EHRs integration, in others such as Spain EHRs are not that widespread. Bearing this in mind, security and privacy are of course handled in different ways.

Legal background

In order to introduce the current state of EHR regulation, the main points in the Spanish and American law about health records are summarized below.

There are two main rules applicable to the EHR systems in the Spanish law [12, 13]. Article 9 of Law 15/1999 states that "*no personal data will be stored in files that do not meet the requirements of integrity and security*". This affect directly to the security subsystem.

Similarly, in the Law 41/2002, Article 16 establishes the usage of health records and the necessity of separate identification data from the clinical-care data to guarantee anonymity. Besides, article 18 states the right of the patient to access his or her health record if third parties are not affected [12, 13].

Another important paragraph from this law explains that "*The Ministry and the regional governments shall promote the implementation of a compatibility system that enables its use by health care centers in Spain*".

At the international level, the law that controls security and privacy in clinical data in the USA is the HIPAA. There exist two amendments that control security and privacy [14].

Privacy rule establishes that Protected Health Information (PHI) can only be revealed by court order or by the consent of the patient, showing the minimum required data.

Security rule was adopted in 2003, and it was developed to handle the challenges derived from the digitalization of the data and the use of EHRs. It establishes three types of security warrants: administrative, physical and technical.

The administrative safeguard reunites policies and procedures such as the creation of a privacy agent responsible for the compliance with the security policies and the correct accesses to the EHRs. It also promotes the creation of a plan in case of emergencies and internal audit to detect security violations.

The physical safeguard focuses on the physical access to protected data, limiting hardware and software handling to authorized persons via maintenance and visit logs.

Technical safeguard controls telematic accesses and allows medical institutions protecting their communications on public networks. Entities are responsible for data integrity (via digital signature) and third-party authentication (via passwords and others). They must also document the entire configuration and carry out a risk analysis and management program.

In 2009, these rules were extended into the HITECH Act. Besides the healthcare providers, now associated companies have the aforementioned obligations. Another addition is the obligation of informing the healthcare department of potential security issues that had occurred. Finally, since January 1st, the maximum retention of EHR revealed data is reduced from six to three years.

Security and privacy in health-related information has gained public attention in the last years. The Office of Civil Rights in the Department of Health and Human Services (HHS) has been very criticized because of the lack of strong penalties in HIPAA's security and privacy rules.

But according to [15], healthcare companies are getting a great variety of information in the security area, thanks to the incremental developments that have been implemented, consisting of three new enforcements. Now companies have more clues to make their services comply with HIPAA, although HHS has become more proactive in terms of sanctioning. As a result, companies need to review their programs to verify the compliance with HIPAA regulation, and therefore use the latest technological advances in security and privacy preservation. The three enforcements mentioned before consist of audits and investigations that in some cases included monetary penalties. Companies should be clear reporting security breaches and other related incidents in order to avoid bigger risks. Although these measures may seem aggressive, in the near future there will not come too many similar actions. All these enforcements are intended to establish a standard for security and privacy laws, so current services can be evaluated.

When establishing new legal measures, it should be very important to consider what their target is. Besides, the content of modern EHRs tends to be more and more complex. A perfect example of this are the large datasets associated with genetic/genomic tests and interpretations. According to [16], this type of data can determine diseases and treatments included in the EHR. This paper offers a discussion on how to deal with security confidentiality and privacy, analyzing whether special measures should be taken to protect this type of information, and focusing on important points to create a policy to regulate genetic data.

After classifying this information as sensitive data and defining what type of tests can be labelled as genetic/genomic, the paper describes the characteristics of genetic/genome test information that should be considered to decide what level of protection is appropriate (see Table 2).

Table 2 Characteristics of genetic/genome test information

Characteristic	Description
Uniqueness	Genetic/genomic information is a potential database for individual identification purposes.
Predictive capability	It can prevent diseases, but also can be used to discriminate based on predisposition.
Immutability	An individual's inherited information does not change throughout life.
Requirement of testing	Many genetic markers must be derived from a test.
Historical misuse	Genetic/genomic test information could be used inappropriately to stereotype individuals.
Variability in public knowledge and perspectives	Wide range of understanding and feelings about the role of genetics in health.
Impact on family	Germline mutations may reveal information about medical risks to blood-relatives.
Temporality	Given the exponential growth molecular diagnostics, the ability to interpret test results will evolve rapidly.
Ubiquity and ease of procurement	Genetic information may be obtained without the knowledge of the patient.

