MODELLING ACCESS CONTROL FOR HEALTHCARE INFORMATION SYSTEMS

How to control access through policies, human processes and legislation

Ana Ferreira[ab], David Chadwick[a]
[a]*Computing Laboratory, University of Kent, Canterbury, Kent, CT2 7NF, UK*
af84@kent.ac.uk, D.W. Chadwick@kent.ac.uk

Luís Antunes[b]
[b]*Computer Science Department, Faculty of Science, Porto, Portugal*
lfa@ncc.up.pt

Keywords: Access control; Electronic Medical Record.

Abstract: The widening use of Information Systems, which allow the collection, extraction, storage, management and search of information, is increasing the need for information security. After a user is successfully identified and authenticated to a system, he needs to be authorised to access the resources he/she requested. Access control is part of this last process that checks if a user can access those resources. This is particularly important in the healthcare environment where there is the need to control access to Electronic Medical Records (EMR). Although EMR can be an important support tool for the healthcare professional there are some barriers that prevent its successful integration. These barriers include the fact that healthcare professionals do not participate in the development of access control to access the EMR imposing them extra effort in its use. New access control policies to be implemented should focus on human processes and needs. The main objective of this project is to reduce EMR barriers by including healthcare professionals and patients in the definition and improvement of access control policies and models. If this can be achieved, we hypothesize that the EMR can be more successfully integrated into the healthcare practice and provide for better patient treatment.

1 INTRODUCTION

Information has become a powerful means of communicating, learning, wielding influence and making a profit. The widening use of Information Systems, which allow the collection, extraction, storage, management and search of information, is increasing the need for information security (Cert Coordination Center, 2003).

Information security is usually defined by three main characteristics: confidentiality as the prevention of unauthorized disclosure of information; integrity as the prevention of unauthorized modification of information; and availability as the prevention of unauthorized withholding of information or resources (Gollman, 1999, Harris, 2003).

In order to understand some other important concepts in information security, there is the need to distinguish privacy from confidentiality. Privacy relates to the right an individual has to protect his or her private information and confidentiality is one mechanism that can be used to protect that information from unauthorized access (Gollman, 1999). Legislation is another mechanism. This research work focuses on confidentiality, more specifically, on access control.

To access information within a system there are usually 3 steps required: identification – where a user says who he is (e.g. with a unique login or username); authentication where the user proves he is who he says he is (e.g. with a password or PIN number); and authorisation where access rights are given to the user. Authorisation can only occur after the first 2 steps are successful, and it checks if that user meets all the requirements to exercise those rights and access the resources he requested. Access control is part of the authorisation process that makes sure that a user may access the resources he asked for. Access control is one of the 5 security services defined in (Iso, 1989) and constitutes the baseline for information security (Anderson, 2001).

The complexity of information security systems make it very difficult to build a fully secure system (Schneier, 2004). This complexity is usually related to 3 competing factors: the technology itself; the difficulty of classifying information in terms of both organization and users' security requirements; and facilitating the ease of understanding and use of that technology by humans, the end users of the system who are usually non-technologically experts and one of the most problematic factor to consider (Schneier, 2004) when it comes to access control. These competing factors coupled with the fact that attackers are always finding new ways to exploit potential vulnerabilities in existing technology make it very difficult to build information security systems. Examples of competing factors are: protecting the privacy of information, whilst needing to be able to access it for audit or law enforcement purposes; making it easy for an authorised user to gain access to information but complex for an unauthorised attacker.

The means of providing access control have, therefore, become more challenging. Moreover with the rising of security incidents among organizations (Pricewaterhousecoopers, 2006) and the urge to provide for information confidentiality by controlling who or what is authorized to access it, the requirements have become more pressing

1.1 Healthcare Environment

A specific environment where access control is of vital importance is healthcare. Confidentiality is a main issue when it is related to patient clinical information that needs to be private. It is essential to protect that information from unauthorized access and, therefore, misuse. The introduction of the Electronic Medical Record (EMR) within healthcare organizations has the main goal of integrating heterogeneous information that is usually scattered over different locations (Waegemann, 2003, Cruz-Correia et al., 2005). This is why the EMR is becoming an essential source of information and an important support tool for the healthcare professional.

There is also an increasing need to access healthcare information at remote locations (Institute, 2005). This and the distributed nature of the information stress the need for access control requirements to be taken seriously (Bakker, 2004).

In healthcare organisations that require intra and inter-organizational interactions, authorisation and access control mechanisms cannot only be organized at a user level, but need also to be defined at other levels that can reflect those dynamic interactions. To do this, a series of structured and formal policies, models and roles must be defined (Blobel et al., 2006).

One obstacle mentioned by healthcare professionals for the use and integration of EMR within healthcare is patient privacy (Knitz, 2005). As stated above, in order to protect patients' privacy it is essential to at least provide for information confidentiality. Access control, which is one means of providing confidentiality, needs to be improved so that patients' privacy can be effectively protected.

