MEDINFO 2010
C. Safran et al. (Eds.)
IOS Press, 2010

doi:10.3233/978-1-60750-588-4-666

Access Control in Healthcare: the methodology from legislation to practice

Ana Ferreira[abc], Ricardo Correia[b], David Chadwick[a], Luis Antunes[d]

[a] *School of Computing, University of Kent, Canterbury, UK*
[b] *CINTESIS – Centre forResearch in Health Technologies and Information systems, Faculty of Medicine, Porto, Portugal*
[c] *Center of Informatics. Faculty of Medicine, Porto, Portugal.*
[d] *Institute of Telecommunications, Faculty of Science, Porto, Portugal*

Abstract

Translating legislation and regulations into access control systems in healthcare is, in practice, not a straightforward task. Excessive regulation can create barriers to appropriate patient treatment. The main objective of this paper is to present a new methodology that can define, from legislation to practice, an access control policy as well as a RBAC model, in order to comprise generic legislation and regulation issues together with the access control needs from the ends users of a healthcare information system. The methodology includes the use of document analysis as well as grounded theory and mixed methods research. This methodology can be easily applied within a healthcare practice or any other domain with similar requirements. It helps to bridge the gap between legislation and end users' needs, while integrating information security into the healthcare processes in a more meaningful way.

Keywords:
Computer security, Access control, Computerized patient medical records, Mixed methods, Grounded theory.

Introduction

Healthcare Information Systems (HIS) allow the collection, extraction, management and search of information and involve several people, processes and services within its environment, stressing therefore the need for information security [1, 2]. Both patient and healthcare organization concerned can be seriously damaged if no proper security is provided [3]. Access control constitutes the baseline for information security [4] and is one of the first interactions between humans and technology. In order to access information within a system there are usually 3 steps: identification – where a user says who he is (e.g. using a unique login or username); authentication where the user proves he is who he says he is (e.g. using a password or PIN number); and authorisation where access rights are given to the user. Authorisation can usually only occur after the first 2 steps are successful, and it checks if users meet all the requirements to exercise those rights and access the resources they requested. Access control is part of the authorisation process that checks if users may access resources they asked for. Current access control policies and models are usually not properly defined. Either they do not exist or do not integrate users' needs (i.e. healthcare professionals and patients), so when it comes to their usage, healthcare professionals can have many difficulties [5]. Also, recommendations and legislation are available in healthcare to protect sensitive medical information and to guarantee that this type of information is only accessed and used in specific and justified contexts [6-9]. These regulations tend to be generic and orient attitudes within the medical practice. However, to translate these orientations into practice is not straightforward. Many times this is not even possible. Research shows that excessive regulation can actually create a barrier that physicians have to surmount when treating patients [10]. The main objective of this paper is to present the development of a new methodology that can define, from legislation to practice, an access control policy as well as a RBAC (role-based access control) [11] model in order to comprise generic legislation and regulation issues together with the access control needs from the end users of a HIS. This methodology will try to bridge the gap between these two parties and help to reduce the barriers that are usually present in the integration and use of a HIS.

Background

One obstacle mentioned by healthcare professionals for the use and integration of EMR within healthcare is the lack of controls to provide for patient privacy [12]. Access control, which is one means of providing confidentiality, needs to be improved so that patient's privacy can be effectively protected. There are also other barriers that impede the effective integration of EMR within the healthcare practice. These barriers can be grouped in: time/cost, relational and educational [13, 14]. The relational barrier includes the perceptions that physicians and patients have about the use of the EMR and how their relationship may be affected by it. An example could be when the physician uses the computer during a consultation and the patient does not trust the information the physician is inputting and searching on the system because he usually does not know how that information can be used and what kind of protection is provided. The educational barrier comprises the lack of proficiency and difficulties that healthcare professionals have in interacting with the EMR in order to perform their daily tasks [15]. Healthcare professionals do not usually participate in the design and development of working tools (in this case the EMR) so they usually have to redes-

