Modelling Access Control for Healthcare Information Systems

How to control access through policies, human processes and legislation

Ana Margarida Ferreira

PhD in Computer Science

Joint Supervision

&

October 2010

To my parents and brothers for all their support.

To Rui for being an inexhaustible source of patience and tenderness.

CONTENTS

Acronyms

ABAC	Attribute Based Access Control
ACF	Access Control Framework
ACM	Association for Computing Machinery
ADF	Access control Decision Function
AEF	Access control Enforcement Function
ANSI	American National Standards Institute
ATM	Automated Teller Machine
BTG	Break-The-Glass
BMJ	British Medical Journal
CCADIG	Corpo Clínico de Acesso aos Dados de Informação Genética
CDISC	Clinical Data Interchange Standards Consortium
CEN	Comité Européen de Normalisation
CNPD	Comissão Nacional de Protecção de Dados
CPR	Computer Patient Record
CRep	Clinical Repository module for the VEPR
DAC	Discretionary Access Control
DB	Database
DNA	DeoxyriboNucleic Acid
EDI	Electronic Data Interchange
EHR	Electronic Health Record
EMR	Electronic Medical Record
EPR	Electronic Patient Record
ESORICS	European Symposium on Research in Computer Security
FG	Focus Group
GP	General Practitioner
GT	Grounded Theory
HCP	Healthcare Professional
HHS	Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HL7	Health Level Seven
HSJ	Hospital S. João

HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
IEEE	Institute of Electric and Electronics Engineers
IHTSDO	International Health Terminology Standards Development Organization
INCITS	International Committee for Information Technology Standards
IS	Information System
ISO	International Standards Organization
IT	Information Technology
JSP	Java Server Pages
MAC	Mandatory Access Control
MAID	Multi-Agent system for Integration of Data
MeSH	Medical Subject Heading terms
MySQL	My Structured Query Language
NHS	National Health Service
NIST	National Institute of Standards and Technology
SAAM	Shibboleth Apache Authorisation Module
SACMAT	Symposium on Access Control Models and Technologies
PDP	Policy Decision Point
PERMIS	PrivilEge and Role Management Infrastructure Standards
PHP	Recursive initialism for “PHP: Hypertext Preprocessor”
PMAC	Privilege Management and Access Control standard
RBAC	Role Based Access Control
SBIM	Serviço de Bioestatística e Informática Médica
TAS3	Trusted Architecture for Securely Shared Services
TBAC	Task Based Access Control
VEPR	Virtual Electronic Patient Record
VIZ	Visualization module of the VEPR
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

List of Tables

List of Figures

Acknowledgements

First and foremost I would like to thank Prof. Altamiro da Costa Pereira for introducing me to the art of research right from the beginning of my career, and for always being supportive of my ambitions and believing in my potential. Without his leadership, teaching, friendship and patience, this work would have never been possible.

To my supervisor, Prof. David Chadwick, I would like to acknowledge his constant support and profound knowledge in the area of information security, and for always pushing me forward, no matter what.

To my supervisor, Prof. Luís Filipe Antunes, I would like to acknowledge his constant support in all the matters needed to produce this work, especially in the fact that he always believed in my scientific merits to achieve the goals of this research.

To my friend, colleague and co-author, Prof. Ricardo Correia, who has followed my research journey almost from the beginning and has always had an effective word of advice and knowledge that makes me take the next step forward.

To my colleagues, Mestre Cristina Santos and Mestre Luís Azevedo, who have helped me in the quantitative studies' definition, data analysis and statistics.

To my colleague, Patrícia Alves, who have helped me with her experience to perform, in a very professional and swift way, the structured telephone interviews.

To my friend, Erick Lopes, who being a PhD student in the same department as me, has shared all my fears and achievements, and has helped me in a very important time of this research work, the implementation of the Break-The-Glass (BTG) prototype.

To my friend Gift, I would like to thank the fact that he took the surmounting job of reading, correcting and suggesting better ways of writing this thesis.

To the Information Systems Security Group, University of Kent, I would like to acknowledge their support.

To the Centre of Informatics, from the faculty of Medicine of Porto, I would like to thank their support, especially in the person of Mestre Pedro Marques, who has taken up more work than he should.

To the $(ISC)^2$ - International Information Systems Security Certification Consortium Organization - and the Portuguese Calouste Gulbenkian Foundation, I would like to acknowledge their indispensable financial support.

Context

After finishing a Masters' degree in Information Security at Royal Holloway, University of London - UK in 2002, a CISSP certification and a brief training at HP Labs in Bristol - UK in 2003 and 2004, respectively, the author started working as an IT specialist at the Centre of Informatics at the Faculty of Medicine, University of Porto in 2004. Her research skills and know-how were then ready to be tested in a practical domain. This opportunity came when a new project to implement an Electronic Medical Record (EMR) in a university hospital was defined and taken up by the department of Biostatistics and Medical Informatics (SBIM) at the Faculty of Medicine, University of Porto. The project was named Hospital S. João Information System XXI (*Sistema de Informação Hospital S. João – XXI)* and was funded by the Health Operational Program – Health XXI (*Programa Operacional Saúde – Saúde XXI)* in 2002. It included the implementation of a middleware layer (*SI.HSJ-XXI/IAI, Integração de Aplicações Informáticas*) to integrate federated databases and a web-based presentation layer (*Sub-projecto SI.HSJ-XXI/ICU, Informação Clínica do Utente*) to allow health professionals to access the patient data retrieved by the middleware layer. This project challenged the author's knowledge of information security and allowed to evolve and apply it in practice in a very hectic environment where security is essential but many times disregarded as something secondary. Moreover, this experience allowed the author to realize how important and influential the end users of a system are in the integration and usage success of any information system. The author focused therefore on further researching and improving one of the first interactions between the end users of a system and its features: the definition and implementation of access control features in healthcare information systems.

She complements this research work by disseminating the obtained results and knowledge with regular lectures and seminars about information security and with the participation in several research projects in the healthcare area, including a National Government project to implement a centralized National EMR (*RSE.pt*).

Furthermore, the work described in this thesis is a testimony of the importance of researching EMR security and access control in particular, in the healthcare domain and practice, with the main goal of improving healthcare workflow and processes. This is also proved by the fact that two students from the Master course in Medical Informatics at SBIM are using parts of this thesis' results to follow and produce their own research. These students are: Carla Pereira (a healthcare professional) who is studying "Evaluation of the usability of a TeleRadiology system at the ACES Nordeste", and using the mixed methods research in order to pursue her research goals; and Pedro Farinha (an IT researcher) who is studying "Access control and management in healthcare information systems" in order to improve the access control platform that is being used in the EMR described above.

Abstract

The introduction of Electronic Medical Records (EMR) within healthcare organizations has the main goal of integrating heterogeneous patient information that is usually scattered over different locations. However, there are some barriers that impede the effective integration of EMR within the healthcare practice (e.g., educational, time/costs, security). A focus in improving access control definition and implementation is fundamental to define proper system workflow and access.

The main objectives of this research are: to involve end users in the definition of access control rules; to determine which access control rules are important to those users; to define an access control model that can model these rules; and to implement and evaluate this model.

Technical, methodological and legislative reviews were conducted on access control both in general and the healthcare domain. Grounded theory was used together with mixed methods to gather users' experiences and needs regarding access control. Focus groups (main qualitative method) followed by structured questionnaires (secondary quantitative method) were applied to the healthcare professionals whilst structured telephone interviews were applied to the patients.

A list of access control rules together with the new Break-The-Glass (BTG) RBAC model were developed. A prototype together with a pilot case study was implemented in order to test and evaluate the new model. A research process was developed during this work that allows translating access control procedures in healthcare, from legislation to practice, in a systematic and objective way.

With access controls closer to the healthcare practice, educational, time/costs and security barriers of EMR integration can be minimized. This is achieved by: reducing the time needed to learn, use and alter the system; allowing unanticipated or emergency situations to be tackled in a controlled manner (BTG) and reducing unauthorized and non-justified accesses. All this helps to achieve a faster and safer patient treatment.

1 INTRODUCTION AND MOTIVATION

Information has become a powerful means of communicating, learning, wielding influence and making a profit. The widening use of Information Systems (ISs), which allow the collection, extraction, management and searching of information, is increasing the need for information security [1]. 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 [2, 3]. In order to understand some other important concepts in information security, there is the need to distinguish between privacy and confidentiality. Privacy relates to the right an individual has to protect his/her personal information from disclosure to others and confidentiality relates to the provision of services and mechanisms that can be used to protect information from unauthorized access [2]. This research work focuses on confidentiality, more specifically, on access control as a means of providing confidentiality.

In order to access information within a system there are usually 3 steps: identification – where a user identifies himself/herself (e.g., using a unique login or username); authentication where the user proves he/she is who he/she says he/she is (e.g., using a password or PIN number); and authorisation where access rights are given to the user. Authorisation usually only occurs after the first 2 steps are successful, and it checks if the users meet all the requirements to be given rights to access the resources they need. Access control is part of the authorisation process that checks if users may access resources they asked for. Access control is one of the 5 security services defined in the International Standards Organization (ISO) 7498-2 standard for Security Architecture [4] and constitutes the baseline for information security [5].

The complexity of information security systems make it very difficult to build a fully secure system [6]. This complexity is usually linked to 3 inter-related 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. Humans, the end users of most systems, are usually not technological experts and are one of the most problematic factors to consider [6] when it comes to access control. These 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 secure ISs. Examples of competing objectives 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 one.

The means of providing access control have, therefore, become very challenging. Moreover, with the rising level of security incidents in organizations [7] and the increasing demand to provide for information confidentiality by controlling who or what is authorized to access information, the security requirements have become more pressing.

1.1 Background

A specific environment where access control is highly significant is healthcare. Confidentiality is a main security issue when it comes to patient clinical information. It is imperative to protect patient information from unauthorized access and misuse. The introduction of Electronic Medical Record (EMR) systems within healthcare organizations has the main goal of integrating heterogeneous patient information that is usually scattered over different locations [8, 9]. This is why the EMR is becoming an essential source of information and an important support tool for the healthcare professional (HCP). There is also an increasing need to access healthcare information at remote locations [10]. This and the distributed nature of the information stress the need for access control requirements to be taken seriously [11].

In healthcare organizations 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 these dynamic interactions. This can be achieved by defining a series of structured and formal policies, models and roles [12].

1.1.1 Access control policies, models and mechanisms

This section briefly introduces the concepts of access control policies, models and mechanisms.

Security policies provide the foundation for an organization's security infrastructure. They comprise documents with a set of rules and procedures that describe the management's intention in relation to security. A security policy identifies the critical resources, activities and operations as well as subjects that play an active role in providing for the security of an organization [3]. An access control policy defines, more explicitly, what the access rights between subjects and resources are, depending on the sensitivity and security required for those resources. Generic steps to define an access control policy are described in Table 1.1, which is extracted from the information security standard ISO/IEC 27002 [13], Section 11, on Information Access Control Management.

Table 1.1 – Example of a high level access control policy and procedures [13].

Objectives	Solutions
1. Control access to information	Develop a policy to control access to information
2. Manage user access rights	Establish a user access control procedure Control the management of system privileges Establish a process to manage passwords Review user access rights and privileges
3. Encourage good access practices	Expect users to protect their passwords Expect users to protect their equipment Establish a clear-desk and clear-screen policy
4. Control access to your networked services	Formulate a policy on the use of networks Authenticate remote user connections Use automatic equipment identification methods Control access to diagnostic and configuration ports Use segregation methods to protect your networks Restrict connection to shared networks Establish network routing controls
5. Control access to your operating systems	Establish secure log-on procedures Identify and authenticate all users Establish a password management system Control the use of all system utilities Use session time-outs to protect information Restrict connection times in high-risk areas
6. Control access to applications and information	Restrict access by users and support personnel Isolate sensitive application systems
7. Protect mobile and teleworking facilities	Protect mobile computing and communications Protect and control teleworking activities

Access control models describe frameworks that dictate how subjects (e.g., users) access resources. Traditional access control models are categorized as:

- Discretionary Access Control (DAC) [14];
- Mandatory Access Control (MAC) [14].

Models like Role-Based Access Control (RBAC) [3] [15] [16] [17], Task-Based Access Control (TBAC) [15] and Attribute-Based Access Control (ABAC) [18] have been proposed later than the traditional models mentioned above in order to address security requirements of a wider range of applications such as web and distributed applications [19].

In the DAC model the owner of the data is the one who says what subjects can access his/her resources. The access control is based on the discretion of the owner. He/she can grant or revoke access permissions to other subjects in regard to his/her resources without the intercession of a system administrator. This is one of the most widely used access control models for web applications and is quite flexible. However, it does not provide high security or high assurance because it can allow access to copies of information to a user who does not have access to the original data.

In the MAC model access control is based on the classification of security labels that are associated with the resources. The classification label specifies the clearance level a user must have to be able to access the resource. Usually the rules for how subjects access data are made by management, configured by the system administrator, enforced by the operating system and supported by security technologies. The information flow is controlled to ensure confidentiality and integrity of information, which is not addressed by DAC. MAC provides a high level of security and assurance and is therefore usually used to support Department of Defence requirements and regulations pertaining to unauthorized access to classified information. However, MAC provides no flexibility and is difficult to enforce, especially in web based applications. This model often requires the use of several other models (e.g., DAC).

In the RBAC model a set of controls can be defined centrally in order to determine how subjects and resources interact. This type of model allows access to resources based on the role the user holds within the organization. These characteristics can support organization specific security policies (i.e., is policy neutral) and can also express access control models such as DAC and other user specific models. It can also express MAC. RBAC is a flexible and easy to administer model. It needs a special administrator role to manage all other roles, so it supports model hierarchy. It also addresses key web applications security requirements such as separation of duties and least privilege.