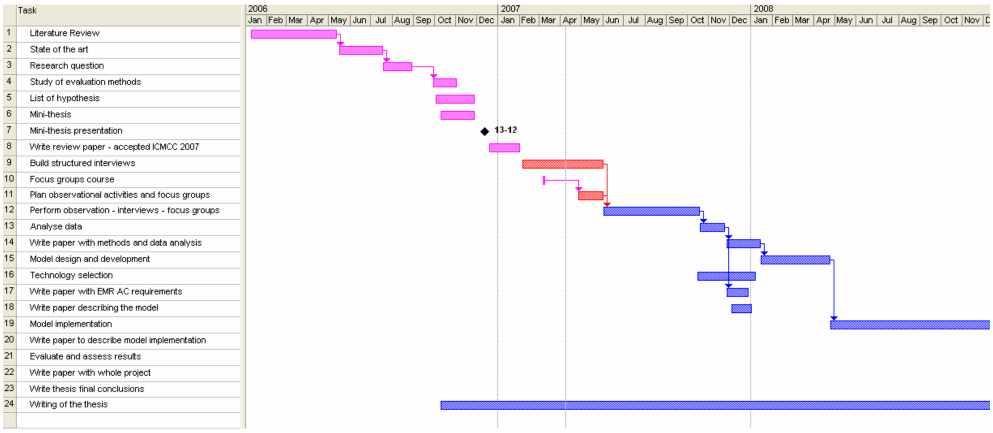
When asked, healthcare professionals say they think EMR have problems in terms of security due to its ease of distribution and wider online access (Miller et al., 2004). If they do not comprehend the technology or how the system can or cannot control access to information it will be more difficult for them to agree to use it, or to help improve its flaws and integrate the system within their daily work.

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 (Sprague, 2004, Miller and Sim, 2004).

Apart from the cost of EMR integration and the time healthcare professionals spend using the system in order to access and insert information there are other issues that relate more with human processes and their daily tasks. These are the relational and educational barriers explained below.

The relational barrier includes the perceptions that the physician and the patient 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 inserting and searching within the computer 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 (Becker and Sewell, 2004). Because healthcare professionals do not participate in the design and development of working tools (in this case the EMR), they usually



	Task
1	Literature Review
2	State of the art
3	Research question
4	Study of evaluation methods
5	List of hypothesis
6	Mini-thesis
7	Mini-thesis presentation
8	Write review paper - accepted ICMCC 2007
9	Build structured interviews
10	Focus groups course
11	Plan observational activities and focus groups
12	Perform observation - interviews - focus groups
13	Analyse data
14	Write paper with methods and data analysis
15	Model design and development
16	Technology selection
17	Write paper with EMR AC requirements
18	Write paper describing the model
19	Model implementation
20	Write paper to describe model implementation
21	Evaluate and assess results
22	Write paper with whole project
23	Write thesis final conclusions
24	Writing of the thesis

Figure 1 - List of activities for the research project

have to redesign their practice workflow and processes, which is very challenging and consumes more time and costs (Miller and Sim, 2004). In order to facilitate their daily workflow, since they access and use the EMR, the users must be involved in its design and development.

1.2 Activities

This research project started in July 2006 as a joint PhD supervision between the University of Kent in the United Kingdom and the University of Porto in Portugal. Until now a literature review and the state of the art within access control, both in a general way and within the healthcare environment, were performed.

Figure 1 shows the activities performed until now in pink. The activities in red are the ones being done at the moment, while the ones in blue are the ones that are programmed to be achieved in the future.

2 STATE OF THE ART

As stated in (Institute, 2005) the main factor that is driving the need for EMR systems to be implemented is the need to improve clinical processes or workflow efficiency. Also (Lehoux, 2006) refers that information technologies are used in healthcare to record, transmit and provide access to administrative and clinical information, so this should imply that access to and use of information respects confidentiality and brings efficiency and quality to healthcare. For now, the reality is that EMRs still do not integrate easily among healthcare professionals' daily workflow in order to be efficiently used (Miller and Sim, 2004).

The problems stated above relate mainly with human processes and workflow. If technology does not exist already, it should be implemented or adapted to the systems according to its main objectives and in order to fulfil professionals' needs instead of bringing more concerns. In healthcare it is very common to force the introduction of technology and expect healthcare professionals to use it (Lehoux, 2006). However, even if they want to use the systems, they usually have no time to learn how to use it and adapt to it according to their daily needs. Or if they do, it will consume their time and efforts possibly to the detriment of patient care.

Although there is usually an initial plan describing the rules to access an EMR, devised by engineers, promoters and implementers, its access in practice is often different from what was envisaged and decided at first (Kling, 1991, Lehoux et al., 1999). Users may have to reorganize their tasks and routines to accommodate the system; or they may even circumvent the rules that have been established for accessing the system (Lehoux et al., 1999, Akrich, 1994) because they were too cumbersome or time-consuming or both (e.g. by sliding in a personal ID card and keying in a password).

