E-Health Telecommunication Systems and Networks, 2014, 3, 43-49
Published Online December 2014 in SciRes. http://www.scirp.org/journal/etsn
http://dx.doi.org/10.4236/etsn.2014.34006

Scientific Research

A Proposed Layered Architecture to Maintain Privacy Issues in Electronic Medical Records

Ameur Bensefia[1], Anis Zarrad[2]

[1]College of Computer Science and Information Science, Imam Muhammad ibn Saud Islamic University, Riyadh, Saudi Arabia
[2]Department of Computer Science and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia
Email: bensefia@imamu.edu.sa, azarrad@psu.edu.sa

Received 23 September 2014; revised 21 October 2014; accepted 29 October 2014

Academic Editor: Wei Wang, Edith Cowan University, Australia

Abstract

Securing large amounts of electronic medical records stored in different forms and in many locations, while making availability to authorized users is considered as a great challenge. Maintaining protection and privacy of personal information is a strong motivation in the development of security policies. It is critical for health care organizations to access, analyze, and ensure security policies to meet the challenge and to develop the necessary policies to ensure the security of medical information. The problem, then, is how we can maintain the availability of the electronic medical records and at the same time maintain the privacy of patients' information. This paper will propose a novel architecture model for the Electronic Medical Record (EMR), in which useful statistical medical records will be available to the interested parties while maintaining the privacy of patients' information.

Keywords

Privacy, Electronic Medical Records, Electronic Health, Security

1. Introduction

The health care process has long been the target of many problems such as the illegibly doctor's written on paper, the difficulty by the doctors to access the patient information, time limitation, and personnel for monitoring patients [1].

How to cite this paper: Bensefia, A. and Zarrad, A. (2014) A Proposed Layered Architecture to Maintain Privacy Issues in Electronic Medical Records. *E-Health Telecommunication Systems and Networks*, **3**, 43-49.
http://dx.doi.org/10.4236/etsn.2014.34006

The health information systems come up during the last few years to overcome some of these problems, especially with the emergence of patients' individual Electronic Medical Records (EMR) and electronic health information (EHI). Implementation of EMR has been suggested to improve quality of productivity and care [2]. The main issues relevant to EMR are privacy concerns, source credibility, and physician-patient relationships [3]. Electronic Medical Records (EMR) include patient charts and other records that were mostly kept in physical format; these records exist before the introduction of the electronic records but are essential to maintain a certain level of care quality.

It is most likely that commercial companies might have a strong aspiration to access medical information, such as patients' information, patients' histories, as well as the procedures and treatments performed, which would motivate them to direct resources to lucrative health care areas and target patients who require the treatments and medications they market. This is a reasonable willingness, but it will affect patients' privacy. In addition to challenging society's privacy values, having fully access to medical information for malignant purposes may result in a possible threat to the society. Medical information is precious and its value continues to increase as the health care costs increase. Therefore, the pressure to review, acquire, study, or even steal information is increasing. With the increasing use of social networks and technology, it seems that it is a matter of time until medical information is being sold, just like shopping information and mailing lists. Once the information is exposed in the highly interconnected networked world, it is not easy to make it private again. Therefore, today, the big challenge is how to maintain integrity, security and availability of this information while dealing with medical commercials, patients, and the social pressures for information sharing versus privacy. The challenge begins with restricted rules, enforceable policies, procedures and guidelines, and is followed by technical system solutions that have data security issues [4].

According to Health Information Management Systems Society (HIMSS), The Electronic Medical Record (EMR) is "a longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting. This information includes patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports. The EMR automates and streamlines the clinician's workflow. The EMR has the ability to generate a complete record of a clinical patient encounter—as well as supporting other care-related activities directly or indirectly via interface—including evidence-based decision support, quality management, and outcomes reporting" [5].

Previously, each medical entity involved (hospital, pharmacy or lab) kept its own electronic health records; however, today an interconnected and integrated architecture can be developed in order to share such data across different systems [5] around the world. Every system can have its own data locally, but to share patients' information, a system has to communicate with another system to access its data storage. This, usually, requires some level of interoperability and integrity between the partner entities' systems.

EMRs have usually been claimed as a major breakthrough in the health care field for improving performance and effectiveness of health care services. The widespread use of EMRs would mitigate the concerns regarding patients' confidentiality and privacy. There are various risks that a patient's electronic record could be stolen, hacked into and altered without the proper authorization. For EMRs, many are concerned about the transmission of information and the possible intrusion by unauthorized third parties such as medical companies for marketing issue. Other main concerns relate less to health information security and more to the scope of EMR adoption [4].