Another access control model is the one that is based on the content of the information or the nature of the tasks or transactions that happen in the application. These are Access Control Tasks/Workflows models and can be static or dynamic in nature and can use RBAC to achieve their goals (TBAC is one example of this type of model). These models can integrate temporal or inter-task constraints and are usually successful in modelling access control for transaction intensive applications such as e-commerce, medical applications and so on.

In the ABAC model, authorization is based on the attributes that are defined regarding a subject (i.e., identity, role, age), a resource (i.e., location, size, value) or the environment (i.e., date, time, system state). ABAC bases the authorization decisions on the attributes of the

related entities. Subject attributes may be established by digitally signed credentials through which credential issuers assert their judgements about the attributes of the subject. These credentials can be used to introduce and authenticate strangers without online contract with attribute authorities [18]. Similar to RBAC, ABAC is simple to manage but does not need to have a centralized management nor is it based on a single dimension of roles such is RBAC. ABAC is a good access control model for distributed domains where the subjects and the resources belong to different security domains. It can handle MAC better than RBAC. It is a flexible and dynamic model.

Each model uses different types of methods to control how subjects access resources. These methods depend on the business and security goals of the organization. The models can be used exclusively or combined so that they can achieve the necessary security level required by the environment.
Table 1.2 summarizes and compares the main features of the introduced access control models. Table contents are based on [19].

Table 1.2 – Comparison of the features for the most common access control models.
(The cells marked with an * represent lack of research for that feature).

	DAC	MAC	RBAC	TBAC	ABAC
Authorization paradigm	Ownership	Administration	Role	Task	Attribute
Type of administration	Hard	Medium	Easy	Easy	Easy
Flexibility	High	Low	High	High	High
Good for distributed environments	Yes	No	Yes	Yes	Yes
Widely used	Yes	No	Yes	*	*
Handles dynamic changes	Yes	No	Yes	Yes	Yes
Handles task-based control	No	No	Yes	Yes	Yes
Level of security	Low	High	High	High	High
Level of assurance	Low	High	High	High	High
Incorporates easily into technologies (e.g., web services)	No	No	Yes	Yes	Yes
Able to express other models	No	No	Yes	Yes	Yes
Break-The-Glass (BTG) support	No	No	No	No	No

Every model has its specific characteristics that can be advantageous depending on the objectives and level of security required. Moreover, the characteristics of the RBAC model provide for its easier extension to the requirements and specificities of the domain and can, this way, give origin to other models such as the ABAC and TBAC presented here. The characteristics of these new models are very similar to the RBAC model and the main difference resides only within their authorization paradigm. This may be the reason why the

RBAC model it is usually the most widely used access control model within the healthcare domain as shown by the access control literature review in Chapter 2. Finally, none of the described access control models support Break-The-Glass (BTG), which means, they do not allow overriding the predefined access control rules when unanticipated or emergency situations occur that may require this to happen.

Authentication and/or access control technologies and mechanisms are used to enforce the objectives and rules of access control policies. In simpler systems, authentication mechanisms are used solely with an implicit access control function. In more complex systems, authentication mechanisms are used to identify and authenticate the user together with access control mechanisms that check the user's access rights. Examples of authentication mechanisms are: username/password or PIN; biometrics; token devices; and smartcards. Examples of access control mechanisms are: access control lists, capability tables, policy based systems or constrained user interfaces [3].

Although access control policies can be very generic, they are the most important concept of the three (i.e., access control policy, model and mechanism) as they describe the security needs of the organization, how resources and information must be protected and how this must be modelled and implemented in practice. So the main focus must reside in defining access control policies as accurately as possible. Only afterwards should models and mechanisms be defined and chosen accordingly to enforce those policies.

1.1.2 Electronic medical record barriers

One obstacle mentioned by HCPs for the use and integration of EMR within healthcare is the lack of controls to provide for patient privacy [20]. As stated earlier, in order to protect patients' privacy it is essential at least to 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. HCPs report that using EMR has problems in terms of security due to its ease of distribution and wider online access [21]. If they do not comprehend the technology or how the system can or cannot control access to patient information it will be more difficult for them to agree on using 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 as: time/cost, relational and educational [22, 23]. Apart from the cost of EMR integration and the time HCPs 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 as explained below.

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 system the physician is using. The patient usually does not know what information the system holds or how that information can be used or what kind of protection is provided.

The educational barrier comprises the lack of proficiency and difficulties that HCPs have in interacting with the EMR in order to perform their daily tasks [24]. HCPs do not usually participate in the design and development of working tools (in this case the EMR) so they usually have to redesign their workflow practices and processes, which is very challenging and consumes significant time and costs [23]. As HCPs need to access and use the EMR to perform their daily tasks, their involvement in its design and development can facilitate and even improve their daily workflow and subsequent patient treatment.

The main factor that drives the need for EMR systems to be implemented is the need to improve clinical processes or workflow efficiency [10]. Furthermore, information technologies are used in healthcare to record, transmit and provide access to administrative and clinical information [25], and so provide for patient information confidentiality whilst bringing efficiency and quality to healthcare. But now, the reality is that EMRs still do not integrate easily into HCPs' daily workflow [23] in order to be efficiently used.

The problems stated above relate mainly to human processes and workflows. If technology does not exist already, it should be implemented and adapted to existing systems according to its main objectives in order to fulfil professionals' needs, instead of bringing them more concerns. In healthcare it is very common to force the introduction of technology and expect HCPs to use it [25]. However, even if they want to use the systems, they may spend more time and effort adapting them to their own needs, to the detriment of patient care.

Although there is usually an initial plan describing the rules to access an EMR, devised by engineers, managers and implementers, its access in practice is often different from what was envisaged and decided at first [26, 27]. 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 [27, 28] because they were too cumbersome or time-consuming or both (e.g., by sliding in a personal ID card, keying in a password and leaving it there indefinitely).

Certainly technology can deeply transform how humans live, work, strive, thrive and die [29]. Patients, healthcare providers and health technologies are mutually reliant on one another and this interdependence regularly affects how healthcare is performed [30].

An example is given in [31] that describes the problems that were encountered when evaluating a health IS. Besides infrastructural and implementation problems, reasons for failure included: not ensuring users understood the reasons for that implementation and the underestimation of the complexity of the healthcare tasks.

Ultimately, access control is closely related to the definition of a system workflow, how the system is used and how tasks are accomplished. Again, access control policies define who the actors of the system are and what they can do with it. Access control models define and model in an explicit way system workflow and authorised actions. Therefore when policies are hard to implement, there must be a focus on defining and improving access control models and implementation, so that some of the problems with EMR workflow and task definition can be minimized.

1.2 Research question

Current healthcare access control policies are usually not properly defined and therefore very difficult or even impossible to model. These policies either do not exist or do not integrate users' needs (i.e., HCPs as well as patients), so when it comes to their usage, HCPs can have many difficulties. Access control models also have some limitations in modelling these policies, not only because the policies have already some limitations themselves, but also the access control models do not reflect users' needs, experiences and workflows, together with generic and regulatory issues, as well as emergency or unanticipated situations that may occur. It can be hard for a model to be flexible enough to integrate such varied sort of access control policies.
The main research question is therefore: how can the current EMR access control systems be improved?
Another research question/problem to be tackled is: how can the barriers to the effective use of EMR systems be reduced?
One hypothesis is that the collaboration of HCPs and patients in the development of access control systems for EMR may help to facilitate access to the information, improve healthcare workflow and processes and lessen the security as well as educational and time/costs issues that are involved. This hypothesis will be tested in this thesis in three stages. Firstly an access control policy will be defined that can integrate rules from generic issues, such as legislation and regulations and also from specific issues, such as HCPs and patients' needs, opinions and experiences. Secondly, with this set of access control rules, a new access control model will be defined in order to overcome some of the current limitations of the existing models, which normally hinder the proper use of EMR. Thirdly, the new model will be implemented and tested in a hospital setting. Access to and use of EMR should, in this way, be closer to real healthcare workflow and tasks, something that current policies and models do not do.

1.3 Objectives

For the research questions that were formulated in Section 1.2, the objectives are:

- to determine the security-related (mainly access control) factors that hinder the implementation of EMR;
- to determine the legislation-related factors that hinder the implementation of EMR;
- to study access control from the end user's perspective;
- to devise and define an appropriate set of access control rules with the users collaboration (including emergency or unanticipated situations);
- to define an access control model that can incorporate the access control rules above;
- to implement and evaluate that access control model in a hospital setting.

Furthermore, this research should be useful to find new ways to study and improve the definition and use of access control systems within other areas of healthcare as well as in similar domains where confidentiality and the interaction between human users and ISs is a crucial requirement.

1.4 Contributions

The main contributions of this thesis are as follows, this research:

I. developed and proposed a process to define and implement, from legislation to practice, access control rules that can integrate both generic (legislation and regulations) and specific (end user) access control needs;

II. showed how Grounded Theory (GT), an approach that uses qualitative analysis, commonly applied in social science research, can be used to explore and develop new ideas and concepts in relation to the security of EMR and its end users;

III. developed a set of access control rules that integrated both legislation and end users' needs of an EMR system;

IV. developed and proposed a new access control model, the BTG-RBAC model, in order to integrate the aforementioned access control rules;

V. provided the results of implementing the BTG-RBAC model prototype as well as the impact analysis from a BTG pilot case study that was implemented within a real healthcare scenario. This case study tested the concept of BTG with an EMR system that is used daily in the healthcare practice as well as the research process mentioned in I.

Several articles and two book chapters have been produced and published with the research work described in this thesis. These are:

ARTICLES

- *Ferreira A, Cruz-Correia R, Chadwick D, Antunes L. Access Control in Healthcare: the methodology from legislation to practice. Proceedings of the 13th MEDINFO Congress. IOS Press. 2010. (in press).*

- *Ferreira A, Antunes L, Chadwick D, Cruz-Correia R. Grounding Information Security in Healthcare. Int. J. Med. Inform. 2010. 79(4):268-283.*

- *Farinha P, Cruz-Correia R, Antunes L, Filipe Almeida, Ferreira A. From legislation to practice: a case study of break-the-glass in healthcare. Proceedings of the International Conference on Health Informatics – Healthinf 2010. 114-120.*

- *Ana Ferreira, David Chadwick, Gansen Zao, Pedro Farinha, Ricardo Correia, Rui Chilro, Luis Antunes. How to securely break into RBAC: the BTG-RBAC model. Proceedings from the 25th Annual Computer Security Applications Conference - ACSAC2009. 2009. 23-31.*

- *Ana Ferreira, Ricardo Correia, David Chadwick, Luis Antunes. Improving the implementation of access control to electronic medical records. Proceedings of the IEEE International Carnahan Conference on Security Technology. 2008. 47-50.*

- *Ferreira A, Antunes L, 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, Cruz-Correia R. Who should access electronic patient records. Proceedings of the International Conference on Health Informatics – Healthinf 2008. 182-5.*

- *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.*

- *Ferreira A, Chadwick DW, Antunes L. Modelling access control for healthcare information systems: how to control access through policies, human processes and legislation. DCEIS. 2007. 3-13.*

- *Ana Ferreira, Ana Correia, Ana Silva, Ana Corte, Ana Pinto, Ana Saavedra, Ana Luís Pereira, Ana Filipa Pereira, Ricardo Cruz-Correia, Luís Filipe Antunes. Why facilitate patient access to medical records. Studies in Health Technology and Informatics. IOS Press. 2007. 127:77-90.*

- *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.*

BOOK CHAPTERS

- *Ana Ferreira, Ricardo Correia, David Chadwick, Henrique Santos, Rui Gomes, Diogo Reis, Luis Antunes. Password sharing and how to reduce it. Certification and Security in Health-Related Web Applications: Concepts and Solutions. Dr. Ioannis Apostolakis, Anargyros Chryssanthou, Dr. Iraklis Varlamis. (in press).*

- *Ana Ferreira, Ricardo Cruz-Correia, Luís Antunes, David Chadwick. Chapter III: Security of Electronic Medical Records. Handbook of Research on Distributed Medical Informatics and E-Health. A. Lazakidou, K. Siassiakos (Editors), in English, Medical Information Science Reference, ISBN 978-1-60566-002-8, 575 pp, Aug 2008.*

Other research work was performed concurrently to the production of this thesis and related to EMR integration, e-Learning and security in the healthcare domain. Published articles and book chapters are listed here:

ARTICLES

- *Ana M. Ferreira, Ricardo Cruz-Correia, Altamiro Costa-Pereira. Why teach computer security to medical students? Proceedings of the 12th MEDINFO Congress. IOS Press. 2007. 129: 1469-1470.*

- *Cristina Costa-Santos, Ana Coutinho, Ricardo Cruz-Correia, Ana Ferreira, Altamiro Costa-Pereira. E-learning at Porto Faculty of Medicine: a case study of blended-learning. Proceedings of the 12th MEDINFO Congress. IOS Press. 2007. 129: 1366-1371.*

- *Ricardo J Cruz-Correia, Pedro M Vieira-Marques, Ana M Ferreira, Filipa C Almeida, Jeremy C Wyatt, Altamiro M Costa-Pereira. Reviewing the integration of patient data: how systems are evolving in practice to meet patient needs. BMC Medical Informatics and Decision Making. 2007. 7:14.*

- *Ferreira A, Barreto L, Brandão P, Cruz-Correia R, Sargento S, Antunes L. A secure wireless architecture to access a virtual electronic patient record. IEEE Pervasive Health Conference and Workshops. 2006. 1-8*

- *Cruz-Correia R, Vieira-Marques P, Ferreira A, Oliveira-Palhares E, Costa P, Costa-Pereira A. Monitoring the integration of hospital information systems: how it may ensure and improve the quality of data. Stud Health Technol Inform 2006. 121: 176-182.*

BOOK CHAPTER

- *Ana Ferreira, Luís Barreto, Pedro Brandão, Ricardo Correia, Susana Sargento, Luís Antunes. Chapter II: Accessing an existing virtual electronic patient record with a secure wireless architecture. Phillip Olla, Joseph Tan (Editors). Mobile Health Solutions for Biomedical Applications. Medical Information Science Reference. ISBN 1605663328, 366 pp, Mar 2009. 24-45.*

1.5 Thesis structure

The structure of this thesis is as follows.