One sure thing is that health technology can deeply transform how humans live, work, strive, thrive and die (Brown and Webster, 2004). Patients, healthcare providers and health technologies are mutually reliant on one another and this interdependence regularly affects how healthcare is performed (Oudshoorn and Pinch, 2003).

Example (Littlejohns et al., 2003) shows very clearly the practical problems of implementing information systems within hospitals. According to this study's review the problems arise due mainly to not ensuring that the end users of the system knew why and how the system was being implemented. Further, the system did not take into account the complexity of healthcare tasks and therefore could not model them accordingly. An EMR should focus on helping and facilitating users to follow their daily processes without much effort and time. It should improve the working life of the health care professionals and bring benefits to them and their patients, rather than imposing costs on them, in terms of time and effort, with no perceivable benefits to either them or their patients. Therefore new security models and technologies to be implemented should focus on human processes and needs rather than on theoretical studies.

In order to ground these problems and to analyse what is commonly implemented and used in terms of access control, two reviews were performed. The first review focused in the development and implementation of generic access control policies, models and mechanisms whilst the second review focused on the same aspects but applied to healthcare.

2.1 Materials and Methods

Two reviews comprising published articles between 1996 and 2006 were performed. The first review included articles relating with generic access control policies, models and authentication mechanisms that incorporated an implicit access control function. Searches were made in IEEE Xplore and ACM (Association for Computing Machinery) conference databases as well as SACMAT (Symposium on Access Control Models and Technologies) and ESORICS (European Symposium on Research in Computer Security). Specific queries were made in IEEE Xplore (access control<in>metadata) and ACM with "access control".

The review method was done in several stages. We started by reading the titles and the abstracts from the list of articles retrieved by the queries. We tried to summarise in a table the most important topics about access control that we wanted to study. We included articles that described at least one of the following topics:

- **Type of access control policy**: Institutional, Legislation, End-user, override and other.
- **Type of access control model**: RBAC, IBAC and DAC, MAC, Hybrid and other.
- **Study and/or implementation**: Access control policy, access control model and Authentication Mechanisms with an implicit access control function.
- **Authentication mechanisms**: Login/password, Single Sign on, smartcard, fingerprint, digital signature, certificates and other.
- **Results**: Just build the model; prototype or real set implementation.
- **Problems**: The limitations.
- **Successes**: The advantages and benefits.

Articles that applied specifically to the healthcare domain were excluded from this review but included in the next one.

From the articles selected we tried to search the full articles and read them. The table was filled with the necessary information whilst the full articles were being read (Figure 3 in the Appendix).

The second review comprised full articles from the last 10 years (1996 until mid 2006) whose content covered access control policies, models and mechanisms applied in the healthcare environment. Searches were made in medical databases such as Medline as well as IEEE Xplore and ACM. As one query was not sensitive enough several queries were made in Medline - "computer security access", "access to information" and "security", "access to information" and "confidentiality"; IEEE Xplore - (access control and health<in>metadata), ("access control' and health"<in>metadata), (access control and health<in>metadata), (pki<in>metadata) and patient; and ACM - "access control" and "electronic patient record" and "security" and confidentiality".

The review method used was similar to the one presented in the previous section. We started by reading the titles and the abstracts from the list of articles retrieved by the queries. We tried to summarise in a table the most important topics about access control that we wanted to study. We included articles that described at least one of the following topics:

- **Type of access control policy**: Institutional, Legislation, End-user, override and other.
- **Type of access control model**: RBAC, IBAC and DAC, MAC, Hybrid and other.
- **Study and/or implementation**: Access control policy, access control model and Authentication Mechanisms with an implicit access control function.
- **Authentication mechanisms**: Login/password, single sign on, smartcard, fingerprint, digital signature, certificates and other.
- **Healthcare Institution**: Hospital, hospital department, primary care, private care and other.
- **Healthcare Information System**: EMR/EPR/CPR, prescription and consultation.
- **User Groups**: Medical doctors, nurses, patients and other healthcare professionals.

- **Portal/Internet access**: Healthcare professionals, patients and other.
- **Results**: Just build the model; prototype or real set implementation.
- **Problems**: The limitations.
- **Successes**: The advantages and benefits.

Next we tried to find the full version of the articles selected according to their titles and abstracts. The summary table was filled whilst the full articles were being read (Figure 4 in the Appendix).

2.2 Results

The generic review comprised 59 full articles published in the last 10 years (1996-2006). 351 articles were obtained within the search queries. After reading titles and abstracts 80 full articles were selected and read. Of these, 59 articles were deemed to be in scope and were included in the review. Table 1 and 2 show the results obtained for this review.

Table 1 - No of papers covering generic access control policies, models and authentication mechanisms.

