ONE WAY TO PATIENT EMPOWERMENT
The Proposal of an Authorization Model

Cátia Santos-Pereira[1,3], Luis Antunes[4,5], Ricardo Cruz-Correia[1,3] and Ana Ferreira[1,2,3]
[1]*Center for Research in Health Technologies and Information Systems – CINTESIS, Porto, Portugal*
[2]*Center for Informatics – CI, Porto, Portugal*
[3]*Faculty of Medicine, University of Porto, Porto, Portugal*
[4]*Institute of Telecommunications, University of Porto, Porto, Portugal*
[5]*Faculty of Science, University of Porto, Porto, Portugal*

Keywords: Patient Empowerment, Computer Security, Confidentiality, Electronic Health Records, Role Based Access Control.

Abstract: American and European Legislation for protection of medical data agree that the patient has the right to play a pivotal role in the decisions regarding the content and distribution of her/his medical records. The Role Based Access Control (RBAC) model is the most commonly used authorization model in healthcare. The first goal of this work is to review if existing models and standards provide for patients accessing their medical records and customizing access control rules, the second goal is to define and propose an authorization model based on RBAC to be used and customized by the patient. A literature review was performed and encompassed 22 articles and standards from which 12 were included for analysis. Results show that existing standards define guidelines for these issues but they are too generic to be directly applied to real healthcare settings. The proposed authorization model combines characteristics of RBAC, ISO/TS 13606-4, temporal constraints and break the glass. With this model we hope to start bridging the gap between legislation and what really happens in practice in terms of patients controlling and being actively involved in their healthcare. Future work includes the implementation and evaluation of the proposed model in a healthcare setting.

1 INTRODUCTION

A variety of new applications such as online social networks and online healthcare databases are very common nowadays and very often require the need for consumers to use and define access control. Within these applications personal and highly sensitive data can be stored. There are great benefits to be gained by making an individual's medical history available to healthcare providers and great risks to making it available to stalkers (Reeder, 2011).

Both American Legislation (Health Insurance Portability Accountability Act - HIPAA) and the European legislation (Recommendation No R (97) 5) for protection of medical data, agree that the subject of care (normally the patient) has the right to play a pivotal role in the decisions regarding the content and distribution of her/his medical records, as well as the right to be informed of its contents (U.S. Department of Health & Human Services, 1996), (Council of Europe, 1997), (Pereira et al., 2011).

Some studies regarding the access of Electronic Health Records (EHR) by the patient suggest modest improvements in doctor-patient communication adherence, patient empowerment and patient education. This process makes patients more careful in following medical recommendations. Although patients may find some parts of their EHR difficult to understand, patients who are offered a chance to review their EHR are mostly satisfied with the experience (Ross and Lin, 2003), (Honeyman et al., 2005), (Ferreira et al., 2007a). On the other hand healthcare providers also recognized the benefit of patient's ability to review and comment on their medical information prior to a visit (Siteman et al., 2006).

An authenticated user is authorized, within the system, to perform only certain actions that are associated to his or her functions e.g. to search through certain medical records of only patients

Santos-Pereira C., Antunes L., Cruz-Correia R. and Ferreira A..
ONE WAY TO PATIENT EMPOWERMENT - The Proposal of an Authorization Model.
DOI: 10.5220/0003787902490255
In *Proceedings of the International Conference on Health Informatics* (HEALTHINF-2012), pages 249-255
ISBN: 978-989-8425-88-1

under his or her care (Shortliffe and Cimino, 2006). The Role Based Access Control (RBAC) (Sandhu et al., 2000) model is the most commonly used access control model in healthcare (Beimel and Peleg, 2009), (Ferreira et al., 2007b) and has emerged as a promising alternative to traditional Discretionary Access Control (DAC) and Mandatory Access Control (MAC) models (Giuri, 1996), (Joshi et al., 2001), (Osborn et al., 2000). In large enterprise systems, the number of roles can be in the hundreds or thousands, and users can be in the tens or hundreds of thousands. Managing these roles, users, and their interrelationships is a formidable task that is often highly centralized in a small team of security administrators (Sejong and Ravi, 2002).