Chapter 1 introduces the background of this research, the main problems regarding access control in healthcare and the goals and contributions of this research work.

Chapter 2 presents a comprehensive technical review of related research. It covers the topics of both generic and healthcare access control research in terms of access control policies, models and authentication mechanisms. It further provides a description of a security audit report for several healthcare institutions as well as the results of a study on the subject of patients' awareness regarding their rights to access their medical records.

Chapter 3 introduces a review on grounded theory and mixed methods, and justifies the selection and use of these methods within this research work in order to assess end users' needs, opinions and experiences, and regulatory and legislation issues regarding access control in healthcare.

Chapter 4 presents a review and analysis of the access control issues of healthcare and information security standards as well as the American and European healthcare regulations, recommendations and legislation. This chapter also includes a list of legislative access control rules that were extracted from this analysis.

Chapter 5 presents the results of the application of grounded theory and mixed methods to the end users of healthcare ISs (both HCPs and patients).

Chapter 6 provides a list of access control rules that was extracted from the appliance of the mixed methods and grounded theory research described in the previous chapter, as well as legislative and standards rules that were described in Chapter 4. It also describes the transformation of this list into standard RBAC rules that can comprise a new access control policy.

Chapter 7 proposes and describes in detail a new access control model – the BTG-RBAC model – that moulds the generated access control rules in Chapter 6 in order to include BTG access control rules into the RBAC standard model.

Chapter 8 describes the development, implementation and evaluation of the BTG-RBAC model prototype as a proof of concept within an authorisation platform.

Chapter 9 presents the results of implementing and testing a BTG pilot case study on a real healthcare setting that is used on a daily basis. It presents the impact analysis that this pilot had on the HCPs' daily workflows. Further, it evaluates the research process that was used in order to enforce legislation into the healthcare practice.

Chapter 10 concludes the thesis by summarizing the contributions, recommendations and limitations as well as some topics that were not covered by this thesis but where future research can be conducted.

Figure 1.1 describes diagrammatically the research process followed in this thesis. It shows, in a generic way, the steps performed for each chapter and how these relate with each other in order to compose the full thesis.

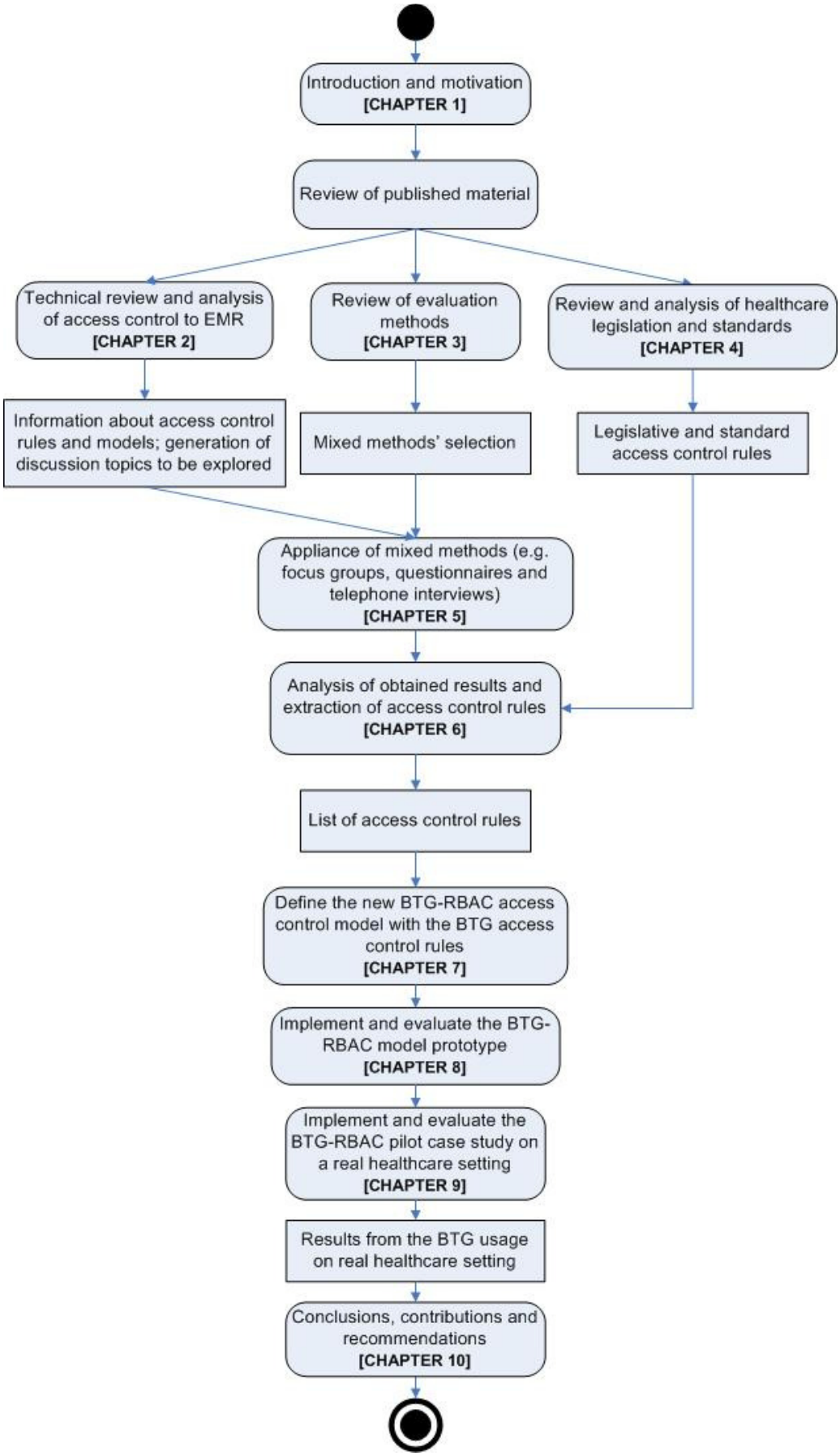

Figure 1.1 – Diagram with the research process performed during the course of this thesis.

2 ACCESS CONTROL LITERATURE REVIEW

2.1 Introduction

In order to learn what the common practice and the main gaps are in designing and defining access control within EMR systems, two systematic reviews were conducted. 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 the healthcare environment [32] [33].

2.2 Materials and methods

Two systematic reviews were conducted of full articles published between 1996 and mid 2006. The first review included articles related to 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) as well as in security conferences, which include SACMAT (Symposium on Access Control Models and Technologies), ESORICS (European Symposium on Research in Computer Security) and CCCS (Conference on Computer and Communications Security). Specific queries were made in IEEE Xplore (access control<in>metadata) and ACM with "access control". The review was done in several stages. Titles and the abstracts were read from the list of articles retrieved by the queries. Then the most important topics about access control were summarised in a table. The articles included in the review described at least one of the following topics:

- **Type of access control policy**: institutional, legal, end-user, override and other;
- **Type of access control model**: RBAC, 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**: build the model; prototype or real implementation;
- **Problems**: the limitations;
- **Successes**: the advantages and benefits.

Articles that applied specifically to the healthcare domain were excluded from this review but were included in the second review. From the articles selected, the full articles that were available were read and the summary table mentioned previously was filled with the necessary information.

Figure 2.1 shows the flowchart that describes the method used as well as the number of papers included in the review.

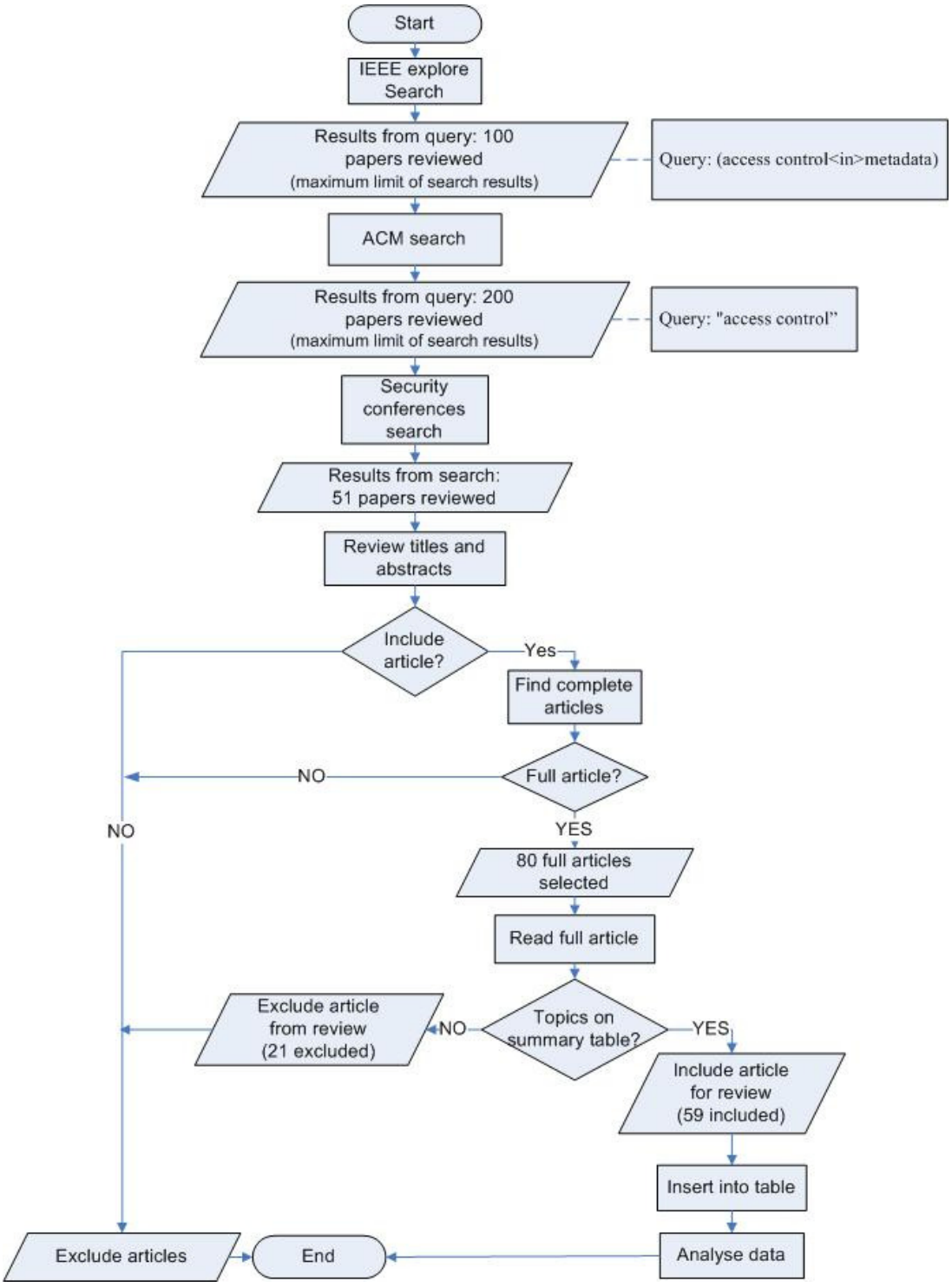

Figure 2.1 – Flowchart representing the review process for generic access control. Notice that in some of the results it is specified that this is the maximum limit of search results shown, although there were more articles available and retrieved by the search query.

For the second review, the method used was similar to the one described above but applied to access control policies, models and authentication mechanisms (that incorporated an implicit access control function) specific to the healthcare environment. Searches were made in medical databases such as Medline (that included the BMJ-British Medical Journal) 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”.

Titles and abstracts were read from the list of articles that were retrieved by the queries. The most relevant topics about access control were summarised in a table. Articles that were included described at least one of the following topics:

- **Type of access control policy**: institutional, legal, end-user, override and other;
- **Type of access control model**: RBAC, 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 HCPs;
- **Portal/Internet access**: HCPs, patients and other;
- **Results**: build the model; prototype or real implementation;
- **Problems**: the limitations;
- **Successes**: the advantages and benefits.

Next, the full version of the articles was searched. The summary table was filled whilst the full articles were being read.

Figure 2.2 shows the flowchart that describes the method used for this review.