ign their practice workflow and processes, which is very challenging and consumes more time and costs [14]. Results from a systematic literature review on access control for both generic and the healthcare domain showed that although access control is a security service that has been widely studied and applied in healthcare systems such as EMR (Electronic Medical Record), the fact is that the most interested parties, the users (both healthcare professionals and patients), are not usually consulted when the access control policies are integrated into these systems, and when the system is integrated within their workflow environments. Healthcare professionals usually needed to change their workflow patterns and adapt their tasks and processes in order to use the systems [5]. This study [16] showed that EMR designers and implementers should monitor healthcare professionals' attitudes, opinions and experiences through the use of comprehensive evaluation methods such as focus groups and structured questionnaires in order to obtain substantial information to input into the design and implementation process. In this way the implemented systems are more likely to succeed. The use of both qualitative and quantitative methods (i.e. mixed methods) can elicit a wider range of information from the end users, thereby helping the designers and implementers to gain a deeper knowledge about the human needs from the EMR system. Further, the analysis of legislation and regulation documents that focus on defining the rules for access control can also be integrated within the same goal. The study and analysis of both generic and specific access control issues for the healthcare environment and the integration of these results within the healthcare access control policy should improve, not only the acceptance of EMR, but also the design of the access control component in order to reduce some of the educational and workflow problems that were found to be very common among the EMR systems in use. This type of research or methodology has not been published before and so the results cannot be compared to previous work.

Materials and Methods

Method Development

As there were not much research available on this subject the process started by analyzing published material on access control, both in generic and healthcare domains [5], as well as on the type of methodology to gather information that is not yet available. So in this case, literature reviews were performed in order to select the most appropriate methods for this purpose [16]. It was decided that there was the need to include both generic issues (legislation and regulations) as well as specific issues (end user needs – both healthcare professionals and patients).

1. For generic issues: a document analysis regarding legislation and regulations was performed to retrieve access control related issues;
2. For specific issues: grounded theory together with mixed methods was selected in order to collect data.
    a. After qualitative data collection, the analysis was performed according to Figure 1.
    b. Results from the qualitative analysis were used to develop the quantitative methods that were subsequently applied.
    c. The analysis of the quantitative data was done according to Phase 4 of Figure 1.
3. Generic assumptions were taken into account since there was not much information available aposteriori;
4. All analyzed data was then transformed into Access Control Rules;
5. Access control rules were standardized into IF THEN rules to comprise a generic Access Control Policy;
6. The generic Access Control Policy was transformed into a RBAC Policy;
7. A new extension of the RBAC model was developed in order to comprise the new RBAC Policy.

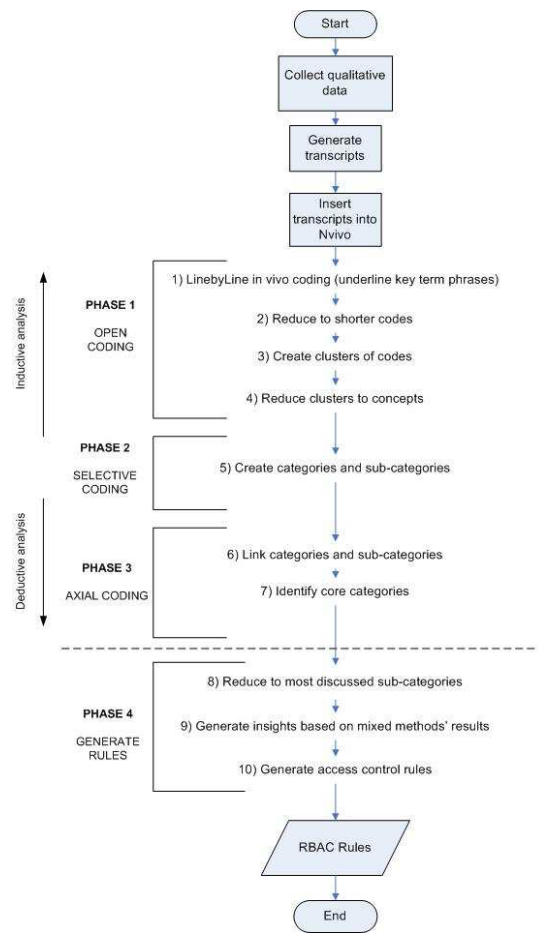

Figure 1 – Grounded Theory method used to analyze qualitatively focus groups' data.