The main conclusions drawn in the paper were that restricted access should be guaranteed for genetic/genomic data, as it occurs with other sensitive health information contained in EHRs. Thus, potential discrimination due to genetic/genomic information is avoided. Also, it is necessary to define the proper usage of such data for research purposes.

Taking these legal matters into electronic medical platforms is an essential but not so straightforward issue. From the Hippocratic Oath to the American Health Insurance Portability and Accountability Act of 1996 (HIPAA), regulations have been imposed to enforce law into healthcare; this has to be especially remarkable with computer-based systems.

Law and regulations are approved by governments in order to protect security and privacy. These act as requirements for engineering systems and must be met. In [17], the authors provide an explanation on how to apply security requirements into the healthcare field, within an EHR system called iTrust. The iTrust has been created and improved in an academic environment, evaluating its compliance with relevant law, specifically, the HIPAA regulation. The methodology followed to carry out this task is composed of 4 stages: Terminology mapping, Requirements identification and disambiguation, Requirements elaboration, Tracing requirements to legal texts.

The development of this study allowed specifying four main lessons. First, actor hierarchies are essential for security and legal compliance; by defining these hierarchies, legal rights and obligations can be stated in the resulting software. Second, unresolved ambiguity can lead to security and privacy non-compliance; infer the intended meaning in the statements is a challenging but rewarding point in this methodology. Third, prioritizing requirements is helpful for identifying critical security requirements; for the practical purpose, four categories were created (Critical, High, Medium, and Low). Fourth, requirements engineers need tool support for determining legal compliance; efficiency would be increased by automating repetitive tasks.

They conclude explaining that software systems outside the HIPAA domain have insufficient requirements documentation and poor traceability, a situation that should change in the future.

The PIPE system is an interesting case study that matches the points made in the literature reviewed. Healthcare sector produces a huge amount of data and its management is very costly. The using of EHRs along with the digitalization of medical images allows the communication and sharing of medical data among the different physicians.

Since sensitive medical information is stored in EHR systems, people may be worried about their privacy because an unauthorized person could exploit a vulnerability of the system and get access to private information.

In order to guarantee an appropriate level of privacy, medical information needs to be stored in a confidential fashion. Besides doing it cryptographically, a form of pseudonyms is applied. This last technique separates the identifying attributes of a set of data from the useful information. Then, medical information can be stored while preserving the privacy of patients.

It is a safe system, not only confidentiality but also data integrity needs to be guaranteed. If not, a malicious user could modify stored data and consequently patients could receive the wrong dose of medication. Whereas the pseudonym technique provides confidentiality, data integrity is secured using digital signatures. This is because pseudonyms are based on storing data in plain text form.

As it can be read in [18], PIPE system (Pseudonymization of Information for Privacy in e-Health) all sets of data are kept in a storage system that consists of two independent databases. One keeps pseudonyms in plain text and the related sets of medical data, which are stored in plain text due to performance reasons. The other database is used to store users' personal information and encrypted pseudonyms.

PIPE consists of patients (users), relatives, healthcare and operators. The patient is the owner of their data and has total control of it. Each patient can grant a relative access to all their medical data. Physicians can be allowed to see these data. Operators, which are the administrative roles, share the secrets with patients to provide a security method in case a smart card to access data is lost or destroyed.

Pseudonym is only known by the patient and ensures that anyone except he or she is able to delete all pseudonyms of an anamnesis (relevant clinical data from a patient's record) and therefore access to medical data. For example, if two healthcare providers are authorized to see a specific set of medical data, there exist three different pseudonyms [19]. Consequently, if those pseudonyms that are shared between the patient and medical healthcare are deleted, the patient could still access their medical data without any problem. This allows patients to have a total control of their data, whether authorizing or revoking rights any moment, as defined in the European law.