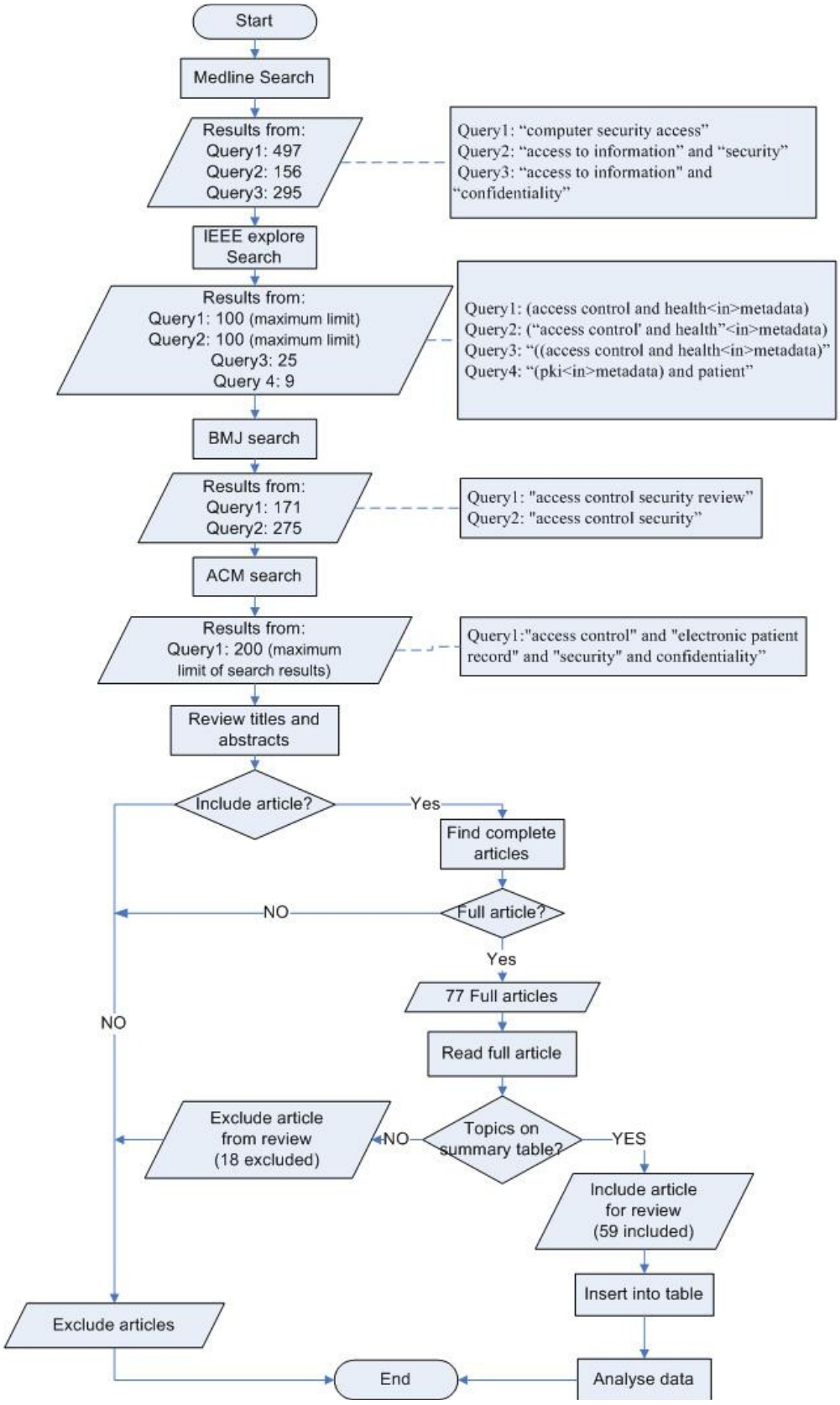

Figure 2.2 – Flowchart representing the review process for healthcare access control. Notice that in some of the results it is specified that this is the maximum limit of search results shown, although there were more articles available and retrieved by the search query.

2.3 Results

2.3.1 Generic access control review

The review for generic access control comprised 351 articles that were obtained from the search queries. After reading the 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. As can be seen in Table 2.1, from the 17 articles that mentioned the definition and use of an access control policy only in 1 case was it implemented, and this was a prototype system. This shows that implementing policies is not trivial because adapting theoretical procedures to a real environment may be impractical if these policies are not closely related to the workflow processes and humans that are involved. Although not many access control policies were implemented in practice, the access control models were. 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 was done within the model and not defined separately, which can complicate the whole process. From the 59 articles that mentioned access control models, 52 concentrated on the study of an access control model and in only 8 cases were these studies implemented, mostly as prototypes with only 1 [34] of these being implemented in a real scenario. This confirms the complexity of applying the models into a real scenario.

Table 2.1 – No of papers reviewed covering access control policies, models and mechanisms between 1996 and 2006.

	1996-99	2000-03	2004-06	Total
Access Control Policy				
Study/Analysis	-	4	12	**16**
Implementation	-		1	**1**
Access Control Model				
Study/Analysis	4	11	37	**52**
Implementation	-	2	6	**8**
Authentication Mechanisms (w/ implicit access control function)				
Study/Analysis	**-**	5	10	**15**
Implementation	**-**	1	2	**3**

Nevertheless, a vast majority (38 in 52 articles) include the use of the RBAC model in order to develop their access control systems. This can be explained by the fact that the RBAC model allows for easier administration and a more flexible approach in order to adapt workflows and hierarchical structures from large and heterogeneous organizations to access controls. In terms of access control mechanisms, the most commonly used were usually digital signatures and

certificates. These mechanisms are usually complex and require an infrastructure that involves many human and technological resources. If the access control requirements are not correctly stated within an access policy where human aspects are usually defined, this infrastructure may be difficult to achieve.

The most commonly studied and prototyped authentication mechanism was digital signatures with public key certificates (9 out of 15).

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.

2.3.2 Healthcare access control review

From the review applied to the healthcare environment, 948 articles were obtained from the Medline search queries, 234 from the IEEE queries, 446 from the BMJ search and 200 from the ACM queries. These articles 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.

From a total of 27 articles that refer to the system's implementation, 25 were built as prototypes whilst only 2 were built in a real life scenario.

From the 34 published articles that mention access control policies, Table 2.2 shows that 22 refer to the study and analysis of those policies, whilst only 4 of them actually implemented policy based systems as prototypes. In 14 out of these 34 papers, the policies were institutionally or legislatively defined, whilst in only 4 of those 34 articles is it mentioned that end-user can set policies. But none of these 4 policies were actually 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.

Table 2.2 – No of papers reviewed covering access control policies, models and mechanisms in healthcare between 1996 and 2006.

	1996-99	2000-03	2004-06	Total
Access Control Policy				
Study/Analysis	2	8	12	**22**
Implementation	-	3	1	**4**
Access Control Model				
Study/Analysis	6	10	8	**24**
Implementation	1	6	1	**8**
Authentication Mechanisms (w/ implicit access control function)				
Study/Analysis	6	10	8	**24**
Implementation	1	6	1	**8**

Finally, 7 articles refer the need for an override policy definition i.e., an access control system that 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. This is specially important because the need to override access control systems can be useful and meaningful in the context of healthcare and therefore needs to be analysed when implementing those systems [35].

As for access control models, from the 40 articles that refer to the use of access control models, 24 of these mention its study and analysis whilst in 8 articles the models were implemented as prototypes only.

The most commonly used access control model was RBAC (22 from 40) whilst the most tested authentication mechanism was digital signatures with public key certificates (29 from 41).

Focusing now on the EMR and its users, Table 2.3 shows the type of ISs that were implemented and in which healthcare institutional setting they were implemented. It also presents the most common types of user groups for those systems.

Table 2.3 – Healthcare institutions, information systems and user groups.

	1996-99	2000-03	2004-06	Total
Healthcare Institution				
Hospital	3	10	7	**20**
Hospital Department		2		**2**
Primary Care		1	1	**2**
Private Care		1	3	**4**
Other		2	5	**7**
Total	**3**	**16**	**16**	**35**
Healthcare Information System				
EPR/EMR/CPR	5	14	15	**34**
Prescription		2	1	**3**
Consultation			1	**1**
Total	**5**	**16**	**17**	**38**
Portal/Internet Access				
HCPs		1	1	**2**
Patients		1		**1**
Total		**2**	**1**	**3**
User groups				
Medical doctors		2	2	**4**
Nurses		3	2	**5**
Patients		1	4	**5**
Others (HCPs,GPs,IT,Pharmacists)	2	13	9	**24**
Total	**2**	**19**	**17**	**38**

Most of the ISs are EMR (34 from 38 articles) and were implemented within hospitals (20 from 35 articles). The end users of the system are mostly HCPs, general practitioners (GPs), IT and pharmacists. Only in 5 articles is it mentioned that patients might have access to their healthcare information but none of these systems were being used in a real environment. These results are not in agreement with most legislation that defines that patients can access their medical record when requested [36]. Patients should define who can or cannot access their sensitive clinical information. According to [37] the access to medical records improves patients' adherence to treatment and the efficiency of the service. According to [38] there are some benefits in patients accessing their medical records and new technologies such as EMR should help improving and supporting this access.

The most common users of the EMR are HCPs that use the system to perform their work and expect EMRs to help them to be more effective in doing so [10]. There is usually a great

difficulty in creating a proper migration plan from paper records to the electronic system and the inability to find an adequate EMR solution that meets HCPs needs. Among all this, there is also some lack of support by medical staff in order to implement EMR systems [10]. Without end users' (e.g., HCPs and patients) interaction and support in the design and development of EMR it becomes very difficult to ensure integration success. It is very important to know their opinions according to their experiences of using prototype systems.

As an example, this study [39] applied a survey in order to find out medical doctor's opinions regarding access control to EMR within a university hospital. Most respondents agreed that different types of roles must exist for access control to EMR and that not all doctors must have total access to all patient records. They indicated that more sensitive information (e.g., HIV) must only be accessed by doctors that treat those patients. A great number of doctors also revealed that patients should not have total access to their own medical records. This must be further analysed as patients have the right, accordingly to law, 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 that 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.

2.4 What happens in practice

2.4.1 Security audit report from 38 Portuguese hospitals

This example demonstrates how difficult it is to provide for security in the healthcare domain and to protect medical data on a daily basis [40]. It is an auditing report that evaluates the security problems involved in the generation, collection, processing and access to medical data within several hospitals in Portugal. In this country, the processing and access to medical data must be notified and approved by a National Commission of Data Protection (CNPD – www.cnpd.pt). This allows the responsible entity to control and authorize the process whilst enforcing the legislation.

From the 38 hospitals that were audited, 6 had never asked for an authorization from that responsible entity. 195 data processes were notified by the 32 hospitals that asked for authorization for this matter but still, CNPD found 193 processes that were never notified. This report describes that around 50% of the medical data that is processed within hospitals is not notified to the responsible authority. Patient data is often used for research without patients' consent or even knowledge that this is happening. There are still some medical applications that do not use any kind of access control or restriction, or even backups; 36% of

the studied applications have no logical separation between administrative and medical data; and paper records that transit through the hospitals have no kind of security protection whatsoever.

2.4.2 Patients' awareness: the right to access their medical records

This section presents a small part of the study results that include the patients' views on accessing their medical records. This study was performed as part of a bigger study of patients (n=200), using structured telephone interviews, in order to assess their views regarding several aspects of access control in healthcare (more details in Section 5.3.3).

Results showed that 124 (62%) respondents did not know what an EMR was while 76 (38%) did. Only 58 (29%) respondents said that they know that it is within the legislation that they can access their own medical records. Furthermore, 131 (65%) would like to access their medical records while 68 (34%) would not and 1 (1%) respondent did not know. From the 132 respondents that would like or don't know if they would like to access their medical records, 102 (77%) said they would need HCPs' help to view and understand the records while 28 (21%) said they would not need that help. 2 (2%) respondents said they did not know. In terms of type of access, 102 (77%) would like to do it with a computer while 30 (23%) would not want to use a computer for this purpose. Finally, 164 (82%) respondents think that their medical records should be available 24/7 (everyday at anytime) while 26 (13%) said there was no need and 10 (5%) did not know.

2.5 Discussion

Typically there is a big focus on the definition of access control models and how they can be implemented, but most of these models are defined without a proper access control policy definition. Furthermore, only a few of these EMR 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. There is a need to develop and implement access control within real healthcare practice to make sure that research in access control is making a difference and enhancing the systems' integration and use.

To complement these results, research showed that in the Portuguese healthcare practice security problems are very common and EMR information is not protected as expected according to legislation and ethical regulations. Furthermore, on the patients' side, there is the will to access their medical records, with a vast majority preferring to use a computer although most patients do not know they are entitled to do it whenever they need or require, according to legislation.

This, together with all the reviewed material and results that were presented in this section, need to be taken into account when defining access control policies in the healthcare domain.

The results from the search performed in Section 2.3.2 regarding the use of access control models in healthcare were updated using Figure 2.2 in order to include the last 3 years of published material (Table 2.4).

Table 2.4 – Number and type of access control models from published articles in healthcare.

Access Control Model	1996-1999	2000-2003	2004-2006	2007-2009	TOTAL
RBAC	3	12	7	17	**39**
IBAC(DAC)		3			**3**
Hybrid			2	1	**3**
Private/own				1	**1**
Other	4	3	6	3	**16**

Again RBAC was the most used access control model. This may be an appropriate choice to start the research on improving access control rules and policies in the healthcare domain.

3 EVALUATION METHODS LITERATURE REVIEW

3.1 Introduction

In order to answer the research questions stated previously it is essential to start by defining the methods to be applied aiming to reach the defined objectives.

Firstly, there is the need to evaluate the generic issues (i.e., legislation, regulations and standards) that mould the access control process in healthcare.

Secondly, and most importantly, it is indispensable to evaluate to the best of our ability the users' needs and workflows in the environment where the system is or will be implemented. This chapter will focus mainly on defining the methods that will be used to evaluate user needs.

The development and design of usable technology is very important as good user interface design can make users more productive and comfortable when using the system. Developers do not usually understand users, their tasks, workflows and environment. A system interface is the bridge between the world of technology and the world of the user and the means by which the user interacts with the system [41]. What can be more important than making sure people use the system in their natural physical, social and cultural environment?