So, the first goal of this paper is to review if existing models and standards provide for patients' accessing their EHR and defining what healthcare professionals can access within their EHR. The second goal is to propose a patient authorization model based on RBAC to be used and customized by the patient.

2 PATIENT'S CUSTOMIZABLE ACCESS CONTROL MODELS: A SYSTEMATIC REVIEW

2.1 Methods

A literature review was performed in June 28, 2011 with searches in Pubmed, IEEE Xplore, ISI Web of Knowledge and International Organization for Standardization (ISO). The queries applied were:*"RBAC [All Fields] AND ("Health"[MeSH Terms] OR "Health"[All Fields]) AND Model [All Fields]"* in Pubmed; *"RBAC Health Model<in>metadata"* in IEEE Xplore; *"Topic (RBAC Health Model)"* in ISI Web of Knowledge and *"Health Access Control Model"* in ISO web site.

The results from these queries were filtered according to the following inclusion criteria: language of the article (English) and review of title and abstracts (adequate context).

The review was done in several stages. Initially, the repeated articles in the various databases were identified, they were then reviewed according to the inclusion criteria and finally read and analysed. For each article/standard, three relevant characteristics were analysed: (a) if they referred to EHR; (b) if they included within their access control policies the possibility for patients to also access their EHR and (c) if there was the capability for the patient himself/herself to customize that model and define his/her own access control rules, regarding their EHR. Cited articles/standards were also included. A total of 22 articles and standards were obtained from the search queries. After applied the inclusion criteria a total of 12 articles/standards were included in the final review.

2.2 Results

From the 12 articles and standards that were selected after the review, 10 presented RBAC extension models while 2 described access control standards and guidelines in healthcare.

The selected RBAC extensions were Motta and Furuie model (Motta and Furuie, 2003) and Patrick et al. model (Patrick, 2007) and the ISO standards selected were ISO/TS 22600-2 (ISO/TS 22600-2, 2006) and ISO/TS 13606-4 (ISO/TS 13606-4, 2009). The models by Motta and Furuie and by Patrick et al. together with the standards ISO/TS 22600-2 and ISO/TS 13606-4 include the patient in the set of roles that can access the EHR. However only the ISO/TS 13606-4 standard and the model by Motta and Furuie introduce also, in a generic way, the capability of the patients to customize access control rules to their EHR. We consider the ISO/TS 13606-4 the most complete work in terms of our research.

Beyond these models, the Generalized Temporal Role Based Access Control (GTRBAC) (Joshi et al., 2002) and the Break The Glass Role Based Access Control (BTG-RBAC) (Ferreira et al., 2009) although not complying with the goals of the systematic review, provide security mechanisms that could integrate the new extension of the RBAC model.

3 PROPOSAL OF A PATIENT'S AUTHORIZATION MODEL

After performing the systematic review several characteristics from various access control models and standards were studied in order to define the proposed patient authorization model. So, RBAC security features (Core RBAC, Hierarchical RBAC, Separation of Duties and Administration RBAC), temporal constraints described in GTRBAC and information sensivity definitions found in ISO 13606-4 will be included in the proposed model because they provide confidentiality and privacy to patient information and, on the other hand, break the glass mechanisms, described in BTG-RBAC,

provide for availability of information in emergency situations.

3.1 Model definition

3.1.1 The ISO/TS 13606-4

The ISO 13606-4 expresses the **record components** that an EHR may integrate such as: Personal Care; Privileged Care; Clinical Care; Clinical Management and Care Management. It also describes which **functional roles** (Subject of Care; Subject of Care Agent; Personal Healthcare Professional; Privilege Healthcare Professional; Healthcare Professional; Health-related Professional; Administrator) can access those record components.