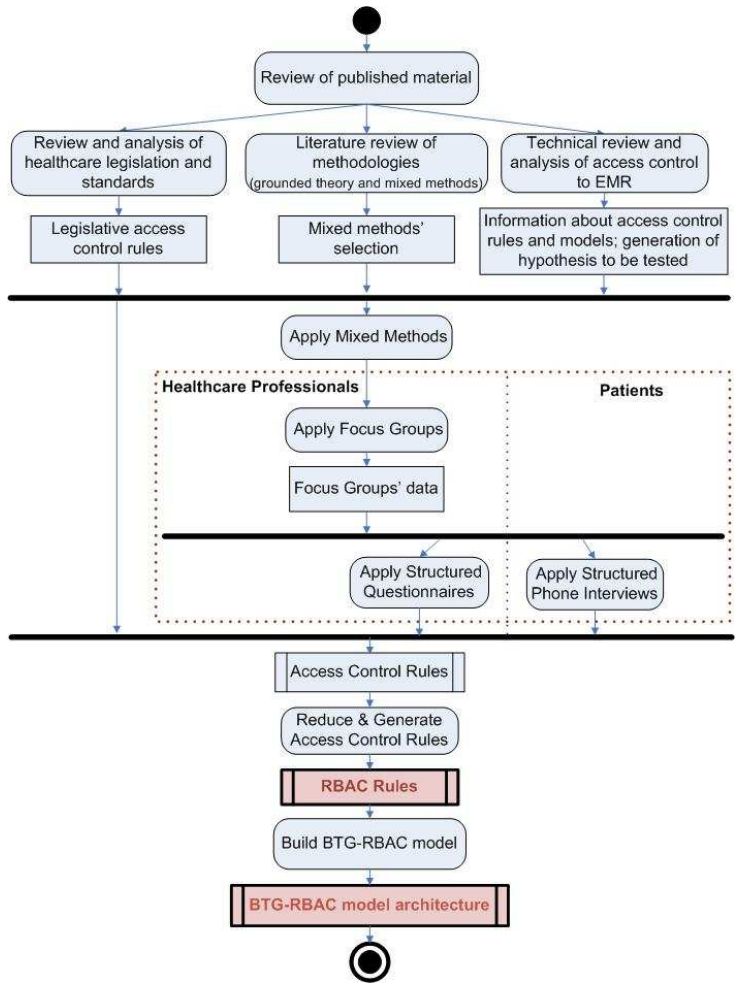

Figure 2 – Methodology description.

The method described in Figure 1 that is included within the bigger methodology presented in Figure 2 ("Reduce & Generate Access Control Rules") for the analysis of focus groups' data is the central part of this research. It describes how qualitative data was analysed and how the whole grounded theory process was done.

In more detail, the data generated from the qualitative research was collected and then transcribed and inserted within qualitative coding software (NVivo [17]). Phase 1 of this process included the line by line coding and grouping of codes of the whole transcripts; Phase 2 included a more focused or selective coding that allowed for the generation of categories and sub-categories from the codes in Phase 1; Phase 3 comprised the organization and ordering of the previous categories; and Phase 4 reduced the generated categories to the most discussed ones that were then included within the Access Control Rules' list.

Method Description

The methodology that was developed and can be used in a generic way by other researchers is described in Figure 2, with an activity diagram.

1. For generic issues: HIPAA [6], European Healthcare Recommendations [8,9] and the code of ethics for health information professionals were analysed; for specific issues, a technical review on access control was performed;
2. From the revised material assumptions were made for both healthcare professionals and patients regarding access control, these were used to confront with the results obtained;
3. A literature review of methodologies was performed. For grounded theory and mixed methods: focus groups (the main qualitative method) were applied first:
    a. Data was analysed according to Figure 1;

   b. Results from the most discussed categories were included into the subsequent quantitative methods;
   c. Structured questionnaires were applied to healthcare professionals;
   d. Structured phone interviews were applied to patients.
4. Access control rules were generated for both healthcare professionals and patients;
5. Each access control rule was separated into fundamental blocks of conditions and operations to be transformed into a RBAC rule, using the format as in [18];
6. A new access control model (the BTG-RBAC model) was developed in order to model the RBAC Policy generated from this method [19].