There is a main concern about how to protect this wide amount of information and data from a wide range of sources while maintaining the integrity of the data and at the same time making the information available to a wide range of health care professionals, patients and staff workers. Since patients would demand the rights to their privacy, there are some strong motivations that will help secure our private medical information. But it requires a cautious surveillance of the technical, procedural and physical systems that must be in place.

There are various privacy issues that could be encountered by patients if their health information included in an EMR, such as privacy and integrity of health-related data and medical identity stealing [6]. In this work we proposed a layered architecture to serve third parties with the appropriate data while maintaining patient privacy. Three layers are presented in order to isolate low-level functions from high-level functions and offer flexibility and reliability to our proposed solution.

The remainder of the paper is organized into four main sections. In Section 2 we provide some literature review and a brief history about EMR. Section 3 describes the proposed solution. In Section 4 we conclude with discussion and future direction of the work.

2. Literature Review

The main privacy issues related to the EMR comes from the fact that the data have to be shared, when the aim is to protect these data [7]. This includes access to key fields such as diagnoses, organization of intricate information in structured database format, compact storage of multiple patient's data and diagnostics. However some patients balance their needs to protect their private data with their perceived benefits from EMR and may be assured as time elapses [8].

In terms of privacy patient preservation many works have been conducted [2] [9] [10]. In this section we present some of them. In [11] authors classified the privacy issues in Health systems in seven categories. This classification result from their experience and observations: consent, transparency, collection limitation, control over the record, data security, accuracy and identifiers. The authors suggested some solutions to protect the sensitive data in any health system. One of their solutions is to implement a secure SOA using web services. Indeed the web services are widely used nowadays in any Information System. The second proposal of the authors is to transmit any electronic health document via the different components of the system in XML format, which is already within the SOA.

In the paper presented by Hadzic *et al.* [12], the authors proposed an interesting architecture for an EMR system coupled with some ideas to secure that system. Regarding the architecture the idea was to model the whole Medical Record Information System (MRIS) in terms of ontologies. Indeed the medical record ontology is used to keep the personal information in a comprehensive format. The authors created 4 subontologies which model respectively: the personal information, the patient health condition, patient appointments and patient treatments. In terms of privacy preservation the authors made some recommendation such as limiting the access of the patient records to the authorized persons only, sure this is easily implemented since the system is organized around ontologies, so we they limited the view of the users according to the subontologies they are authorized to work in.

Another solution proposed in [13] to focus in the identities management of the users accessing a web health portal. The idea was to divide a user identity into a set of sub-identities I_i where each of them is represented by a pseudonym P_{Ii}. These identities can be assigned to any subset of the EMR user view. Indeed, these subsets don't need to be disjoint. Subject to the person, the medical data are presented to; the user is able to choose one of her sub-identities (e.g. a special prepared, non compromising one) and consequently opens the assigned subset of medical data. According to this idea the authorized EMR user can hide sensitive data in a special sub-identity in order to prevent disclosure attacks.

Among the health care existing laws such as HIPAA (Health Insurance Portability and Accountability Act) or PIPEDA (Personal Information Protection and Electronic Document Act) [14] proposed a system based on HIPAA privacy laws. This system has been build around a classification: classification of the health documents (Highly confidential, confidential, less confidential and public) and classification of people (Highly trusted, trusted, less trusted and not trusted). An access control matrix is than defined between the health documents and the system users. The intersection cell between a given user and a given document define a set of allowed operations: creation, modification, read and write.

Some works have been already considered in securing the electronic medical records in a cloud computing environment [15]. Indeed, the cloud computing environment can be very advantageous in terms of accessibility and storage in addition to the fact that can be very helpful to smaller hospital or clinics that have fewer resources with adequate EMR storage space. In [15] Chang et al assures that their system guarantee an EMR anonymity based on the patient number generated from the treatment serial number, a random number and an SID number embedded into a card owned by the patient only.

The outcomes of studying all these solutions is that the privacy issues can take different forms, therefore the proposed solutions differ from one system to another. However they converge all in the need to preserve the patient identity and grant the access only to the authorized persons. In the next section we will present our contribution in preserving the patient's data by spreading them among different storage space and by protecting the flow of exchange between the user and the data.

3. Problem Statement & Proposed Solution

The main target of health information security is to assure the integrity, availability, and confidentiality of the data.