For example in [42] 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, an interface redesign improved its efficiency, making the tool easier to use and understand.
Another example is briefly described in [41] where programmers designing a medical records' system completely changed their initial software interface after they visited the users' site. They discovered that the workflow among departments and individuals proceeded in a different manner to what they had imagined. They watched people performing their tasks and interviewed healthcare staff about the nature of their work. The message then is to design from reality and not from assumptions. Evaluation methods must focus on users' behaviour as well as their attitudes and opinions. How do researchers evaluate the attitudes and needs of HCPs and patients regarding EMR or any of its features such as access control? The evaluation of healthcare ISs' is not trivial [43]. Medical informatics is a combination of domains that makes any evaluation very complex and never definitive. There is not a specific method for all cases and one of the most important things to take into account is to choose the right method at the right moment in time, if possible.

A brief review was performed using the Google Internet search engine. It comprised 27 articles (3 of which are websites) from 1999 till 2006 about evaluation methods applied to ISs, 8 of which were in the healthcare domain. The main results of this review are presented in Table 3.1.

Table 3.1 – Results from the review of IS evaluation methods.

Objectives of publication	**Total**
Presents methods to evaluate information systems	13
Evaluates evaluation methods	10
Checks for technology or applications' improvements	
Information System's Evaluation	4
Methods used to perform Evaluation	
Others	6
Usability testing	4
Questionnaires/interviews	4
Literature review	3
Not mentioned	3
Cognitive science	2
Quantitative/qualitative	2
Soft-systems methodology	2
Heuristics	2
Ergonomic methods and tools	1
Problems Encountered	
No proper evaluation methods to evaluate information systems	12
Evaluated applications are difficult to use	6
Applications have complex workflow analysis and decisions	5
Applications have high costs and insufficient policies	2
There was insufficient Infrastructure for the evaluated applications	1

The reviewed articles either try to introduce new methods of evaluation or present the results of analyzing some existing evaluation methods. The articles are concerned with either finding the most adequate evaluation methods or trying to check what the main problems with the existing methods are. The most common used methods to evaluate IS, besides proprietary ones, are usability methods, questionnaires and interviews. The most frequent problems encountered within the reviewed articles are that the evaluation methods are usually not right for the evaluation that needs to be performed. Also, regarding the ISs that were evaluated, the results show that the problems of the evaluated applications are not, as was probably expected, the cost of developing and running the applications. Instead, the articles found that applications were often difficult to use and the workflow and decision support were usually too complex and could not be implemented.

Table 3.2 shows the most common problems encountered when evaluating the healthcare systems. These results are summarized from the review described in this chapter as well as from the review presented in Section 2.3.2.

Table 3.2 – Most common usability problems encountered when evaluating healthcare ISs.

Problem type	No of occurrences
Disruption to workflows & performance	7
Educational barriers	5
Management problems	4
Cultural barriers	2
Increase in time for patient session	1
Security concerns	1
Relational barriers	1

Not surprisingly, most problems relate mainly to the disruption of workflows and performance when the EMR is used. Educational and management problems also rank highly. This confirms the fact that the end users of the system (i.e., HCPs) are frequently connected with the lack of success of integrating EMR into their practice. This does not mean they are the problem. It simply means that end users of the system, a key stakeholder in the process, do not have a word to say in its design, development and implementation, and therefore cannot contribute with their experience and knowledge in order to ensure the systems are usable on a daily basis.

In summary, there are many unresolved issues to consider regarding IS evaluation and this remains very challenging as no adequate methods exist that can be used in a generic fashion. Nevertheless, there are some examples where the application of specific evaluation methods, usually more than one, helped to improve the use and integration of ISs [41] [42]. These examples can be considered as a starting point to solve the stated research problem.

3.2 Grounded theory

Grounded theory (GT) is a research approach that focuses on developing theory from qualitative analysis of data without any particular commitment to specific kinds of data, lines of research or theoretical interests [44]. Instead of identifying a sample at the outset, GT involves a process of theoretical sampling[1] of successive sites and sources, selected to test or refine new ideas as they emerge from data. GT relies mainly on qualitative data acquired through a variety of methods such as observation, unstructured interviews in the initial stages and then more structured forms of data collection as the study becomes more focused.

[1] After the researcher analysing the results from a study, he/she asks "Where can I find instances of *X* or *Y*?". The technical term for this is theoretical sampling for after previous analysis, the researcher seeks for samples of population, events or activities that are guided by the emerging theory at that moment [44].

The process of analyzing data focuses on coding the data collected using qualitative methods into categories for the purpose of comparison, using the hermeneutic cycle presented in Table 3.1. These categories are not mere labels but conceptualizations of key aspects of the data. Data collection stops when the categories reach theoretical saturation. Theoretical saturation means that further data no longer prompts new distinctions or refinements of the categories and emerging theory [45].

The GT approach is commonly used in social science research where social scientists try to explore all aspects of human behaviour and environment. They re-examine the social world in order to understand or explain better why and how people behave [46]. GT can also be applied in other areas of research where there is a need to generate theories and ideas from research data [45]. In GT, a theory can evolve in a continual process so researchers are creative participants that will start with a case to study, theorise the case, use this information in order to select the next case, move to the selected case, theorise it and then compare the theories generated (Figure 3.1).

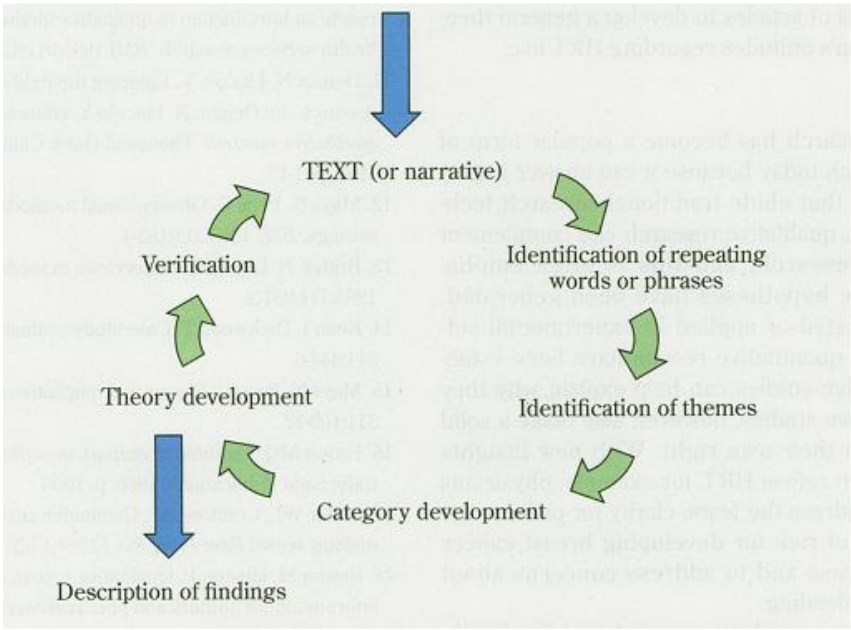

Figure 3.1 – Iterative process of the qualitative analysis of data [47].

One of this thesis' objectives is to focus on understanding HCPs' experiences, workflows and behaviour as well as the social context throughout the development and use of EMR to include in an access control policy. Healthcare is a complex environment, so it is important to understand and learn as much as possible about it by collecting qualitative data and analysing it based on the iterative process in Figure 3.1. In order to achieve the proposed objectives in this thesis, data is first collected with a qualitative method and then words and phrases that relate directly to the study are identified and grouped afterwards into main themes. From these

themes, several categories will be developed. However, this is not done directly as more data will be collected specific to these categories and further analysis will be done in order to confirm the existing categories or generate new ones. With the final main categories that are developed, it will be possible to formulate access control rules that can describe, closer to reality, users' interactions with the EMR and then include these in the subsequent design and implementation of an access control policy and model.
GT is therefore an appropriate approach to use in this study.

3.3 Mixed methods' research

It is common among social scientists to draw a distinction between qualitative and quantitative research (Table 3.3). This distinction may have its origins in the history of some disciplines like sociology with the quantitative application of questionnaires and survey methods and their statistical treatment; and social anthropology where qualitative analysis of field data is more frequent. Qualitative methods are usually used by researchers who work as ethnographers [46] [48], clinical and organizational psychologists or sociologists. Qualitative methods tend to focus on situational and structural contexts but are weak on cross-comparisons as they often study only single situations, organizations and institutions. Quantitative methods, on the other hand, focus on multivariate situations but are weak in context [44]. At the most basic level, quantitative research involves the use of methodological techniques that represent the human experience statistically while qualitative research provides detailed descriptions and analysis of the quality or substance of the human experience [46].

Table 3.3 – Differences between qualitative and quantitative methods (adapted from [49]).

Research activity	Qualitative	Quantitative
Selection of research participants	Theoretical sampling	Random sampling
Data collection	Direct observation techniques	Pre-coded surveys or similar techniques
Data analysis	Analysis focused on context-specific meanings and social practices	Statistical analysis aimed at highlighting universal cause and effect relationships
The role of conceptual framework	Views theory and methods as inseparable	Separates theory from methods

Despite the fact that there is a clear distinction between qualitative (theory generation) and quantitative (theory testing) methods, there is also much overlap both in practice and theory, and these methods should not be seen as orthogonal. They are similar in that they both build on

empirical or observable reality and regardless of their methodological and theoretical differences researchers agree that social research should be about the real world.

Some researchers opt for the use of mixed methods which combine both qualitative and quantitative techniques for the same study.

Mixed methods research refers to those studies or lines of inquiry that integrate one or more qualitative and quantitative techniques for data collection and/or analysis [50]. The quantitative/qualitative distinction made by some researchers can be criticized by the fact that philosophical aspects of a particular approach should be replaced by a more practical need to use a more suitable approach for the task at hand [46]. Although mixed methods can lead to different and sometimes conflicting results, they can be a rich source of discussion and can enhance the robustness of the study. Such results may also lead to different and useful conclusions from those that would have been drawn from relying on one method alone and this demonstrates the value of collecting both types of data within a single study [51]. Combining methods may generate deeper insights than each method applied alone and can activate their complementary strengths and help to overcome their discrete weaknesses. The principle of complementarity relies on using the strengths of one method to enhance the other [52]. Each new set of data increases the confidence that the research results reflect reality rather than a methodological error. Divergent findings are equally important because they signal the need to analyze a research problem further and to be cautious in interpreting the significance of any set of data [53]. Efforts to integrate the complementary strengths of different methods should be done by using a qualitative and quantitative method for different but well coordinated purposes within the same overall research project. This has to be done by making two important decisions: (a) *Priority decision*: what is the principal and what is the complementary method and (b) *Sequence decision*: in which sequence should the methods be applied [54]. For the latter, the most common strategy is to use what is learned from one to inform what is learned from the other. According to the research objectives, the researcher must choose one of the four combinations that pertain to the priority-sequence model for using mixed methods (Table 3.4).

Table 3.4 – The priority-sequence model: complementary combinations of qualitative and quantitative methods [52].

Principal Method (Sequence Decision)	Purposes	Expected Results	Example
Quantitative (qual→QUANT)	Smaller qualitative study helps guide the data collection in a principally quantitative study	Can generate hypotheses, develop content for questionnaires, etc	Focus groups help to develop culturally sensitive versions of a new health promotion campaign
Qualitative (quant→QUAL)	Smaller quantitative study helps guide the data collection in a principally qualitative study	Can guide purposeful sampling, establish preliminary results to pursue in depth, etc	A survey of different units in a hospital locates sites for more extensive ethnographic data collection
Quantitative (QUANT→qual)	Smaller qualitative study helps evaluate and interpret results from a principally quantitative study	Can provide interpretations for poorly understood results, help explain outliers, etc	In-depth interviews help to explain why one clinic generates higher levels of patient satisfaction
Qualitative (QUAL→quant)	Smaller quantitative study helps evaluate and interpret results from a principally qualitative study	Can generalise results to different samples, test elements of emergent theories, etc	A statewide survey of a school-based health program pursues earlier results from a case-study

3.4 Chosen methods for this research

If a concept or a phenomenon needs to be understood because little research has been done on it, such as in this study, then it merits a qualitative approach. The qualitative research is exploratory and useful when a researcher does not know the main variables to examine. Moreover, a mixed methods design is useful when either the qualitative or quantitative approach by itself is inadequate to understand a research problem better or the strengths of both methods can provide the best understanding [54].

The choice for these methods should focus on HCPs' workflow, culture, tasks and routines as well as patient needs and requirements. It makes sense to apply different and complementary methods so that a more complete view on this topic is obtained. Health researchers are more likely to try and connect the strengths of different methods to address the complexity of their research topics because they usually integrate both pure research and applied uses in practical settings [52].

One way to choose the sequence of the mixed methods to use, when the objective of the research is to study users' needs and experiences about a specific subject, is to use a flowchart like the one presented in Figure 3.2.