3.1.2 NIST RBAC

The Role Based Access Control model integrates the Core RBAC, the Hierarchical RBAC, and Constrained RBAC, which includes Separation of Duties (SoD).

In the proposed model, the functional roles were organized into 3 main groups: subject of care (Group I), healthcare professionals (Group II) and administrative access (Group III), which include role inheritance (see Figure 1). Static Separation of Duties will integrate the proposed patient authorization model because the user will only be able to use one exclusive role per session in order to avoid conflicts between functional roles. The administrator of the roles and permissions of an EHR is associated with the patient of that EHR (Sejong and Ravi, 2002). The patient will actively manage the roles and permissions as well as give permissions of administration to other roles, if necessary.

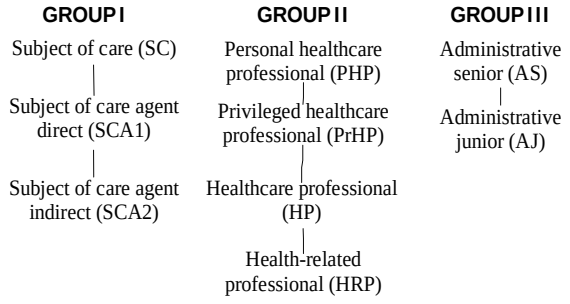

Figure 1: Hierarchical functional roles divided into three groups.

3.1.3 Break the Glass Access

Break the Glass (BTG) allows a user to override the access control rules stated by the access control manager and access what the user requests, even though he was not previously authorized to do it. When this is done, other BTG rules come into play which may monitor, record or report the user´s actions, thus making him responsible and oblige him to justify what he did.

3.1.4 Temporal Constraints

The Generalized Temporal Role Based Access Control (GTRBAC) model introduces a set of language constructs for the specification of temporal constraints on roles, including constraints permissions. These constraints are also included within the proposed patient authorization model in order to restrict access to Groups II and III in terms of temporal duration, for instance, during the healthcare professionals' shift.

3.2 Patient's Healthcare Network and Model Architecture

The concept of Patient's Healthcare Network (PHN) refers to all the healthcare institutions that the patient usually attends as well as health centers, referral hospitals, private hospitals, commercial laboratories and health insurers. It is important to define the institutions where the patient attends consultations and treatments because only the professionals that work in these institutions should usually have access to that patient's EHR. All professionals outside of the PHN are normally excluded from access to the EHR of the patient. However, the patient can define, within his/her model, a temporary role for healthcare professionals outside that PHN to access their EHR in a predefined period of time, preferably in their presence.

In some situations, when the patient integrates an institution inside the PHN the providers of that institution may wish to share information with other providers (e.g. to get a second opinion) who do not belong to the patient's PHN. In this situation, if the role provider has delegation permissions he could attribute temporary access to a user outside the PHN to obtain a second opinion. Figure 2 illustrates this case with an example. Jennifer is a patient that is being followed in Institution A (belongs to PHN), Jennifer has the role subject of care and manager senior in their own EHR. Dr. Jain is Jennifer's Gynecologist and has permissions to access Jennifer's EHR with the role Gynecologist. Dr. Chen is Jennifer's Neurologist and has the role

Neurologist. Besides having the permissions associated with the role Neurologist, Dr. Chen has user delegation permissions as well. He needs a second opinion for Jennifer's treatment, about a drug prescription. Dr. Chen contacts Dr. White for a second opinion but the later does not belong to Jennifer's PHN. Dr. Chen temporarily delegates permissions to access that patient's EHR to Dr. White. However the permissions delegated to Dr. White, have the particular characteristic that is to allow Dr. White access to that patient's anonimyzed medical information.