Results

In order to validate the presented methodology, a case study was performed. It used the BTG (Break the Glass) concept [19, 20] and instantiated every step of the method in Figure 2 as described below.

The first step of revise published material was previously performed and applied generically for every case study, and so it was used for this specific one.

1. **Document Analysis**: Portuguese Legislation - Law 12/2005;
2. **Generated Assumption**: There is the need for an override policy (e.g. Break The Glass);
3. **Mixed methods appliance and results** (Table 1):

Table 1- Description of the mixed methods applied.

Method	N	Data results
Focus groups	26 (4FG)	Access in emergency situations: requires different access(6 references);
Struct. questionnaire	27	A majority of respondents 74% (n=20) agreed with the existence of providing access in emergency situations depending on the situation and healthcare professionals
Struct. Phone interviews	200	YES: 191; NO: 3; no answer: 5; does not know: 1

4. **List of generated access control rules after applying the method in Figure 2**:

   A. Specific roles must be able to BTG and access (visualize only) information in emergency (or other unanticipated) situations
   B. It must be possible to define a fine-grained BTG (i.e. it may depend on roles as well as time and location restrictions)
   C. Logging and obligations must be provided at all times
   D. Access to genetic information must be managed and accessed only by medical doctors from the genetic specialty
   E. The number of healthcare professionals that are authorized to access information regarding DNA and biological products must be restricted in order to guarantee security as well as prevent losses, modification or destruction

5. **Access Control Policy based on RBAC-ACF [18]**:

Access control policies are often expressed through policy specification languages each of which may have different syntaxes. However, fundamental building blocks of any access control policy are: **subject, object, operation**, **condition**, **effect**, **obligation** and **purpose** [17].

A subject is a computer system entity that can initiate requests (e.g., user, agent, application process) to perform an operation or series of operations on objects. An object is a system entity on which an operation can be performed (e.g., a file, a table, a view). A condition describes the additional restrictions that must be evaluated in order to GRANT or DENY access to a particular subject for a particular data object. Effect is the outcome of evaluating a policy rule (e.g., GRANT or DENY). For these rules, the effect is always GRANT or allow because they are all described in the positive. Obligations are additional actions to be performed when the access control rule is triggered. The purpose has usually two objectives: business or data purpose.

The access control rules are defined as:

> Allow **[user/role/subject]** to perform **[operation]**
> on **[object]** provided **[condition]**
> Carry out **[obligation]**

The access control rule D was separated in two rules (D & E) in order to comprise both actions *access* and *manage*.

A. Allow **[specific users/roles]** to perform **[BTG (visualize only)]** on **[medical data]** provided **[emergency or unanticipated situations occur].** Carry out **[BTG obligations: logging, alert, email to responsible parties and proof of justification]**
B. Allow **[specific users/roles]** to perform **[definition of BTG operations with or without constraints]** on **[other users/roles]** provided **[they are authorized]**
C. Allow **[users]** to perform **[logging and obligations]** on **[medical data]** provided **[a BTG action is performed]**
D. Allow **[medical doctor(role)]** to perform **[access]** on **[genetic information]** provided **[medical doctor is from a genetic specialty]**
E. Allow **[medical doctor(role)]** to perform **[manage]** on **[genetic information]** provided **[medical doctor is from a genetic specialty]**
F. Allow **[users/roles/subjects]** to perform **[restrict access to a minimum required]** on **[DNA + biological products information]** provided **[they are authorized]**

6. The generated access control policy for BTG is comprised of 6 access control rules. Rules A to C can be modelled by the **BTG-RBAC model** [19], while rules D to F can be modelled by a generic RBAC model, and therefore, the BTG-RBAC model as well.

Discussion

This paper presents a new methodology that did not exist in the literature in order to ground security in the healthcare domain. It is a simple methodology to apply and integrate both generic and specific needs of the healthcare environment approaching this way legislation to the healthcare daily practice. This methodology can be applied not only in healthcare but also in similar domains with similar requirements in terms of security. It is flexible enough to be adapted according to the requirements of the system, both in terms of types of qualitative and quantitative methods chosen as well as the number of participants in each one of them.