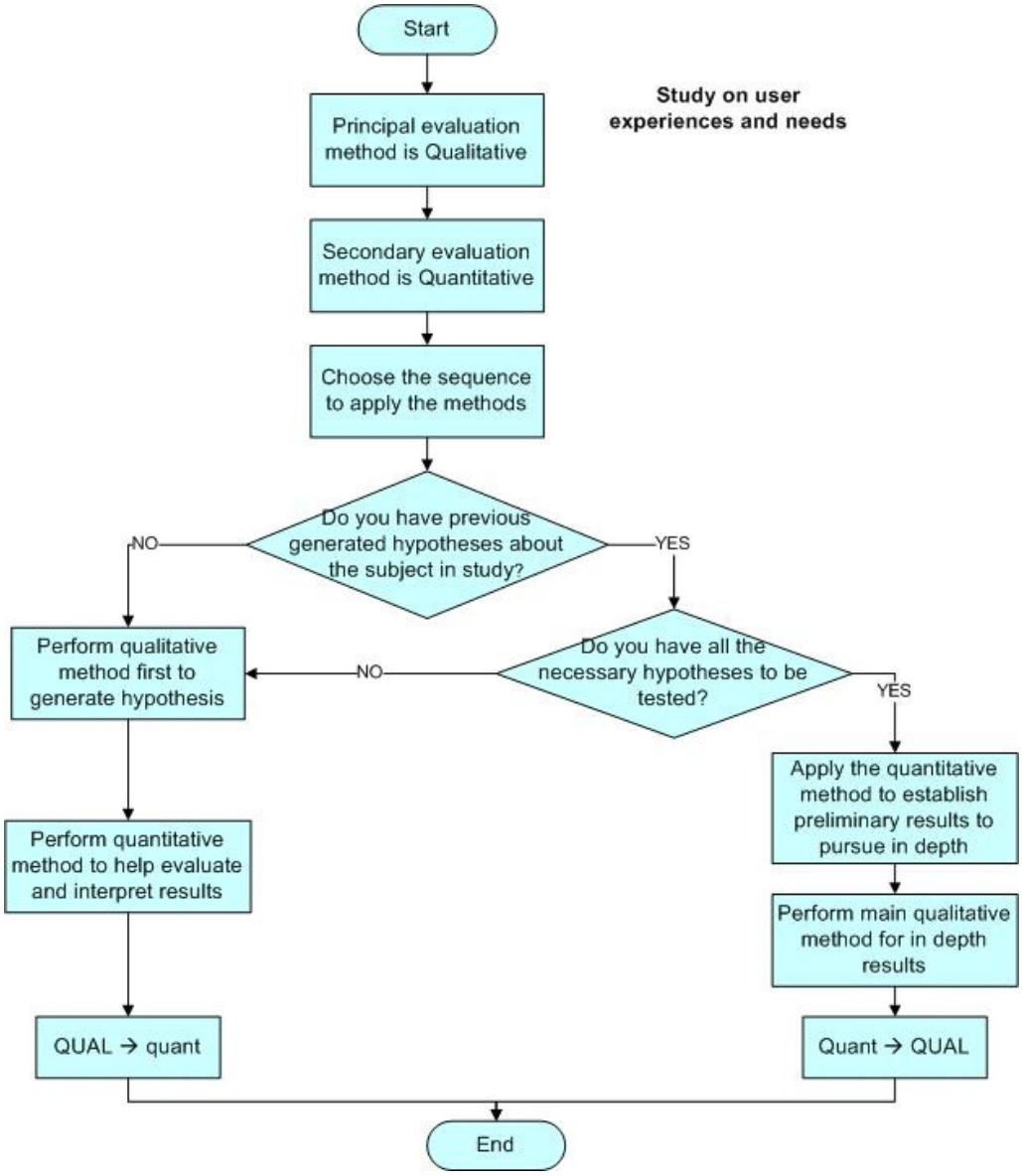

Figure 3.2 – Flowchart describing the process to choose how to apply mixed methods when studying user needs and experiences about a specific subject.

According to the priority-sequence model presented in Table 3.4 and the research objectives of this work, a smaller quantitative study was chosen to evaluate and interpret the results from a larger qualitative study (last row of Table 3.4 - QUAL→quant). The quantitative method provides a means to expand on what was learned through the main qualitative study. The classic use of this design is to explore the generalisability or transferability of conclusions from the qualitative research. Even a small quantitative follow-up can typically cover a much larger sample or range of setting than were present in the initial, in-depth qualitative research [52].

3.4.1 Literature review

In order to understand better how and why Focus Groups (FGs), as a qualitative method, have been applied in research, two literature reviews were made in the IEEE and Medline databases. One review ($review_A$) studied the application of FGs in generic information technology (IT) domains. The information collected for each article included: year of publication; type of IS evaluation; number of FGs applied; objectives and results for the study; types of data collection and analysis; and other evaluation methods that were applied to the same study either before or after the FGs' application.

Figure 3.3 shows the method used to achieve this review.

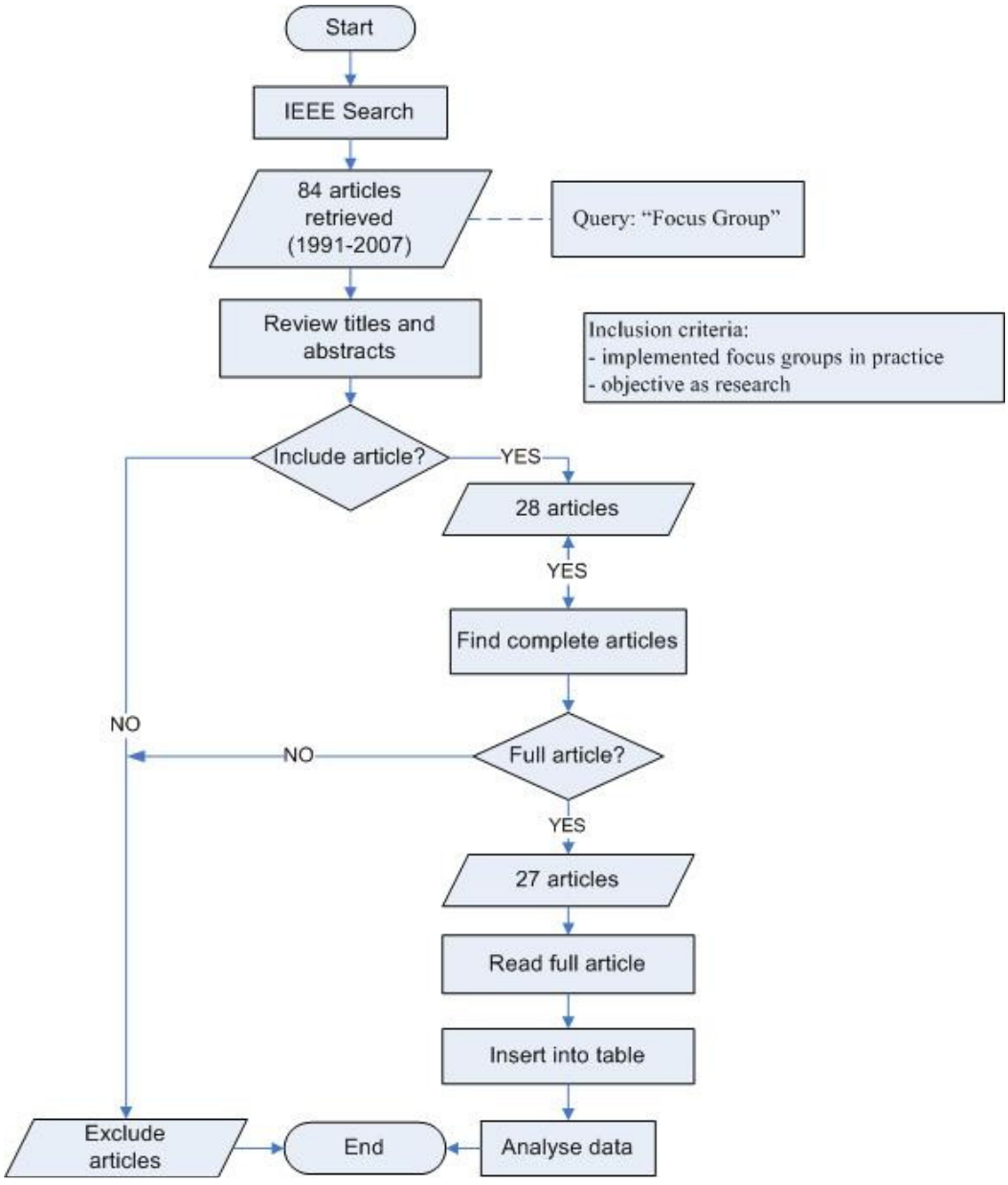

Figure 3.3 – Search method in IEEE database for $review_A$.

The second review ($review_B$) focused on a more specific domain. It consisted of published material concerning FGs applied to evaluate or analyse EMR. The information collected for each article included: year of publication; type of study participants; number of FGs applied; the use of segmentation (division of participants by common characteristics, for example: gender, age or professional category); the main results for the study; types of data collection and analysis; and other evaluation methods that were applied to the same study either before or after the FGs' application. The same procedure as presented in Figure 3.3 was used and the resulting numbers were: 40 articles were retrieved from the Medline Database with the following query: "focus groups"[Mesh] AND "Medical Records Systems, Computerized"[Mesh]. The titles and abstracts were reviewed according to the inclusion criteria (i.e., performed FGs in practice and had the main objective of doing research). 27 articles were selected but only 13 full articles were found and included within $review_B$.

3.4.1.1 $Review_A$: results

27 articles were included within this review. Table 3.5 shows the yearly distribution of the reviewed articles. Most published articles refer to the last two years where a search was made. This means that FGs are increasingly being applied to evaluate ISs in a diverse range of areas, not only social sciences or marketing research.

Table 3.5 – Number of generic IT articles reviewed by year of publication.

Year of publication	2007	2006	2005	2004	2003	2002	2001	1999	1997	1996	1993
No of articles	7	5	2	4	1	1	2	1	1	2	1

Of the 27 analysed studies/articles, 12 studies used one FG, 2 studies used two FGs and 4 studies used three FGs. Three studies resulted in improvements to the systems being evaluated while 14 ended in the achievement of the proposed goals. In terms of data analysis, 11 studies referred to the use of themes' categorization by relevance while only one mentioned the use of GT and of a specific software application to analyse the collected data.
Table 3.6 shows the other evaluation methods that were used within the same studies where FGs were applied. Most methods are applied before the FGs, but questionnaires and surveys are similarly applied before and after the FGs. FGs are usually used in conjunction with other methods so that more diverse and richer information is gathered.

Table 3.6 – Evaluation methods used before or after the application of FGs.

Evaluation methods	Before the FG	After the FG
Interviews	4	-
Observation	2	1
Questionnaires/surveys	5	4
Case study	-	2
TOTAL	**11**	**7**

3.4.1.2 Review$_B$: results

13 articles were included within this review. Table 3.7 shows the yearly distribution of the reviewed articles.

Table 3.7 – Number of EMR articles reviewed by year of publication.

Year of publication	2007	2005	2004	2003	1998
No of articles	1	2	6	2	2

Of the 13 articles reviewed, 6 analysed the attitudes, experiences and opinions of clinicians, physicians and health personnel about: EMR usability (3), new EMR development (2) and comparison between technologies (1); 3 articles analysed issues in relation to patients about: EMR usability (1), the use of medical records for research (1) as well as other needs in terms of ambulatory care (1); and 4 of them analysed both HCPs and patients' attitudes in regard to EMR about: usability (2), new EMR development (1) and a change of a medical discipline (1). The most common number of FGs applied was two FGs (4), one FG (3) and three FGs (2). Five studies specified the use of segmentation within their FGs. The researchers responsible for the FGs' studies divided the groups mostly by professional category and gender. Regarding the results obtained, 4 studies mentioned that improvements were made to the evaluated EMR while 8 resulted in important information being obtained that was analysed to benefit the systems in the study. In terms of data analysis, 6 studies referred to the use of themes' categorization by relevance while only 2 mention the use of GT to analyse the collected data.

Table 3.8 shows the other evaluation methods that were used within the same studies where the FGs were applied.

Table 3.8 – Evaluation methods used before or after the application of FGs.

Evaluation Methods	Before the FGs	After the FGs
Interviews	8	3
Observation	2	2
Questionnaires/surveys	1	-
TOTAL	**11**	**5**

Most methods are applied before the FGs, but observational studies are similarly applied before and after the FGs. Again, FGs are usually used in conjunction with other methods so that more information is gathered.

3.4.2 Selected methods

3.4.2.1 Generic issues

In order to evaluate the generic issues (i.e., legislation, regulations and standards) that were mentioned at the beginning of this chapter, and relate them directly to the access control process in healthcare, a search and subsequent analysis of the existing American legislation and European recommendations for legislation on the protection of healthcare information was performed. Further, a similar analysis was performed for the existing standards for healthcare information security and access control. This was done using a document analysis methodology that focused on finding the issues that mainly related to the access control of healthcare information. This generated a list of access control rules that came directly from these documents. Chapters 4 & 6 of this thesis present the results of this analysis.

3.4.2.2 Specific issues

To evaluate access control specific issues related mainly to the end users of EMR, the reviews presented in Section 3.4.1 showed that most published studies, with similar objectives to this research (i.e., trying to capture attitudes and opinions of both HCPs and patients about some healthcare domain characteristic), chose both qualitative and quantitative methods to gather the data. These methods included structured interviews or questionnaires as well as FGs [55-62]. Therefore, the most appropriate evaluation methods to achieve the objectives of this research in accordance with the chosen follow-up complementary design where the principal research method is qualitative (last row of Table 3.4) are firstly FGs and secondly Structured Questionnaires.

1. **Focus Groups** – the main objective of FGs is to gather opinions and experiences related to specific topics. This is obtained through sampling groups of individuals (6 to 8 people) of the required population who meet to discuss among each other about the set of topics. The discussion can last from one to two hours and is guided by a skilled moderator who records the discussions. The data is analysed in a qualitative manner, ideally using GT.

2. **Structured Questionnaires** – these are questionnaires with groups of questions organized in a specific order. A sample of the population is selected and the questions are either applied face to face or completed by the participants in their own time. The

questions can be refined and oriented to focus on specific topics for example, they can be based on previously obtained information such as from FGs' discussions. Data is analysed quantitatively.