The pseudonymity method manages to avoid discrimination by insurance companies and employers, since the link between a patient and the EHR cannot be determined [20]. Also, security analysis shows that this technique can prevent data misuse in common intruder scenarios.

The PIPE system approach ensures patients the necessary level of privacy. In other words, even if the communication among these actors is transmitted over an unsafe channel as Internet, confidentiality is guaranteed because all attributes in the database are already secured by encryption.

International comparison

This subsection explains briefly what kinds of methods have been adopted in some parts of the world to achieve a secure and private EHR system.

As explained in [21], in Germany the choice of the standalone smartcard PHR is close to national implementation. In the United States, implementations and/or tests of all the suggested architectures except the standalone smartcard are underway. In the United Kingdom, the National Health Service (NHS) appears to have settled on an integrated architecture for PHRs. It is also becoming clear that Canadian healthcare agencies are settling on integrated architectures for electronic patient health records.

Traditionally, protection of privacy in the European Union, including medical information, has been considered more coherent than that one in the United States. Taking this into account, to manage the implementation of a solid EHR system in the USA, it is necessary to discuss not only the technical aspects but also the policy framework that guides it.

In [22] EU and USA are compared in terms of privacy and security from the legal point of view, concluding that EU is more proactive, having the USA a more reactive role. Whereas the USA invests more money in healthcare than the EU, security and privacy issues prevent a public adoption of EHR systems in the country. The main problem is the fear to identity theft, creating the necessity of better storage and transmission frameworks. Besides, the EU establishes exceptions in which the access of personal data requires the patient's authorization. On the other hand, USA patients do not have privacy control of their data, which can be even utilized by insurance companies if not sufficiently protected. To conclude, authors also analyze the trade-off existing between offering easiness of access and the protection of patient information, showing that it is difficult to provide them at the same time.

Even though in USA the development of EHR systems has lead to a better quality in healthcare services, according to [23], it is uncertain if these benefits affect to all patients equally, including racial/ethnic minorities. The main reasons to take this into consideration is that they may have less financial resources to afford these systems and that minorities receive healthcare service in different settings. Giving the importance of this issue, this paper studies the adoption of EHR systems by minority-service providers and compares it with that of the rest of providers.

The data was obtained from surveys of medical practices in Massachusetts in 2005. A random sample was taken, from physicians of all kinds of specialities and a questionnaire was elaborated to this purpose.

This analysis tries to answer three questions: do providers that care for large-minority populations have lower rates of adoption of EHRs? Do these providers face different barriers to adoption of EHR systems? Is their satisfaction with EHR systems comparable with other providers?

The results show rates of EHR adoption are similar in all providers. Physicians that serve minorities note financial and other barriers to implementing EHR systems at similar rates as the rest of providers; however, these physicians were less likely to be concerned with privacy and security concerns of EHRs. At last, physicians from high-minority practices had comparable opinions about the positive impact of EHRs on quality and costs of care.

The article concludes that there is no evidence that providers adopted less EHR systems when serving minority population. Also, they did not face different barriers when adopting these systems, neither were less satisfied with them.

The limitations of the method utilized in this paper are described as follows: The data used comes from a single state; physicians' self-report of the racial composition was used; it was not checked objectively if minority serving physicians obtain the same benefits from EHRs.

But these issues do not only affect developed countries, also emergent and under development territories are subjected to telemedicine improvements, according to [24]. This article explains a way to set up an approach to an EHR system using existing social customs. A portable electronic device is used to store the patient's medical history and other medical data. Then, the patients wear it as a talisman whenever and where ever he visits a doctor, clinic or a hospital.

E-Health integration in Korea [25] includes realizing EHRs and providing interoperability of information amongst hospitals. To achieve this, it is necessary to take into account security and privacy in e-Health data to prevent discrimination. The article concludes stating that the government should take part in the process of implementing e-Health, in order to apply the appropriate policy. Individual privacy issues appear when creating an EHR system, and should be handled in a centralized way by the public sector, whereas data collection and transactions need the cooperation among different agencies to manage interoperability.