In this proposed model, for users to access the EHR and its components they need only to provide three pieces of information: a login (for identification); a password (for authentication); and a role (for authorisation). The first two are presented initially and only if authentication is successful will, a list of roles, that are associated to that user be available. The user can only select one role for each session. Each role has different permissions associated to different parts of EHR components, according to what the patient has previously defined within the model. Moreover, the model predicts also the utilization of a stronger authentication factor, with the use of smart-cards or tokens whenever needed.

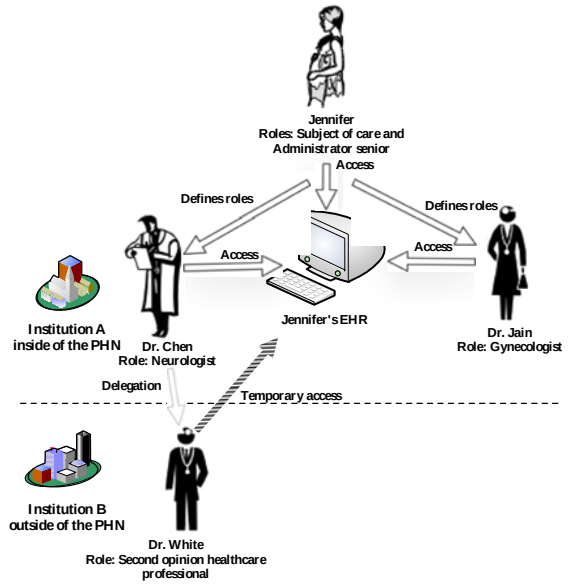

Figure 2: Example of a user delegation outside of the PHN performed by Dr. Chen to Dr. White.

The access permissions of a role to a specific record component is going to depend on the mapping that was previously made by the administrator senior (usually the patient). A specific role will have access to a record component if the administrator would have defined any of the Create, Read, Update and Delete (CRUD) operations or BTG to be part of his/her access permissions.

Figure 3 presents the architecture of the proposed authorisation model as the new relations of the proposed model from the RBAC model (Sandhu et al., 2000), that include (Ravi et al., 1999), (Ferreira et al., 2009) and (Joshi et al., 2002). The proposed model integrates both the specification of access and the definition by the patient of permissions to access his/her EHR. It puts the patient in the centre of these operations. Patient as an administrator senior can customize/manage the permissions of all the other roles.

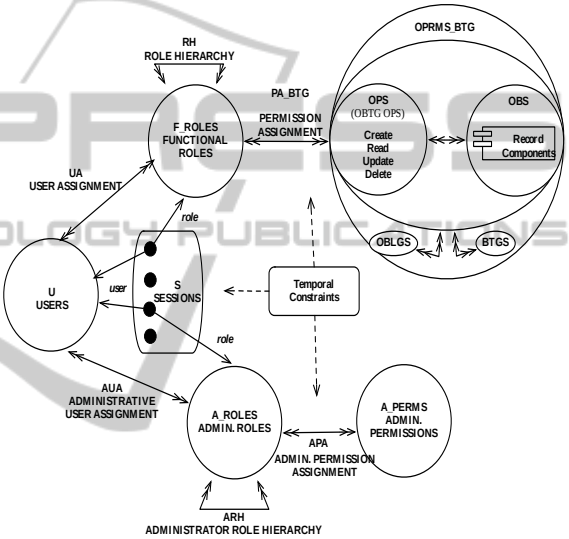

Figure 3: Architecture of the proposed patient authorization model based on (Ravi et al., 1999), (Sandhu et al., 2000), (Joshi et al., 2002), (Ferreira et al., 2009) and (ISO/TS 13606-4, 2009).

3.3 Proof of Concept

Two storyboards will be described next to better understand how the proposed model can work in real practice. Storyboard 1: "The patient corrects data in this EHR" and storyboard 2: "The patient has the need for medical care while travelling".