Limitations of this work include the need for time and costs involved within the qualitative and quantitative methods setup, appliance and data analysis. Studies that do not involve end users of an information system may not benefit from this methodology.

In order to improve and refine the methodology presented in this study, it must be applied and tested with several other similar case studies and, if possible, in other domains besides healthcare.

Conclusion

The methodology presented in this paper can be used to generate, from legislation to practice, access control rules to be integrated within an access control policy for the healthcare practice. This methodology helps to bridge the gap between legislation and users' needs while integrating information security in a more meaningful way into the healthcare processes.

Acknowledgments

The research leading to these results has received funding from the (ISC)2 Organization and the Calouste Gulbenkian Portuguese Foundation.

References

[1] CERT Coordination Center CMU. CERT/CC Overview Incident and Vulnerability Trends. Carnegie Mellon University; 2003.

[2] Kurtz G, "EMR confidentiality and information security", Journal of Healthcare information management, 2003, 17(3): 41-48.

[3] Danley I, Smith S. "Privacy in clinical information systems in secondary care", BMJ – British Medical Journal, 1999, 318:1318-1331.

[4] Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems: Wiley; 2001.

[5] Ferreira A, Cruz-Correia R, Chadwick DW, Antunes L. Access Control: how can it improve patients' healthcare. Studies in Health Technology and Informatics. 2007;127:65-76.

[6] Medicine MSo. Health Insurance Porability and Accountability Act of 1996 (HIPAA). Privacy/Data protection project 2005. Available from: privay.med.miami.edu/glossary/xd_hipaa.htm.

[7] Databases ae. Health Insurance Portability and Accountability Act (HIPAA). Making information useful: Seaside Software Inc. DBA askSam systems; 2008.

[8] Membres CdMaÉ. Protection des Données Médicales. Recommendation n° R (97) 5; 1997.

[9] Ministers CoE-Co. On the impact of information technologies on health care – the patient and Internet Recommendation Rec (2004) 17; 2004.

[10] Ross-Lee B, Weiser M. Healthcare Regulation: Past, present and future. JAOA - Healthcare policy. 1994;94(1):74-84.

[11] Information Technology – Role Based Access Control. ANSI/INCITS 359-2004. International Committee for Information Technology Standards.

[12] Knitz M. HIPPA compliance and electronic medical records: are both possible? . Graduate research report: Bowie State University. Maryland in Europe; 2005.

[13] Sprague L. Electronic health records: How close? How far to go? NHPF Issue Brief. 2004 Sep 29(800):1-17.

[14] Miller RH, Sim I. Physicians' use of electronic medical records: barriers and solutions. Health Aff (Millwood). 2004 Mar-Apr;23(2):116-26.

[15] Becker MY, Sewell P. Cassandra: flexible trust management, applied to electronic health records. 2004; 2004. p. 139-54.

[16] Ferreira A, Correia R, Chadwick D, Antunes L. Improving the implementation of access control to electronic medical records. Proceedings of the IEEE International Carnahan Conference on Security Technology. 2008. 47-50.

[17] NVIVO 7. QSR International. Available at: http://www.qsrinternational.com/. Accessed on the 13th April 2009.

[18] Ferraiolo D, Kuhn D, Chandramouli R. Role-Based Access Control. 2nd ed. Norwood: Artech House; 2007.

[19] Ferreira A, Chadwick D, Farinha P, Cruz-Correia R, Zao G, chilro R, Antunes L. How to securely break into RBAC: the BTG-RBAC model. Proceedings of the 25th Annual Computer Security Applications Conference. 2009. 23-31.

[20] Ferreira A, Cruz-Correia R, Antunes L, Farinha P, Oliveira-Palhares E, Chadwick D W, Costa-Pereira A: How to break access control in a controlled manner? Proceedings of the 19th IEEE Symposium on Computer-Based Medical Systems. 2006; 847-851.

Address for correspondence

Ana Ferreira. Av. Fernão Magalhães, 978, 2D, 4350-154 Porto, Portugal.