In this specific research scenario, the chosen research methods start from generic perspectives in order to formulate categories about access control and then select those categories that are appropriate or generate new ones. The application of FGs before any other method can provide a generic idea about the topic, namely what the HCPs feel and think about access control, how important it is for them and how it should be implemented in order to facilitate their work. Well organized FGs can generate many ideas and information that would never be possible to obtain from questionnaires or other evaluation methods. After the application of FGs, the researcher will be better prepared to use other methods such as observation or interviewing to generate deeper problem solving knowledge.

From the information generated by the FGs, the questions for the structured questionnaires can be more focused on the specific issues that came up during the FGs' discussions and are important to explore in more depth. The questions will have a specific order and will guide the interviewee in an organized and meaningful way, allowing easier data analysis and subsequent processing by the interviewer.

The application of these two research methods will provide a more complete collection of data and will help to achieve the main objectives of this research. Chapter 5 of this thesis presents the results from the application of the chosen mixed methods.

3.5 Discussion

Complementarity is a concept that integrates mixed methods or several types of methods in order to collect and analyse different types of data so that the strengths of each method is enhanced. Further, what is learned from one method can be used and applied to the next one. The choice of different research methods that integrate both qualitative and quantitative data offer a richer and more complete way of collecting data about the subject of study. It is common in healthcare studies to use this kind of methodological approach to evaluate health related problems, but it can also be useful to apply this approach in more technical fields such as security and the development of healthcare security systems. This research is interested in the implementation of access controls and the problems this causes. Mixed methods will therefore help in pursuing this research.

4 LEGISLATION AND STANDARDS: REVIEW & ANALYSIS

4.1 Introduction

The increase in data collection and processing and the availability of health ISs, coupled with the high sensitivity of medical data stresses the need for data regulation and protection. This chapter reviews the existing standards in information security, healthcare and access control that can be used as guidelines in the later part of this research.

The list of access control rules extracted from the standards that are described in the next section (Section 4.2) is presented in Section 6.3.2, in Table 6.4.

This chapter also presents an analysis of the existing legislation, both American and European, regarding access control to medical data. At the end of this chapter (Section 4.4) is presented a list of legislative access control rules that were extracted from the analysis performed in Section 4.3.

4.2 Standards for information security and healthcare

Standards are an important means of guidance to design, develop and implement correct, secure and meaningful healthcare ISs. This section presents some highlights of standards that must be considered when developing such a system.

4.2.1 Comprehensive guidance for information security management

The International Organization for Standardization (ISO) released its first information security management standard, called Code of Practice for Information Security Management - ISO/IEC 17799:2000 [63]. It was based on the British standard BS7799 Code of Practice for Information Security [64]. The first updated version of ISO/IEC 17799 was released in 2005 and in 2007 it was renamed to ISO/IEC 27002:2005 Information technology - Security techniques - Code of Practice for Information Security Management [13]. The main objective of this standard is to provide guidance for managing information security, for both IT systems as well as information assets. There are 15 sections in the standard but the most relevant are the following: 4 – Risk assessment and treatment; 5 – Security policy; 6 – Organization of information security; 7 – Asset management; 8 – Human resources security; 9 – Physical and environmental security; 10 – Communications and operations management; 11 – Access control; 12 – ISs acquisition, development and maintenance; 13 – Information security incident management; 14 – Business continuity management; 15 – Compliance.

In more detail, the topic related to access control (Section 11 of the standard) focuses on Business requirements for access control; User access management; User responsibilities;

Network access control; Operating system access control; Application and information access control; and Mobile computing and teleworking.

Specific to the healthcare environment, ISO 27799:2008 [65] defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002. ISO 27799:2008 specifies a set of detailed controls and best practice guidelines to manage health information security. By implementing this International Standard, healthcare organizations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organizations' circumstances that will maintain the confidentiality, integrity and availability of personal health information whatever the form (words and numbers, sound recordings, drawings, video and medical images), whatever means are used to store it (printing or writing on paper or electronic storage) and to transmit it (by hand, fax, over computer networks or by post).

4.2.2 Health informatics' security standards

TC251 is the Technical Committee of CEN (European Committee for Standardization) that develops standards for the domain of healthcare informatics [66]. CEN and ISO work very closely together and the activities of CEN/TC251 mirror to some extent the working groups of ISO TC215 for the domain of health informatics [67]. CEN/TC251 is divided into 4 working groups: WG1 – Information Models; WG2 – Terminology and knowledge representation; WG3 – Security, safety and quality; WG4 – Technology for interoperability. There are nine working groups belonging to ISO TC215 and these are displayed in Figure 4.1.

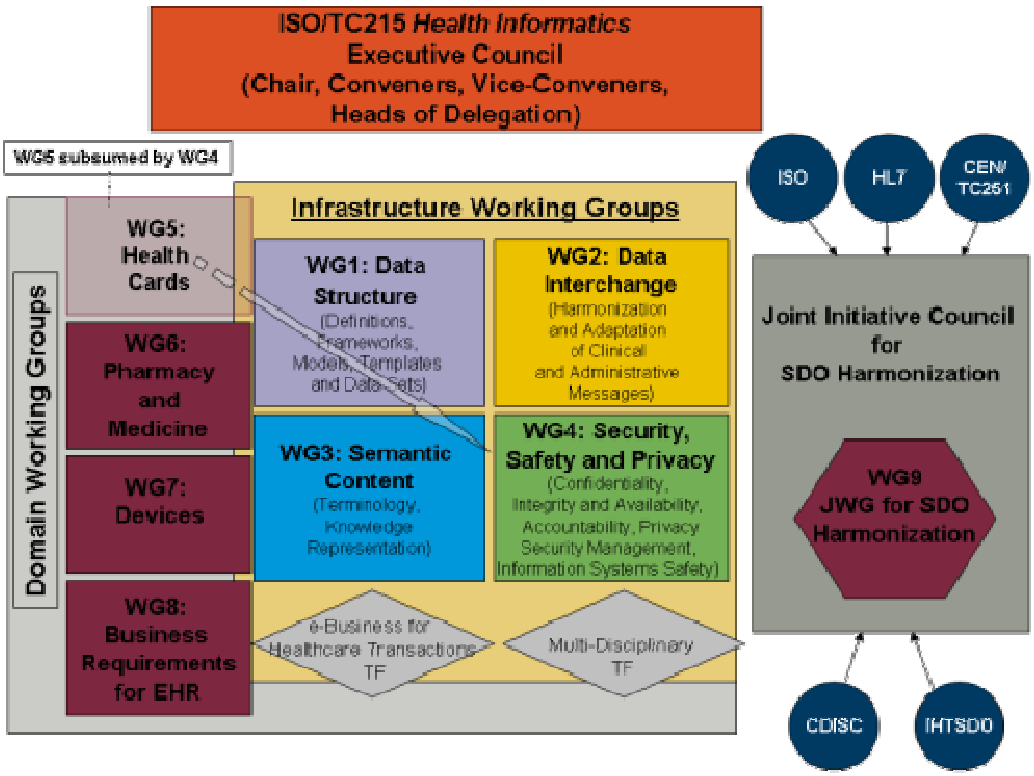

Figure 4.1 – ISO TC215 - 9 Working Groups. (Picture taken from http://sl.infoway-inforoute.ca/content/dispPage.asp?cw_page=infostand_ihisd_isowg1_e).

WG3 of CEN/TC251 is similar to WG4 ISO TC215 [67]. Output from WG3 (Security, safety and quality) includes the following standards: EN 12388 – Algorithm for digital signatures services in healthcare; EN 12924 – Security categorisation and protection for healthcare ISs; EN 13608 – Security for healthcare communication (Part 1 – Concepts and terminology; Part 2 – Secure data objects; Part 3 – Secure data channels); EN 12251 – Secure user identification – management and security of authentication by passwords [68]; EN 13729 – Secure user identification – Strong authentication using smartcards. Output from WG4 of CEN/TC251 (Technology for interoperability) contains an important standard for security: EN 13606-4 Electronic health record communication – Part 4: Security [69].

There is a range of health informatics' standards that can help in the design, development, and implementation of health ISs. These can be a set of useful guidelines and a good starting point for the implementation of secure and structured health ISs, allowing for easier integration and better communication among them.

4.2.3 Access control standards in healthcare

There are generic standards that define a framework for access control. ISO/IEC 10181-3:1996 – Access Control Framework (ACF) [70] is one of them. This framework supports access control in both standalone and networked systems and defines four roles for

components participating in an access request: Initiators, Targets, Access Control Enforcement Functions (AEFs) and Access Control Decision Functions (ADFs). Initiators submit access requests. An access request specifies an operation to be performed on a Target. The AEF mediates access requests. The AEF submits a decision request to the ADF. A decision request asks whether a particular access request should be granted or denied. The ADF decides whether access requests should be granted or denied (Figure 4.2).

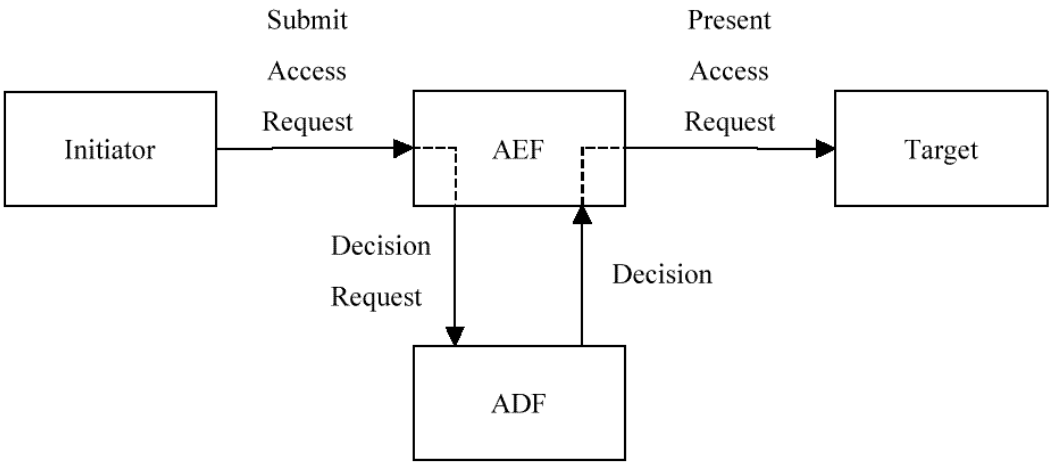

Figure 4.2 – Access Control Framework (ACF) from standard ISO/IEC 10181-3.

Inputs to an ADF show the access control decision information (ADI) an ADF uses to make an access control decision. This is where access control policies are checked as well as contextual information and constraints (Figure 4.3). Retained ADI is information from previous decision requests that might be useful for the unsent decision request (e.g., how many previous requests of this initiator were granted or denied).

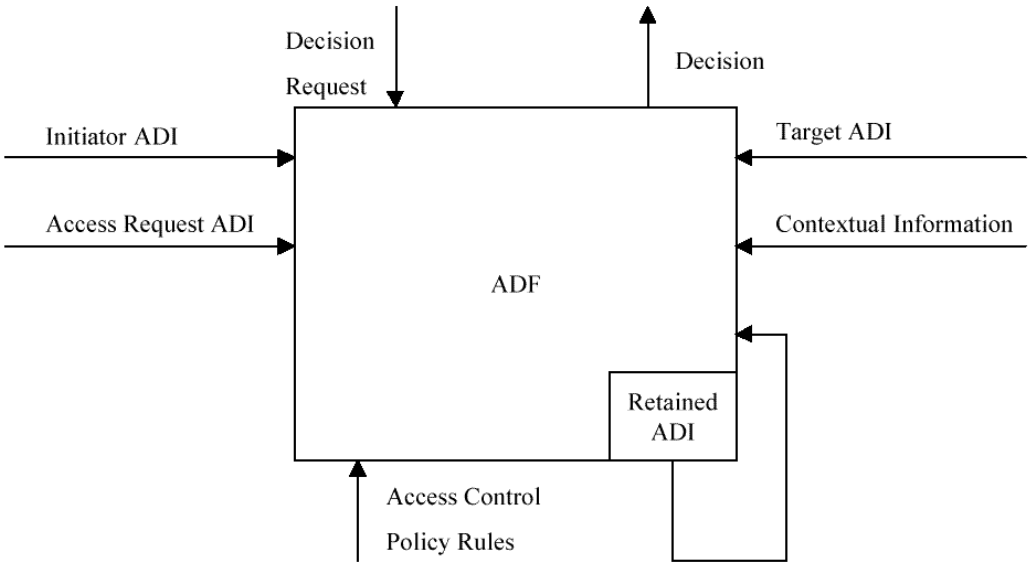

Figure 4.3 – Inputs to an ADF.

There are also some standards specific to healthcare that focus on access control and guide the development of access control systems in the healthcare environment. EN 13606-4 is a standard that focuses on the security of electronic health record communications and in the issues involved in the communication of EMR within and across organisational boundaries [69]. These characteristics stress and challenge the security needs involved in such environments. Access control is a central piece in those needs; to provide for patients' privacy, each part of a patient's medical record should be capable of being associated with an access control policy that defines the rights to access that record. Furthermore, emergency or unanticipated situations that require access to the information on a 24/7 basis must also be available and controlled.

This European standard [69] does not define the access control rules to be used. These are set according to legislation, institutional requirements as well as a system's characteristics, end users and so can constitute the access control policy to be used for that system. This standard defines generic guidelines to be used in order to specify the access control policy that might relate to any particular EMR authored by the patient or representatives.

As part of WG4 of ISO TC 215 (Figure 4.4), the ISO Privilege Management and Access Control (PMAC) standard (ISO/TS 22600) [71] defines a generic model for the representation of a RBAC policy and the negotiation process that is required to get to an access decision. It defines how permissions are assigned to roles.