Storyboard 1: *John is 59 years old and resides in Porto, Portugal. He has recently moved to another house and needs do update his data on the EHR. He decides to access it by inserting his authentication credentials (login and password). He then chooses to update the demographic data record components.*

Figure 4 illustrates a use case that represents storyboard 1. When user John accesses his EHR, as

the functional role subject of care, he has permissions to perform all the operations (CRUD) in all the EHR record components.

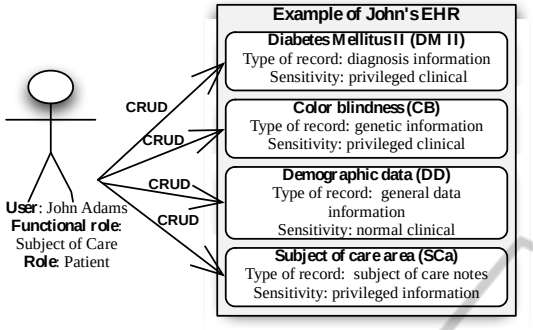

Figure 4: Use case 1 for storyboard 1.

Storyboard 2: *John is 59 years old and he resides in Porto, Portugal. During his holidays in the Algarve John feels sick with fever and cough. He goes to the hospital in Faro and the doctor that treats him has no access to John's EHR because he is not within his PHN. The patient has previously defined the role temporary privileged healthcare professional and accesses his EHR with this role. Since John will be the one to introduce the authentication credentials, he decides to use a two- factor authentication with a smartcard, to guarantee that his credentials are not breached. After a successful authentication John proceeds normally to choose the role available from a list of roles, in this case the role temporary privilege healthcare professional (TPrHP). Now the provider attending the patient has permissions to access the information that the patient defined for that role, for a specific period of time and therefore assists in his treatment.*

Figure 5 illustrates the use-case relating to storyboard. Since the provider did not have access to the patient's EHR, the patient can access the system by previously defining the role he wants to use for that session. In this use-case, the patient chose the role temporary privileged healthcare professional and gave temporary access to the provider that was treating him at that time. The provider can only access (read- only) components Diabetes Mellitus II and Penicilin Allergy of that EHR. The role TPrHP has not defined the permissions to perform BTG in any other component of the record so the healthcare professional does not even know of any other components' existence. As the proposed authorization model allows to define temporal constraints, since this is a temporary role, John associated a limited timeframe to be used (only 1hour).

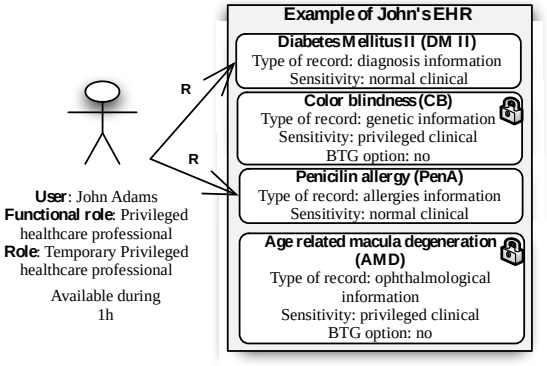

Figure 5: Use case 2 for storyboard 2.

4 DISCUSSION

In spite of generically allowing the patients to access or customize the access control rules of their medical records, the models and standards that were found in the review are too generic to be applied directly to specific healthcare scenarios. The analysed models and standards do not describe how the patient can customize his/her EHR in more specific scenarios. There is, therefore, a lack of research within this area, so we propose an access control model that can give the patients the needed empowerment.

Regarding the proposed model the first storyboard and use case presents a very common scenario where the patient wants to access his EHR in order to perform some operations within its record components. This scenario shows how easy it can be for the patient to access his EHR and perform all the necessary operations to keep it up to date. In this scenario one of the available record components is "subject of care area", so the patient has the possibility to insert and manage his personal notes. However this specific area will depend on the structure of the EHR, so, if the EHR does not include this feature could be integrated into other Personal Health Records platforms such as *Microsoft Health Vault* (Microsoft, 2011) and *myPHN* (American Health Information Management Association Foundation, 2011).