The availability of patients' data, their conditions, procedures, and treatments will be beneficial to all of pub-

lic health organizations as well as organizations related to medical services. When linked properly, this data can be analyzed and be very useful. If complete medical histories are available to health care givers, they can potentially improve care procedures and offer enhanced care.

It is obvious that commercial entities have a strong desire to access medical information, such as procedures and treatments, along with patient histories, which would allow them to target patients who require the medications and treatments they market and direct resources to profitable health care areas. This is a reasonable desire for commercial medical companies; but on the other hand it will compromise patients' privacy.

As it is the case for different Information Technology (IT) projects, to solve any problem we have to consider three key factors: administrative decisions, physical equipment, and technological issues. In this section I will propose a three-tier model that will enhance the privacy of medical records while taking into account the necessity for medical information to be available as needed.

3.1. Administrative Decisions

There has been an extensive effort to enhance the privacy of medical records all over the world, but of course with variation for each country and cultural values.

The administrative decision are very important to make general guidelines for medical companies and IT software enterprises to follow and to be held accountable if they cross the line regarding the privacy of patient's and doctors' information. It is known that it's almost impossible to agree upon an administrative rules and regulations to follow, but there are international standards that we can utilize from, for example, The Health Insurance Portability and Accountability Act (HIPAA), one of the privacy rules in this act is "This act gives the right to privacy to individuals from age 12 through 18. The provider must have a signed disclosure from the affected before giving out any information on provided health care to anyone, including parents" [16].

So, the challenge in this part is to maintain availability, integrity, and security of this very critical information while dealing with the commercial and social pressures for privacy versus sharing of information. The challenge starts with applicable rules, guidelines, policies, and procedures and is followed by IT solutions that have the actual data security issues.

As mentioned above, these procedures are specific to each country, so it is hard to set a predefined and fixed rules in our model to be applicable everywhere. However, despite the diversities of cultures and countries, the keywords under these procedures are "access control" and "employee trainings and commitment":

- Access control: enforce the procedures that control who access the patients data or any other sensitive data, by using passwords, chip cards, hiding the screen one no one is in the front of the computer;
- Employee trainings and commitment: Once the procedures are selected, they need to be applied by the employees, so their commitment is very important. In fact, the employees should be aware of the importance to keep the patient records private and safe. An interesting study have been conducted in [17] on different risks scenario results due to the employees faults.

3.2. Physical Equipment

The physical equipment of the IT network could be very critical to the security of the overall IT system in any organization, it could include many guidelines

- Choosing secure hardware infrastructure, this ranges from choosing advanced routers and switches to adopting an intelligent framework such presented in [18];
- Servers and any critical hardware devices should be placed into a secure place with access only to privileged personnel;
- Limiting software installation and configuration to authorized users and IT Personnel.

Part of these duties can be done easily by the system administrator: for example, the choice of the hardware infrastructure, limiting the access to the users in installing some software or keeping the antivirus up to date. However, some other duties are the responsibility of the organization managers themselves such us: allowing an appropriate place or building to the servers or other machines, or investing in some extra severs (proxies) to protect and restrict the access to the patient data.

3.3. Technological Issues

The actual privacy and security issues regarding EMRs should all be handled using the IT skills by well-expe-

rienced and trained personnel. We will recommend the following guidelines to maintain privacy and security for EMRs while keeping medical information available as needed:

- Creating a specific database that will store patients' information without any hints about the patient's specific data, for example we can store the symptoms of a specific medical case, how many patients are having these symptoms, the kind of treatment they have, the type of prescription they have, and the result of treatment. This information could be very helpful for similar medical cases to take advantage of, for research purposes, society, and for commercial medical companies;
- Storing the statistical information in the aforementioned point in a separate electronic database system, so that if there is any system breaches, sensitive patients' information will not be exposed;
- The raw data with full details should be saved in a strict security conditions. Conditions access is important, only system administrators and high level management can edit and display the data.

In addition, we propose that the access to all these data, stored in separate databases, will be done by using a web services technique as proposed in [19]. Indeed, the web services allow an instant access for a specific data according to a predefined template, in the query and in the answer, so the requester cannot have an access to another unauthorized data. For example, if the requester is a doctor who wants to know the last medicines taken by his patient, he can get access only to this information and nothing else, and only if this service (accessing the last medicines taken by a patient) is provided by the system.