Policy	1996-99	2000-03	2004-06	Total
Study/Analysis		4	12	**16**
Implementation			1	**1**
Model				
Study/Analysis	4	11	37	**52**
Implementation		2	6	**8**
Types of Models				
RBAC	4	15	19	**38**
IBAC (DAC)	1	4	3	**8**
MAC	1	4		**5**
Hybrid		1		**1**
Private/Own				
Other			1	**1**
Mechanisms				
Study/Analysis		5	10	**15**
Implementation		1	2	**3**
Types of Mechanisms				
Login/Password		1	1	**2**
Single Sign on				
Smartcard	1	2	1	**4**
Fingerprint				
Digital Signatures	1	2	4	**7**
Certificates	1	3	5	**9**

Table 2 - No of implemented systems.

Implementation	1996-99	2000-03	2004-06	Total
Protocol	3	17	26	**46**
Prototype		5	6	**11**
Real set - daily use		1		**1**
TOTAL	**3**	**23**	**32**	**58**

During the last ten years the 3 countries with more publications in this particular area are the USA with 40, UK with 8 and Germany with 7.

The healthcare review also comprised 59 full articles published between 1996 and 2006. 1007 articles were obtained from the Medline search queries, 234 from the IEEE queries, 446 from the BMJ and 200 from the ACM queries. These articles relating to access control in healthcare were reviewed according to their titles and abstracts. From these, 77 full articles were selected and read. Of these, 59 articles were deemed to be appropriate and were included in the review. Tables 3, 4 and 5 show the results for this review.

Table 3 – No of papers covering access control policies, models and mechanisms in healthcare.

Policy	1996-99	2000-03	2004-06	Total
Study/Analysis	2	8	12	**22**
Implementation		3	1	**4**
Types of Policies				
Institutional	1	2	4	**7**
Legislation		4	3	**7**
End user definition	1	2	1	**4**
Override	1	3	3	**7**
Other		4	5	**9**
Model				
Study/Analysis	6	10	8	**24**
Implementation	1	6	1	**8**
Types of Models				
RBAC	3	12	7	**22**
IBAC (DAC)		3		**3**
MAC			2	**2**
Hybrid				
Private/Own	4	3	6	**13**
Other	3	12	7	**22**
Mechanisms				
Study/Analysis	6	10	8	**24**
Implementation	1	6	1	**8**
Types of Mechanisms				
Login/Password	2	6	5	**13**
Single Sign on		5	3	**8**
Smartcard	2	10	8	**20**
Fingerprint		1		**1**
Digital Signatures	1	12	6	**19**
Certificates		16	11	**27**

Table 4 - Healthcare institutions, information systems and user groups.

Healthcare Institution	**1996-99**	**2000-03**	**2004-06**	**Total**
Hospital	3	10	7	**20**
Hospital Department		2		**2**
Primary Care		1	1	**2**
Private Care		1	3	**4**
Other		2	5	**7**
Information System				
EPR/EMR/CPR	5	14	15	**34**
Prescription		2	1	**3**
Consultation			1	**1**
Portal/Internet Access				
Healthcare professionals		1	1	**2**
Patients		1		**1**
User groups				
Medical doctors		2	2	**4**
Nurses		3	2	**5**
Patients		1	4	**5**
Others	2	13	9	**24**

Table 5 - No of implemented systems within healthcare.

Implementation	**1996-99**	**2000-03**	**2004-06**	**Total**
Prototype	2	14	9	25
Real set - daily use		1	1	2
TOTAL	**3**	**23**	**32**	**58**

During the last ten years the 3 countries with more publications in this particular area were the USA with 15, UK with 10 and Greece with 7.

The following section discusses in more detail the obtained results.

2.3 Discussion

The main observation from the two reviews was that the results were very similar and access control in healthcare reflects what is happening generally concerning access control in information systems. Both reviews showed that there is a great interest in defining and studying access control models. However, without a proper access control policy definition, a model cannot be properly implemented and configured, and will never accurately represent both the organization and users' needs in terms of access control. Still, this kind of academic modeling approach works because the vast majority of the models were not implemented in practice. They are analyzed as models or, at most, implemented as prototypes.

In 17 articles that mention the use of an access control policy only in 1 case was it implemented (Table 1). This shows that implementing policies is not trivial because adapting theoretical procedures to a real set environment may be impractical if these policies are not closely related with the workflow processes and humans involved. Although not many access control policies are implemented in practice, access control models are. How can a model be developed and implemented without having a policy stating the rules and procedures for access control? Most of the times, this is done within the model and not defined separately, which can complicate the whole process. The fact that 46 of the 58 studies are just protocol and model definitions, 11 were implemented as prototypes and only 1 was actually implemented (Andreas et al., 2001) in a real set environment confirms the complexity of applying the models into a real scenario (Table 2). Nevertheless, a vast majority (38 in 52 articles) include the use of the Role Based Access Control (RBAC) model (David et al., 2001) in order to develop their access control systems. The preference for using RBAC as the starting point to build an access control model can be explained by the fact that this model allows easier administration and more flexibility in order to be adapted to the workflow and hierarchical needs of a heterogeneous organization. In terms of access control authentication mechanisms, the most studied were digital signatures and public key certificates in a Public Key Infrastructure (PKI). These mechanisms are extremely complex and usually require expensive resources, both in terms of manpower expertise and software, and this can explain the difficulty in implementing and using them in real healthcare scenarios within hospitals and to access EMR. At the time the articles under review were written (mostly prior to 2004) PKI systems had not been widely implemented and used in real and complex healthcare scenarios such as public hospitals and other large organizations where resources are usually scarce. After 2004 we could find only one study where PKI was implemented in a real healthcare scenario, but not within an EMR (Lemaire et al., 2006).