In the second use-case scenario with the use of the role temporary privileged healthcare professional, the provider does not belong to the PHN so he would have to blindly treat the patient as a newcomer, without any previous information. The proposed patient authorization model allows the healthcare professional to have a minimum information content that can help in a faster and

more successful patient treatment.

The proposed patient authorization model allows for a greater participation, responsibility and control over information security and contents of patient's EHR. This model is innovative as it allows the patient to define access control permissions within his PHN but also outside this network when necessary, providing a better healthcare treatment at the point of care. The functional roles subject of care agent direct and indirect can also be beneficial because they can allow patients' relatives to also take part and help in their treatment. Furthermore, these can help treating patients' relatives when, for example, they can have access to relevant genetic information about their parents or other relatives. Even if this information is not directly accessible, those functional roles could have the BTG permission to access it and the owner of the EHR would always be notified of the actions performed within his/her EHR. The flexibility of access and definition of access by the patient is not meant to invade or compromise healthcare professionals' workflows or privacy as there will be a restricted area (EHR component) only to be used and accessed by that healthcare professional. The temporal constraint with the separation of duties integrated within the authorization model allows to define the level of patients' privacy as fine-grained as the patient desires. To access a patient's EHR the user should belong to the patient's PHN, however a user can also access the patient's EHR if there are any delegated permissions (user delegation) defined for him or in emergency situations activating the mechanism BTG.

However, in order to use this model, the patient has to understand and use information technologies (IT) and have basic IT skills to define and use a platform that will integrate this new model. Problems with this model include the fact that users may mistrust what they are accessing as well as not being able to access all they think should be available to them. Also, the patient may not be capable of defining proper access control rules and unwantedly hide healthcare information that can be crucial to perform effective treatments. However, this can also happen no matter what type of record or access is made to the EHR. The patient can always omit relevant information for his/her treatment.

5 CONCLUSIONS

This paper constitutes the starting point to define a RBAC based patient authorization model that can be used in real practice. With this model we hope to bridge the gap that exists between legislation (with medical data protection definition) and what really happens in practice. With the growth of new technologies and the interest that patients have to be in control and take an active part in their treatment, the authors feel that the patients need to have a simple but focused model that allows them to easily define access permissions but also closely collaborate and interact with their healthcare professionals.

Future work includes the implementation and evaluation of the proposed authorization model with a specific case study in real healthcare practice.

ACKNOWLEDGEMENTS

This work is funded by FEDER funds (Programa Operacional Factores de Competitividade – COMPETE) and by National funds (FCT – Fundação para a Ciência e a Tecnologia) through project OFELIA – Open Federated Environments Leveraging Identity and Authorization [PTDC/EIA-EIA/104328/2008].

REFERENCES

American Health Information Management Association Foundation. 2011. *myPHR* [Online]. American Health Information Management Association. Available: http://www.myphr.com/ [Accessed October 2011].

Beimel, D. Peleg, M. 2009. The Context and the SitBAC Models for Privacy Preservation – An Experimental Comparison of Model Comprehension and Synthesis. IEEE Transactions on Knowledge and Data Engineering

Council of Europe 1997. Protection of Medical Data - Recommendation nºR (97) 5. *In:* committee of ministers to member states (ed.). Europe.

Ferreira, A., Chadwick, D., Zao, G., Farinha, P., Correia, R., Chilro, R. ,Antunes, L. 2009. How securely break into RBAC: the BTG-RBAC model. *Proceedings from 25th Annual Computer Security Applications Conference - ACSAC 2009*.

Ferreira, A., Correia, A., Silva, A., Corte, A., Pinto, A., Saavedra, A., Pereira, A. L., Pereira, A. F., Cruz-Correia, R., Antunes, L. F. 2007a. Why Facilitate Patient Access to Medical Records. *Medical and Care Compunetics 4*, 127, 77-90.