Moreover, in the past it has been proven that even if we use the web services technique, the hackers can emulate the client query to gather the information from the server, to resolve this issue we propose to create a proxy which will be in the front of the server, only this proxy can have the exact IP address of the server. Any client which needs to access some information from the server will send its query to the proxy first, which checks first if the IP of this client is already stored in it, if this is the case so the query will be routed to the server otherwise the query will be rejected immediately by the proxy (**Figure 1**).

Figure 2 shows brief description about the proposed three-layer model architecture to maintain EMRs privacy as well as maintaining the availability of EMRs medical information, each layer implementation is important to the other one so that the whole system will be integrated and well-organized.

4. Conclusions and Future Work

Electronic Medical Records (EMRs) have recently become a compelling and necessary paradigm for delivering and managing health information services.

The increasing improvements of information technology are affecting the EMRs, and eventually turning the promise of satisfying health information systems into a reality. However, although there are significant advantages offered by EMRs, the current technologies are not employed enough to realize its full potential while maintaining patients' privacy. There are many key constraints and challenges in this domain, including privacy and security of EMRs, which are still open and need more attention from the researcher's communities.

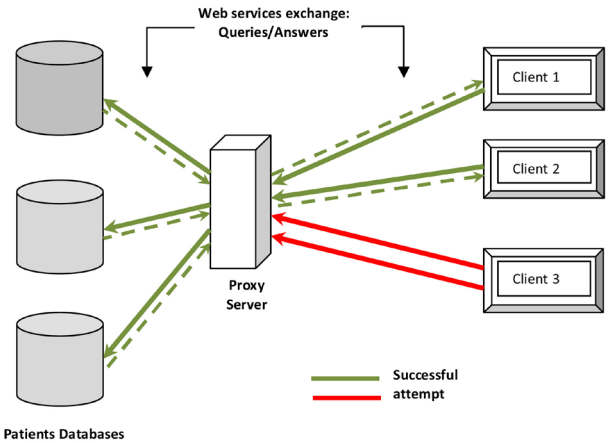

Figure 1. Successful web services queries to access the patients databases by registered clients in the proxy server and an unknow client (Client 3).

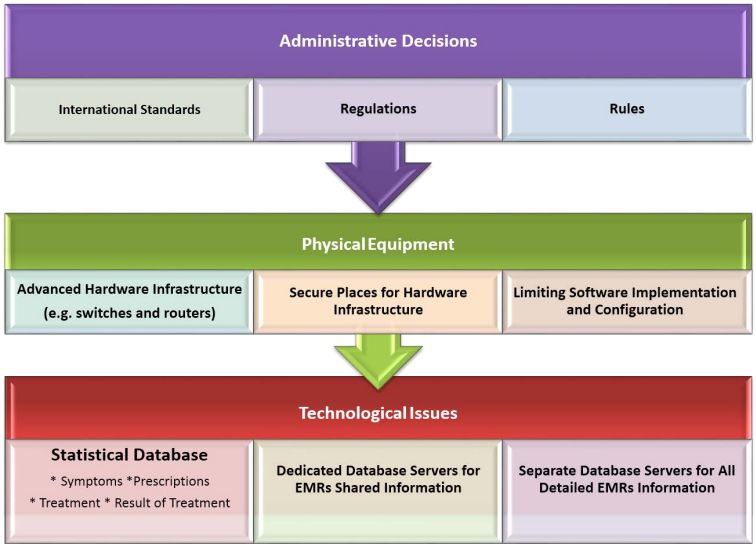

Figure 2. EMRs Privacy Layered Architecture.

In this paper, we proposed new EMRs Privacy Layered Architecture; the architecture provides three layers or components that are necessary to meet the challenge of data privacy and availability, especially when the amount of stored data is large. This architecture will keep the availability of useful medical information at the time that patients' and EMRs information are kept private and confidential.

The first layer focuses on regulations and rules to be followed by all parties involved in the EMR; the second layer focuses on hardware infrastructure as a physical media; the last layer separates sensitive private data from other medical information that can be shared with other entities.

We proposed also to use the web services technique to enable the exchange between any client of the EMR system and the servers. In order to make this exchange more secure we proposed to use a proxy server with a registered IP address of all the clients. Only those ones will have access to the EMR servers.

As a future work we propose to investigate the ways of securing the patients data by exploring some of the encryption methods. The encryption, for sure, has a great benefit in preserving the data privacy; however, its disadvantage is the slowness of the system performances. Investigating this area means proposing an appropriate method which balances encryption reliability and performance.

References

[1] Meingast, M., Rossta, T. and Sastry, S. (2006) Security and Privacy Issues with Health Care Information Technology. 28*th IEEE EMBS Annual International Conference*, **1**, 5453-5458.