Similar results were obtained from the review of access control policies, models and mechanisms in healthcare. From the 34 articles that mention the use of an access control policy, only 4 implemented that same policy as a prototype (Table 3). Also, in 4 of those 34 articles it is mentioned within the access control policy how the end-user can set policies for his daily work when they use the system. None of these 4 policies were implemented, not even as prototypes. Further, none of the 34 articles that mention access control policies included the end-users of the system as part of the group that designed and developed those policies. 14 out of 34 of these policies are defined following legislation and institutional requirements. This is also necessary in order to reflect generic needs but it is also required to model more specific needs such as workflow processes, end-user needs and also cultural issues in defining access control policies to be used by the healthcare professionals, and possibly patients. Finally, 7 articles refer to the need for an override policy definition i.e. an access control system which allows the user to override the current policy in times of emergency, and gain access to patient confidential information that they would not otherwise be able to see (Ferreira et al., 2006).

Furthermore, we realized that most healthcare information systems that need access control are EMR systems (34 in 38 articles) built within heterogeneous and complex organizations such as hospitals (20 in 35 articles) (Table 4). EMR is becoming more available because its advantages are well acknowledged (Institute, 2005). However, according to the review, access controls in EMR are usually not implemented and used in real life environments. From those which are implemented within a real set the end users of the system do not participate in its development and, most of the time do not support its introduction and use (Institute, 2005).

It is also relevant to refer that none of the access control systems used within the EMR and in a real environment were being accessed by the patients. According to the European legislation (Membres, 1997) patients should be able to access their medical information whenever they request and in an understandable format. Several studies refer as well the importance and even some benefits that patients can have when accessing their medical records (Ross and Lin, 2003, Honeyman et al., 2005). It can improve patients' adherence to treatment and the efficiency of the service (Mandl et al., 2001).

According to (Ferreira et al., 2007)there are some benefits in patients accessing their medical records and new technologies such as EMR should help improving and supporting this access. However, only one of the studies analyzed provided the access by patients to their information via an internet portal. Again, both healthcare professionals and patients did not intervene in the development of this access control system; a system that focused on patients' access to medical information with the objective to provide for their needs and subsequent healthcare support. Patients should be able to define who can or cannot access their sensitive clinical information.

As an example, this study (Pinho et al., 2006) applied a survey in order to find out doctors' opinions regarding access control to EMR within a university hospital. Most respondents agree that access control levels must exist for EMR and that not all doctors must have total access to all patient records. They indicate that more sensitive information (e.g. HIV) must only be accessed by doctors that treat those patients. A great number of doctors also reveal that patients should not have total access to their own medical records. This must be further analysed as patients should have the right to access all their medical information, if they require. It is surprising that doctors think they can access all the information about a patient they are treating and, at the same time, feel the patients themselves cannot have the same right regarding their own information. This can be one important issue to analyse when trying to define access control systems closer to end users' needs.

In conclusion, the design and implementation of access control systems in EMR should become closer to the needs of the real environment where it is used and, therefore, applied in real scenarios with real users, and not only as prototypes systems. If the issues presented are not taken into account, there is usually great difficulty in creating a migration plan from paper records to the electronic system, and the inability to find adequate EMR access control solutions that meet healthcare professionals and patients' needs.

3 RESEARCH PROBLEM

The previous section shows that access control could be a key factor in order to improve access and use of EMR. Typically there is a big focus on the definition of access control models and how they can be implemented, but most of these are without a proper access control policy definition. However, only a few of these systems are in full production with real end users. Most of them are just prototypes that are implemented so that the model can be tested.

Healthcare professionals and patients are not usually taken into consideration when these systems are implemented or even at the time when they are designed. Their needs and opinions are not usually taken into account and so some of the EMR barriers mentioned before are difficult to overcome.

According to what was described above, technology should be useful, effective, easy to understand and use and most of all fulfil users' needs and goals. Technology should serve people and not the other way around. This is also true with information security technology. A balance between the fact that information needs to be protected and at the same time useful must be found. These two components are crucial in order to perform accurate and effective healthcare. A successful EMR needs to have appropriate access control mechanisms in place whilst allowing for its users to take most advantage of the information it stores.