Other country where EHR systems begin to be implemented is Iran. In [26], authors carry out a comparative study in order to describe what Security Requirements and Solutions would need a healthcare electronic system in Iran. EHR information security requirements of Australia, Canada, England and U.S.A. are analyzed following a three-stage method: comparative study, design of the preliminary model, evaluation of the reliability of the proposed model.

After performing a study of the EHR security requirements of the four selected countries, these are described, and addressed according to different issues: organizing information security, classifying and controlling information asset, security of human resources, environmental and physical security, operational and communication management security, information access control security and development and maintenance security of Electronic Health Records information systems.

These seven pivots obtained in the research process are suggested to compose an EHR model that guarantees security. Although each of the subject countries uses only part of this new model, the paper states that Iran has still much to do in the electronic medical field.

Discussion

EHR systems require a high level of security and privacy control because they can provide great accessibility (whether wired or wireless, local or remote) to the patients' personal medical information. The majority of current systems address these implications in a different form, and even different countries apply their unique policy to their respective e-Health systems.

As any other digital platform that deals with private information, EHRs need to be robust without any open issue; moreover, EHRs contain data that may decide the life of a person in a critical situation. Since people can attend different hospitals and suffer unpredictable illnesses, EHRs need to be available anywhere and anytime, but that implies more security and privacy. Whether the information is accessed via Internet or stored in a portable device, different architectures are proposed, dealing with security issues in distinct ways. That means that, for now, when a EHR system is to be implemented, the type of architecture used will depend on how it is going to be used and what resources are available at that moment.

To conclude, Table 3 shows the strengths and weaknesses detected in current EHR systems in terms of security and privacy.

Conclusion

E-Health systems are the main application of modern technologies to the area of medicine. A lot of EHR platforms are being developed, but most of them present weaknesses when they are opened to the public. These architectures gain significance when they are patient-oriented and cover all the requisites related to security and privacy.

In the literature that has been analyzed, privacy and security are shown in different aspects of the field of EHRs. The digitalization of medical data allows turning the information into manageable bits, so it can be transformed by using different techniques. From the viewpoint of the authors, most of these techniques allow to protect personal information from attackers. However, the reviewed litera-

Table 3 Strengths and weaknesses of security and privacy in current EHRs

Strengths	Weaknesses
Advanced information processing (encryption, etc.)	Lack of interoperability
Avoids using physical resources	Legal system still under development
Multiuser features	Involves sensitive information that may not be protected
More accessibility	EHR adoption depends highly on the willingness of physicians to maintain them
More control of sensitive information	Fear of data theft and phishing

ture shows that when new technologies appear, the previous needs to be replaced, as it happens with encryption mechanisms. Therefore, it is necessary to avoid implementing EHR systems using obsolete technologies. The other important point discussed in this article is the state of the legal background in EHR systems. Important steps have been taken to regulate EHRs and ensure a competent level of privacy. However, more measures will be necessary in order to create strong laws according to the importance of medical data. Besides, as new technologies and protection techniques are introduced into the development of EHRs, laws will need to be adapted to create compliant systems.

In the future, a completely secure and interoperable architecture needs to be designed and implemented to realize the main objective of a system that handles personal medical information. This architecture will need to be supported by a robust legal system that protects the privacy of patients.