Ferreira, A., Cruz-Correia, R., Antunes, L. ,Chadwick, D. 2007b. Access Control: how can it improve patients' healthcare? . *Stud Health Technol Inform*, 127, 65-76.

Giuri, L. 1996. Role-based access control: a natural approach. *Proceedings of the first ACM Workshop on*

Role-based access control. Gaithersburg, Maryland, United States: ACM.

Honeyman, A., Cox, B. ,Fisher, B. 2005. Potential impacts of patient access to their electronic care records. *Informatics in primary care,* 13, 55-60.

ISO/TS 13606-4 2009. Health informatics - Electronic health record communication *In:* ISO/TS (ed.) *Part 4: Security.* Switzerland: ISO/TC.

ISO/TS 22600-2 2006. Health Informatics - Privilege management and access control *In:* ISO/TS (ed.) *Part 2: Formal Models.* Switzerland.

Joshi, J., Aref, W. G., Ghafoor, A., Spafford, E. H. 2001. Security models for web-based applications. *Commun. ACM,* 44, 38-44.

Joshi, J., Bertino, E., Ghafoor, A. 2002. Temporal hierarchies and inheritance semantics for GTRBAC. *Proceedings of the seventh ACM symposium on Access control models and technologies.* Monterey, California, USA: ACM.

Microsoft. 2011. *Microsoft Health Vault* [Online]. Available: http://www.microsoft.com/en-us/healthvault/ [Accessed October 2011].

Motta, G. H. M. B., Furuie, S. S. 2003. A contextual role-based access control authorization model for electronic patient record. *Ieee Transactions on Information Technology in Biomedicine,* 7, 202-207.

Osborn, S., Sandhu, R., Munawer, Q. 2000. Configuring role-based access control to enforce mandatory and discretionary access control policies. *ACM Trans. Inf. Syst. Secur.,* 3, 85-106.

Patrick, C. K., Hung and Yi Zheng 2007 Privacy Access Control Model for Aggregated e-Health Services. *Eleventh International IEEE EDOC Conference Workshop (EDOCW'07).*

Pereira, C., Oliveira, C., Vilaça, C., Ferreira, A. 2011. Protection of clinical data - Comparison of European with American Legislation and respective technological applicability. *HealthInf 2011 - International Conference on Health Informatics.* Rome.

Ravi, S., Venkata, B., Qamar, M. 1999. The ARBAC97 model for role-based administration of roles. *ACM Trans. Inf. Syst. Secur. 1094-9224,* 2, 105-135.

Reeder, R. W. 2011. Usable access control for all. *Proceedings of the 16th ACM symposium on Access control models and technologies.* Innsbruck, Austria: ACM.

Ross, S. E., Lin, C. T. 2003. The effects of promoting patient access to medical records: A review. *Journal of the American Medical Informatics Association,* 10, 129-138.

Sandhu, R., Ferraiolo, D., Kuhn, R. 2000. The NIST model for role-based access control: towards a unified standard. *Proceedings of the fifth ACM workshop on Role-based access control.* Berlin, Germany: ACM.

Sejong, O., Ravi, S. 2002. A model for role administration using organization structure. *Proceedings of the seventh ACM symposium on Access control models and technologies 1-58113-496-7.* Monterey, California, USA: ACM.

Shortliffe, E., Cimino, J. 2006. *Biomedical Informatics - Computer applications in Health Care and Biomedicine,* New York, Springer.

Siteman, E., Businger, A., Gandhi, T., Grant, R., Poon, E., Schnipper, J., Volk, L. A., Wald, J. S., Middleton, B. 2006. Clinicians recognize value of patient review of their electronic health record data. *AMIA ... Annual Symposium proceedings / AMIA Symposium. AMIA Symposium,* 1101.

U.S. Department of Health & Human Services 1996. Health Insurance Portability and Accountability Act *In:* Services, U. S. D. O. H. H. (ed.).