The previous sections reviewed some of the main problems that EMR systems have that hinder their successful integration within healthcare practice. These are very important problems that may affect the quality and efficacy of healthcare treatment. To focus on one of the first interactions between users of a system and the system itself, which includes access control, may be one solution and a key enabler in order to lessen some of the EMR barriers. This is an area in which work needs to be done.

The research question/problem to be tackled is the following: how can the educational and other barriers to the effective use of EMR systems be reduced? The collaboration of healthcare professionals and patients in the development of access control systems for EMR may very well be one solution, which will help to facilitate access to the information, improve healthcare workflow and processes and lessen the time and costs. This hypothesis will be tested in this research project.

4 OBJECTIVES

The main objective of this project is to reduce EMR barriers by focusing on improving access control policies, models and mechanisms' definition and usage.

Secondary objectives closely related with the main objective include:

- finding generic methods to integrate, as well as evaluate the collaboration of end users (e.g. healthcare professionals, patients) of a EMR in the definition of access control policies, models and mechanisms
- building an access control model that can represent that integration in a generic and systematic way
- testing and evaluating the model in a real environment

5 FUTURE WORK

In order to start tackling the research question, some evaluation methods are going to be selected. As is expected, those methods should relate to the end users of the EMR (where attitudes, opinions and concerns about access control to information systems are going to be assessed) as well as the system itself (in terms of design and usability). Further, as with similar projects, this evaluation must start with the realization and understanding of the following: the purposes for creating a product; the people who would use the product; what tasks they would use it to do; and where and how they would use it (Hackos and Redish, 1998). Developers should understand users, their tasks, workflow and environment. A system interface is the bridge between both the world of technology and the world of the user, the means by which the user interact with the system (Hackos and Redish, 1998). What can be more important than making sure people use the system in their natural physical, social and cultural environment?

For example in (Brostoff et al., 2005) usability and design methods were used to evaluate a specific software tool. Questionnaires were also applied to achieve a more generic feeling for the tool. According to their results, this evaluation and interface redesign improved its efficiency, making the tool easier to use and understand. Another example is briefly described in (Hackos and Redish, 1998) where programmers designing a medical records system completely changed their initial software interface after they visited the site. They discovered that the workflow among departments and individuals proceeded in a different manner to what they had imagined.

The methods to be used for this project will be for the purpose of evaluating users' attitudes, opinions and behaviours related with access control in the healthcare environment. These will be applied in 3 steps: 1) structured interviews applied to the healthcare professionals and patients; 2) focus groups to analyse specific issues and get in touch to what people think and feel about the problem; 3) observation of professionals within their working environment.

After the collection and analysis of all the data it will be possible to build an access control model that will be closer to end users' needs and therefore more transparent and easier to use.

6 EXPECTED OUTCOMES

At this state of the research the expected outcomes are:

- To show that all the stakeholders within healthcare can and must participate in the process of building and improving access control systems
- A new access control model that can be applied successfully not only in healthcare but also in other domains where confidentiality is a crucial requirement
- *In a short-term*: improve and ease the process of access control in the EMR
- *In a long-term*: improve healthcare treatment in terms of efficiency, time and costs – by reducing some of the EMR barriers

REFERENCES

Akrich, M., 1994. Comment sortir de la dichotomie technique/société : Presentation des diverses sociologies de la technique. De la préhistoire aux missiles balistiques : De líntelligence sociale des techniques. *La Découverte. Latour & Lemonnier*, 105-131.

Anderson, R., 2001. *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley.

Andreas, S., Jonathan, M.,Jeremy, J., 2001. The role-based access control system of a European bank: a case study and discussion. *Proceedings of the sixth ACM symposium on Access control models and technologies.* Chantilly, Virginia, United States, ACM Press.

Bakker, A., 2004. Access to EHR and access control at a moment in the past: a discussion of the need and an exploration of the consequences. *Int J Med Inform,* 73**,** 267-70.

Becker, M. Y.,Sewell, P., 2004. Cassandra: flexible trust management, applied to electronic health records.

Blobel, B., Nordberg, R., Davis, J. M.,Pharow, P., 2006. Modelling privilege management and access control. *Int J Med Inform,* 75**,** 597-623.

Brostoff, S., Sasse, M. A., Chadwick, D., Cunningham, J., Mbanaso, U.,Otenko, S., 2005. "R-What?" Development of a Role-Based Access Control (RBAC) Policy-Writing Tool for e-Scientists. *Software - Practice and Experience,* 38**,** 835-856.

Brown, N.,Webster, A., 2004. *New medical technologies and society: reordering life*, Cambridge Polity Press.

CERT Coordination Center, C. M. U., 2003. CERT/CC Overview Incident and Vulnerability Trends. Carnegie Mellon University.