References

1. Häyrinen, K., Saranto, K., and Nykänen, P., Definition, structure, content, use and impacts of electronic health records: A review of the research literature. *Int. J. Med. Inform.* 77:291–304, 2008.
2. Slamanig, D., and Stingl, C., Electronic health records: An enhanced security paradigm to preserve patient's privacy. *Communications in Computer and Information Science* 52:369–380, 2010.
3. Sadan, B., Patient data confidentiality and patient rights. *Int. J. Med. Inform.* 62:41–49, 2001.
4. Huang, L., Chu, H., Lien, C., Hsiao, C., and Kao, T., Privacy preservation and information security protection for patients' portable electronic health records. *Comput. Biol. Med.* 39 (9):743–750, 2009.
5. Sucurovic, S., and Simic, D., An approach to access control in electronic health record. *J. Med. Syst.* 34:659–666, 2010.
6. Jin, J., Ahn, G., Hu, H., Covington, M. J., and Zhang, X., Patient-centric authorization framework for electronic healthcare services. *Comput. Secur.* 30:116–127, 2011.
7. Steele, R., and Min, K. Role-based access to portable personal health records. Management and Service Science, pp. 1–4, 2009.
8. Guo, X., and Zhuang, T., A region-based lossless watermarking scheme for enhancing security of medical data. *J. Digit. Imaging* 22(1):53–64, 2009.
9. Alanazi, H. O., Jalab, H. A., Alam, G. M., Zaidan, B. B., and Zaidan, A. A., Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance. *J. Med. Plants Res.* 4(19):2059–2074, 2010.
10. Van der Lindena, H., Kalrab, D., Hasmanc, A., and Talmon, J., Inter-organizational future proof EHR systems: A review of the security and privacy related issues. *Int. J. Med. Inform.* 78:141–160, 2009.
11. Dorr, D., Bonner, L. M., Cohen, A. N., Shoai, R. S., Perrin, R., Chaney, E., and Young, A. S., Informatics systems to promote improved care for chronic illness: A literature review. *J. Am. Med. Inform. Assoc.* 14:156–163, 2007.
12. Law 41/2002 of November 14, basic regulator of the patient's autonomy and rights and obligations of clinical information and documentation matters. BOE 274, sec. 1, pp. 40126–40132.
13. Law 15/1999 of December 13, of the Protection of Personal Data. BOE 298, sec. 1, pp. 43088–43099.
14. U.S. Department of Health & Human Services, HIPAA Administrative Simplification Statute and Rules, www.hhs.gov, last visit March 6 2011.
15. Nahra, K. J., HIPAA security enforcement is here. *IEEE Secur. Priv.* 6:70–72, 2008.
16. McGuire, A. L., Fisher, R., Cusenza, P., Hudson, K., Rothstein, M. A., McGraw, D., Matteson, S., Glaser, J., and Henley, D. E., Confidentiality, privacy, and security of genetic and genomic test information in electronic health records: Points to consider. *Genet. Med.* 10(7):495–499, 2008.
17. Massey, A. K., Otto, P. N., Hayward, L. J., and Antón, A. I., Evaluating existing security and privacy requirements for legal compliance. *Secur. Requir. Eng.* 15:119–137, 2010.
18. Riedl, B., and Grascher, V. Assuring integrity and confidentiality for pseudonymized health data. Proceedings of ECTI-CON 2010, pp. 502–506, 2010.
19. Riedl, B., Grascher, V., Fenz, S., and Neubauer, T. Pseudonymization for improving the Privacy in e-Health Applications. Hawaii International Conference on System Sciences, pp. 255–255, 2008.
20. Neubauer, T., and Heurix, J., A methodology for the pseudonymization of medical data. *Int. J. Med. Inform.* 80(3):190–204, 2011.
21. Daglish, D., and Archer, N. Electronic personal health record systems: A brief review of privacy, security, and architectural issues. Privacy, Security and Trust and the Management of e-Business, pp. 110–120, 2009.
22. Hiller, J., McMullen, M. S,, Chumney, W. M., and Baumer, D. L. Privacy and security in the implementation of health information technology (Electronic Health Records): U.S. and EU Compared. J. Sci. Technol. 1: 2011.
23. Jha, A. K., Bates, D. W., Jenter, C., Orav, E. J., Zheng, J., Cleary, P., and Simon, S. R., Electronic health records: Use, barriers and satisfaction among physicians who care for black and Hispanic patients. *J. Eval. Clin. Pract.* 15:158–163, 2009.
24. Srinivasan, U., Datta, G., Hons, M. S., Hons, B. E. Personal Health Record (PHR) in a Talisman. International Conference on e-Health Networking, Application and Services, pp. 277–279, 2007.
25. Cheong, H. J., Shin, N. Y., and Joeng, Y. B. Improving Korean service delivery system in health care: Focusing on national E-health system. International Conference on eHealth, Telemedicine, and Social Medicine, pp. 263–268, 2009.
26. Farzandipour, M., Sadoughi, F., Ahmadi, M., and Karimi, I., Security requirements and solutions in electronic health records: Lessons learned from a comparative study. *J. Med. Syst.* 34:629–642, 2010.