[2] Middleton, B., Bloomrosen, M., Dente, M.A., Hashmat, B. *et al.* (2012) Enhancing Patient Safety and Quality of Care by Improving the Usability of Electronic Health Record Systems: Recommendations from AMIA. *Journal of the American Medical Informatics Association*, **1**, 1-7.

[3] Mukherjee, A. and McGinnis, J. (2007) E-Healthcare: An Analysis of Key Themes in Research. *International Journal of Pharmaceutical and Healthcare Marketing*, **1**, 349-363.

[4] Murtaza, M.B. (2012) Risk Management for Health Information Security and Privacy. *American Journal of Health Sciences*, **3**, 125-134.

[5] National Institutes of Health (NIH) (2006) Electronic Health Records Overview, National Center for Research Resources. National Institutes of Health, Bethesda.

[6] Clarke, I., Flaherty, T., Hollis, S. and Tomallo, M. (2009) Consumer Privacy Issues Associated with the Use of Electronic Health Records. *Academy of Health Care Management Journal*, **5**, 364-378.

[7] Ralston, J.D., Revere, D., Robins, L.S. and Goldberg, H.I. (2004) Patients' Experience with a Diabetes Support Programme Based on an Interactive Electronic Medical Record: Qualitative Study. *British Medical Journal*, **328**, 1159-1163. http://dx.doi.org/10.1136/bmj.328.7449.1159

[8] Pyper, C., Amery, J., Watson, M. and Crook, C. (2004) Patients' Experiences When Accessing Their On-Line Elec-

tronic Patient Records in Primary Care. *British Journal of Genetic Practice*, **54**, 38-43.

[9] Adams, T., Budden, M., Hoare, C. and Sanderson, H. (2004) Lessons from the Central Hampshire Electronic Health Record Pilot Project: Issues of Data Protection and Consent. *British Medical Journal*, **328**, 871-874. http://dx.doi.org/10.1136/bmj.328.7444.871

[10] Bolton Research Group (2000) Patients' Knowledge and Expectations of Confidentiality in Primary Health Care: A Quantitative Study. *British Journal of General Practice*, **50**, 901-902.

[11] Ray, P. and Wimalasiri, J. (2006) The Need for Technical Solutions for Maintaining the Privacy of HER. 28*th IEEE Engineering in Medicine and Biology Society*, **1**, 4686-4689.

[12] Hadzic, M., Dillon, T. and Chang, E. (2006) Use of Ontology Technology for Standardization of Medical Records and Dealing with Associated Privacy Issues. *IEEE* 2006, Mumbai, 15-17 December 2006, 2839-2845.

[13] Slamanig, D. and Stingel, C. (2008) Privacy Aspects of eHealth. 3*rd International Conference on Availability*, *Reliability and Security*, 1226-1233.

[14] Khadka, S. (2012) Privacy, Security and Storage Issues in Medical Data Management. 3*rd Asian Himalays International Conference on Internet*, 1-5.

[15] Le, Z., Chang, E., Huang, K. and Lai, F. (2011) A Secure Electronic Medical Record Sharing Mechanism in the Cloud Computing Platform. *IEEE* 15*th International Symposium on Consumer Electronics*, Singapore, 14-17 June 2011, 98-103.

[16] Pear, R. (2009) Clinton to Unveil Rules to Protect Medical Privacy. The New York Times, New York.

[17] Van Deursen, N., Buchanan, W. and Duff, A. (2013) Monitoring Information Security within Health Care. *Computers and Security*, **37**, 31-45. http://dx.doi.org/10.1016/j.cose.2013.04.005

[18] Gallo, R., Hawakami, H. and Dahab, R. (2013) FORTUNA—A Framework for the Design and Development of Hardware-Based Secure Systems. *Journal of Systems and Software*, **86**, 2063-2076. http://dx.doi.org/10.1016/j.jss.2013.03.059

[19] Ray, P. and Wimalasiri, J. (2006) The Need of Technical Solutions for Maintaining the Privacy of HER. 28*th IEEE EMBS Annual International Conference*, **1**, 4686-4689.

Scientific Research Publishing (SCIRP) is one of the largest Open Access journal publishers. It is currently publishing more than 200 open access, online, peer-reviewed journals covering a wide range of academic disciplines. SCIRP serves the worldwide academic communities and contributes to the progress and application of science with its publication.

Other selected journals from SCIRP are listed as below. Submit your manuscript to us via either submit@scirp.org or Online Submission Portal.