Cruz-Correia, R., Vieira-Marques, P., Costa, P., Ferreira, A., Oliveira-Palhares, E., Araújo, F.,Costa-Pereira, A., 2005. Integration of Hospital data using Agent Technologies – a case study. *AICommunications special issue of ECAI,* 18**,** 191-200.

David, F. F., Ravi, S., Serban, G., Kuhn, D. R.,Ramaswamy, C., 2001. Proposed NIST standard for role-based access control. *ACM Trans. Inf. Syst. Secur.,* 4**,** 224-274.

Ferreira, A., Correia, A., Silva, A., Corte, A., Pinto, A., Saavedra, A., Pereira, A., Pereira, A., Cruz-Correia, R.,Antunes, L., 2007. Why facilitate patient access to medical records. *Studies in Health Technology and Informatics*.

Ferreira, A., Cruz-Correia, R., Antunes, L., Farinha, P., Oliveira-Palhares, E., Chadwick, D. W.,Costa-Pereira, A., 2006. How to Break Access Control in a Controlled Manner. *CBMS2006.* Salt Lake City, USA.

Gollman, D., 1999. *Computer Security*, John Wiley & Sons.

Hackos, J.,Redish, J., 1998. *User and Task Analysis for Interface Design* Wiley.

Harris, S., 2003. *CISSP All-in-One Exam Guide*, McGraw-Hill Osborne Media.

Honeyman, A., Cox, B.,Fisher, B., 2005. Potential impacts of patient access to their electronic care records. *Inform Prim Care,* 13**,** 55-60.

Institute, M. R., 2005. 7th annual survey of electronic health record trends and usage for 2005. Medical Records Institute. 2005. Medical Records Institute, Medical Records Institute.

ISO, 1989. ISO 7498-2 - Information processing systems, Open Systems Interconnection, Basic Reference Model, Part 2: Security Architecture. ISO - International Organization for Standardization.

Kling, R., 1991. Computerization and social transformations. Science, technology and human values. *Science, Technology and Human Values,* 16**,** 342-267.

Knitz, M., 2005. HIPPA compliance and electronic medical records: are both possible? . Bowie State University. Maryland in Europe.

Lehoux, P., 2006. *The Problem of Health Technology: Policy Implications for Modern Health Care*, Routledge.

Lehoux, P., Sicotte, C.,Denis, J., 1999. Assessment of a computerized medical record system: disclosing its scripts of use. *Evaluation and Program Planning,* 22**,** 439-453.

Lemaire, E. D., Deforge, D., Marshall, S.,Curran, D., 2006. A secure web-based approach for accessing transitional health information for people with traumatic brain injury. *Comput Methods Programs Biomed,* 81**,** 213-9.

Littlejohns, P., Wyatt, J.,Garvican, L., 2003. Evaluating computerised health information systems: hard lessons still to be learnt. *BMJ,* 326**,** 860-863.

Mandl, K. D., Szolovits, P.,Kohane, I. S., 2001. Public standards and patients' control: how to keep electronic medical records accessible but private. *Bmj,* 322**,** 283-7.

Membres, C. d. M. a. É., 1997. Protection des Données Médicales. *Recommendation n° R (97) 5.*

Miller, R. H., Hillman, J. M.,Given, R. S., 2004. Physician use of IT: results from the Deloitte Research Survey. *J Healthc Inf Manag,* 18**,** 72-80.

Miller, R. H.,Sim, I., 2004. Physicians' use of electronic medical records: barriers and solutions. *Health Aff (Millwood),* 23**,** 116-26.

Oudshoorn, N.,Pinch, T., 2003. *How users matter: The co-construction of users and technologies*, The MIT Press.

Pinho, C., Sá, C., Mendes, E., Santos, E., Silva, F., Sousa, F., Gomes, F., Abreu, F., Mota, F., Aguiar, F., Faria, F., Macedo, F.,Martins, S., 2006. Electronic Patient Records - who should access what? Doctors' view. Biostatistics and Medical Informatics Department - Faculty of Medicine of Porto.

PriceWaterHouseCoopers, 2006. Information Security Breaches Survey. Department of Trade and Industry.

Ross, S. E.,Lin, C. T., 2003. The effects of promoting patient access to medical records: a review. *J Am Med Inform Assoc,* 10**,** 129-38.

Schneier, B., 2004. *Secrets and Lies: digital security in a networked world*, Wiley.

Sprague, L., 2004. Electronic health records: How close? How far to go? *NHPF Issue Brief***,** 1-17.

Waegemann, C., 2003. EHR vs. CPR vs. EMR. *Healthcare Informatics online*.

APPENDIX

This appendix contains the flowcharts with the process used to make the reviews described within this paper.

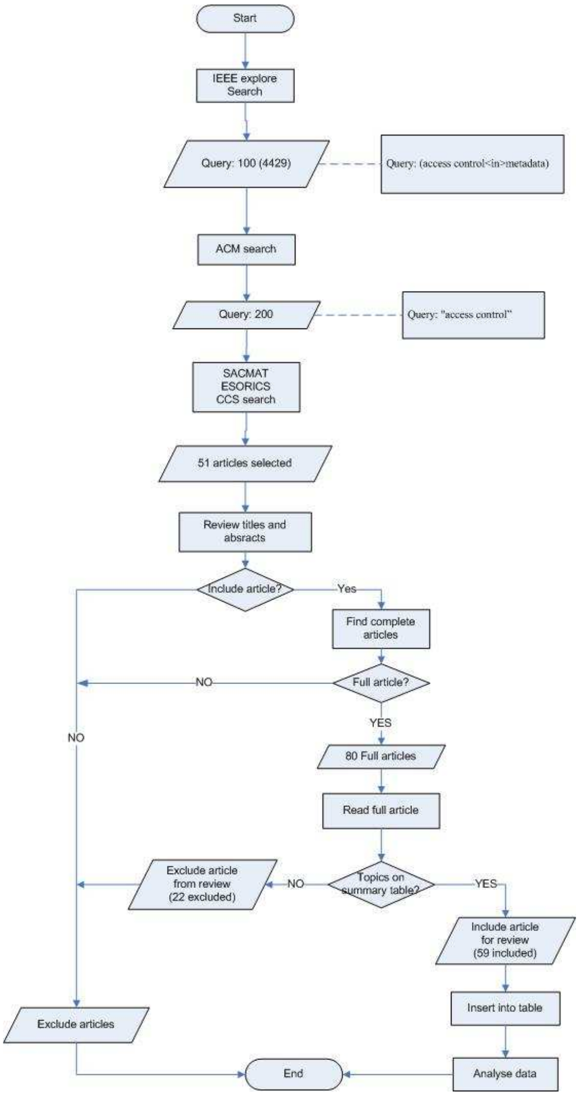


Figure 2 - Flowchart representing the review process for generic access control

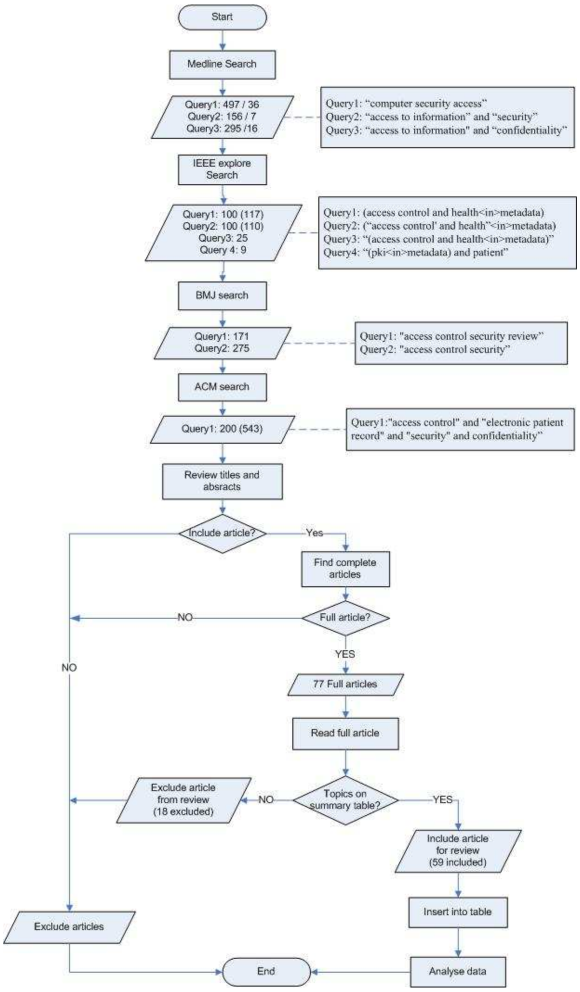

Start
Medline Search
Query1: 497 / 36
Query2: 156 / 7
Query3: 295 /16
Query1: “computer security access”
Query2: “access to information” and “security”
Query3: “access to information" and “confidentiality”
IEEE explore Search
Query1: 100 (117)
Query2: 100 (110)
Query3: 25
Query 4: 9
Query1: (access control and health<in>metadata)
Query2: (“access control' and health”<in>metadata)
Query3: “(access control and health<in>metadata)”
Query4: “(pki<in>metadata) and patient”
BMJ search
Query1: 171
Query2: 275
Query1: "access control security review”
Query2: "access control security”
ACM search
Query1: 200 (543)
Query1:"access control" and "electronic patient record" and "security" and confidentiality”
Review titles and absracts
Include article?
Yes
Find complete articles
Full article?
NO
YES
NO
77 Full articles
Read full article
Topics on summary table?
NO
YES
Exclude article from review (18 excluded)
Include article for review (59 included)
Insert into table
Exclude articles
End
Analyse data

Figure 3 - Flowchart representing the review process for healthcare access control.