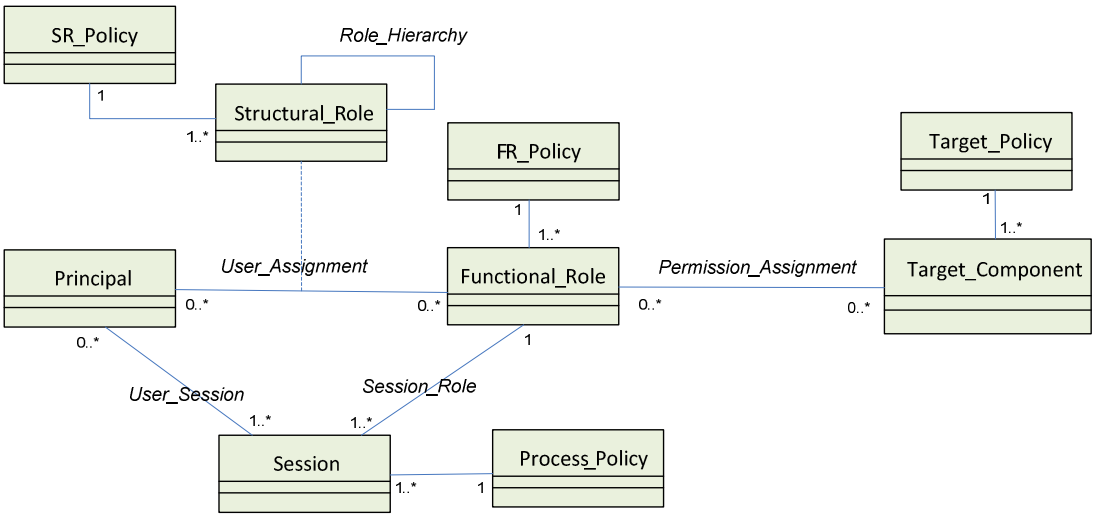

Figure 4.4 – Key concepts of RBAC as defined in the PMAC standard.

Principals are mapped to one or more functional roles that can be influenced by the structural roles they may hold. A doctor may, for example, hold one or more structural roles (consultant paediatrician or head of child screening for the region). These roles may permit him/her to act

with a different functional role than the one he/she usually uses. Functional roles are mapped to permissions to perform specific actions to some objects.

For each EMR record component, several sensitivity values and levels are defined. These are shown in Table 4.1.

Table 4.1 – Sensitivity levels for each record component.

Data Sensitivity value	Sensitivity level	Who can access the record component
Personal care	5	One or two other people trusted by the patient
Privileged care	4	Restricted to a small group of people caring intimately for the patient
Clinical care	3	Normal clinical care access
Clinical management	2	Wide range of personnel not all of whom are actively caring for the patient
Care management	1	Wide range of administrative staff

Each person requesting access to an EMR component should have one of the functional roles that are presented in Table 4.2.

Table 4.2 – List of functional roles.

Functional Role	Brief Description
A. Subject of care	Principal data subject of the EMR
B. Subject of care agent	e.g., parent, guardian, carer or other legal representative
C. Personal healthcare professional	Healthcare professionals that are closest to the patient
D. Privileged healthcare professional	Nominated by the subject of care OR nominated by the healthcare facility
E. Healthcare professional	Party involved in providing direct care to the patient
F. Health-related professional	Party indirectly involved in patient care, teaching, research
G. Administrator	Any other parties supporting service provision to the patient

When the system needs to reach an access decision it should use a table similar to Table 4.3. This table defines the basis for how sensitivity levels and functional roles can be mapped. Access permissions are associated accordingly for each specific functional role the information requester may have.

Table 4.3 – Mapping of functional roles to sensitivity levels.

	Record component sensitivity				
Functional role	Care Management	Clinical Management	Clinical care	Privileged care	Personal care
A	Y	Y	Y	Y	Y
B	Y	Y	Y	Y	Y
C	Y	Y	Y	Y	Y
D	Y	Y	Y	Y+	++
E	Y	Y	Y		
F	Y	Y			
G	Y				

NOTE 1 – Y indicates access will be granted unless dictated by other policy constraints

NOTE 2 - + indicates access will be granted if the EMR requester is a member of the same specialty or clinical service in which the record component was created. This access may also be granted in healthcare emergency situations if so authorized.

NOTE 3 - ++ indicates that access to Personal care information may sometimes be granted by mandate to Privileged healthcare professionals in some care settings.

The annex A of the standard [69] provides diagrams that represent access control examples and how simple policies can offer a flexible way of managing access to EMR data. Figure 4.5 represents the example of a nurse (Helen) that works in a sexual health clinic, having the functional role of Privileged healthcare professional.

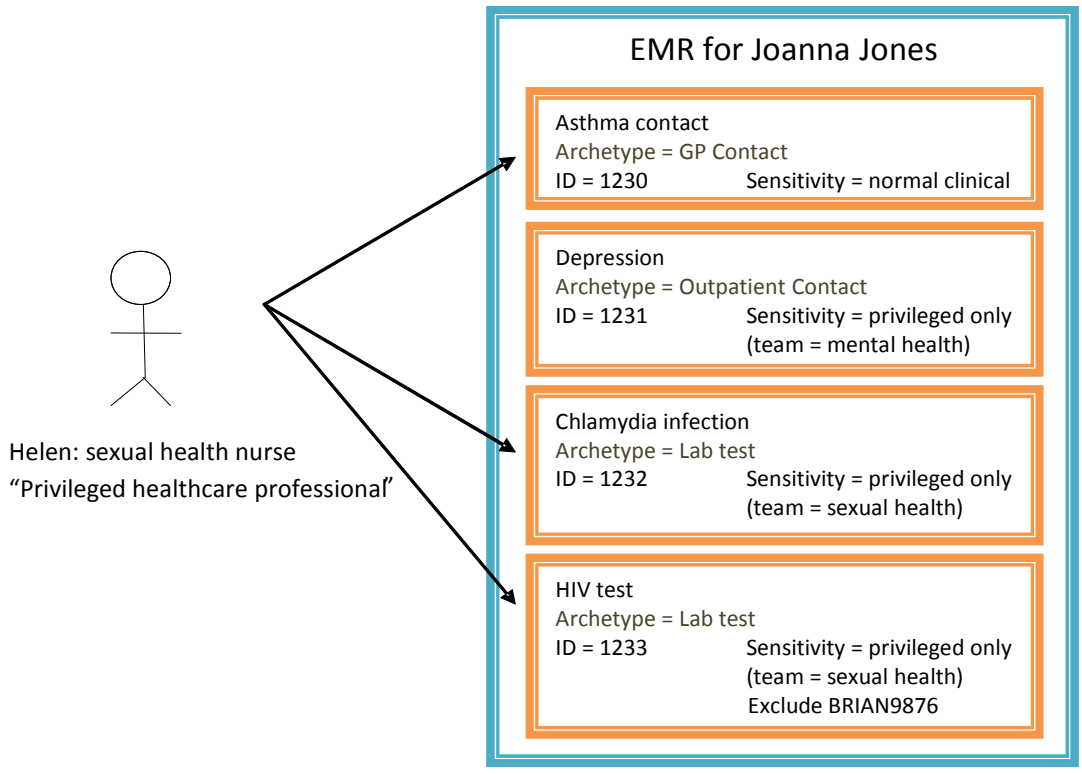

Figure 4.5 – Example of an access control case.

Helen is able to see normal clinical records and sexual health records of the patient Joanna Jones. However, she is not able to access other privileged care information such as mental health, unless she is a member of the same specialty or clinical service. So she is not able to access the record related to the diagnosis of depression.

In conclusion, the standards and examples presented here are access control guidelines that can serve as a starting point to define an access control policy within a healthcare environment and are flexible and generic enough in order to be adapted to the characteristics and requirements of a specific healthcare institution.
The access control rules extracted from this section (Section 4.2) are presented in Section 6.3.2, in Table 6.4.

4.3 Legislation

In 1996 the Health Insurance Portability and Accountability Act (HIPAA) was defined and later enforced in the United States of America in April 2003 as a federal law that establishes standards for the privacy and security of health information as well as standards for electronic data interchange (EDI) of health information. HIPAA has two main goals: making health insurance more portable when persons change employers and making the health system more accountable for costs in order to reduce waste and fraud [72].

In Europe, the 1997 European Recommendation on the Protection of Medical Data by the European Committee focuses on ensuring the proper safeguard and management of the confidentiality, integrity and availability of personal medical data [73]. Member states are bound to take proper steps to ensure that this recommendation is followed and put into practice since each member state must define specific legislation that follows the European Recommendations.

Seven years later, in 2004, the European Committee approved another recommendation, this time focusing on the use of new technologies in healthcare, such as the Internet, and the way these technologies can impact medical data collection, processing and access [74]. This recommendation paved the way for citizens to participate in the collection of and access to their health information by creating a regulated basis for patient empowerment [75].

Legislation and regulations that define the protection of medical data are available in most European countries. European member states are bound to protect medical data and individuals' privacy but how successful are they in pursuing these objectives? Have the regulations been translated into the daily processes and practice of healthcare institutions so that the medical data

that they keep on millions of patients is handled in accordance with the principles needed to safeguard patients' privacy?

In fact, research shows that excessive regulation can create a barrier for physicians when treating patients because these regulations have diverted the time and resources of physicians away from patient care into the many directives that are needed to intervene between physicians and the care of their patients on a daily basis [76]. Another review that analyses the benefits and barriers to the implementation of EMR claims that legislation can be one of those barriers. Too many rules can prevent good healthcare treatment as resources that should be used for treatment are instead spent on administration [77]. Other research shows that it can take longer than 21 days to complete the process of patients requesting access to their medical records [78]. Patients must first fill in a written form in order to request the needed information and then, depending upon the healthcare institution, there can be a lengthy and sometimes complex process between this request and the provision of a copy of their medical record. However, according to American legislation, patients must have free and easy access to their medical records. But it is common for American citizens to have to pay some fee in order to get a copy of their medical records within US hospitals. The authors of another review argue that EMR can help solve the problem of giving patients access to their own records, inexpensively and in a format more likely to be more useful than paper based records [79].

The following sections present the main regulations regarding healthcare information in both the United States and Europe with a specific focus on security and access control. They highlight and summarize some specific parts of the healthcare recommendations and legislation [73, 74] that relate mainly to HCPs' responsibility, patient rights and consent as well as security and access control to medical data.

4.3.1 HIPAA

HIPAA includes the definition of four health information standards and four associated sets of regulations [72]:

- Standardized formats for all computer-to-computer information exchanges
- Standardized identifiers for health providers, health plans and (maybe) patients
- IS security standards
- Privacy standards

The Administrative Simplification standards adopted by Health and Human Services (HHS) under the HIPAA Act of 1996 apply to any entity that is

- a health care provider that conducts certain transactions in electronic form (called here a "covered health care provider")

- a health care clearinghouse
- a health plan

An entity that is one or more of these types of entities is referred to as a "covered entity" in the Administrative Simplification regulations.

This section presents the specific parts from HIPAA that relate to the HCPs' responsibility, patient rights and consent as well as security and access control to medical data.

4.3.1.1 Healthcare professionals' responsibility

Sec. 1177 (a) OFFENSE – A person who knowingly and in violation of this part [80]:

(1) uses or causes to be used a unique health identifier;

(2) obtains individually identifiable health information relating to an individual; or

(3) discloses individually identifiable health information to another person,

shall be punished;

HIPAA privacy rule – Provision of access – Who may exercise the right of access? [81]:

- *Verification*: the privacy rule requires covered entities to develop and implement reasonable policies and procedures to verify the identity of any person who requests protected health information (PHI).

4.3.1.2 Patient rights and consent

HIPAA privacy rule [81]:

An individual's right to access his/her PHI is a critical aspect of the Privacy Rule, the application of which naturally extends to the electronic environment. The privacy rule establishes, with limited exceptions, an enforceable means by which individuals have a right to review or obtain copies of their PHI, to the extent it is maintained in the designated record set(s) of a covered entity.

Timely action

The privacy rule requires covered entities to respond to requests of access to medical records in a timely manner. Except as otherwise specified, the privacy rule requires the individual to be notified of the decision within 30 days of the covered entity's receipt of the request.

Provision of access – Who may exercise the right of access?

- *Individuals and personal representatives*: while the privacy rule's right of access belongs primarily to the individual who is the subject of the PHI, the privacy rule also generally requires that persons who are legally authorized to act on behalf of the individual regarding health matters be granted the same right of access.

Provision of access – content – designated record sets:

An individual's right of access generally applies to the information that exists within a covered entity's designated record set.

Denial of access – grounds for denial

The privacy rule contemplates circumstances under which covered entities may deny an individual access to PHI. It also distinguishes between those grounds for denial that are reviewable from those which are not.

4.3.1.3 Security and access control

Sec. 1173. (d) (2) SAFEGUARDS – each person described in Section 1172 (a) who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical and physical safeguards [80]:

(A) to ensure the integrity and confidentiality of the information;

(B) to protect against any reasonably anticipated:

i. threats or hazards to the security or integrity of the information;

ii. unauthorized uses or disclosures of the information; and

(C) otherwise to ensure compliance with this part by the officers and employees of such person;

HIPAA privacy rule – Requests for access [81]:

The privacy rule allows covered entities to require that individuals make requests for access in writing, provided they inform individuals of such a requirement.

4.3.2 Rec. No. R(97) 5 – on the protection of medical data

This recommendation [73] describes that where the data subject (patient) is required to give his/her consent to process and use their medical record, this consent should be free, express and informed.

Medical data must be collected and processed fairly and lawfully and only for specified purposes. These purposes must be defined before the data is processed and if any change is to be done, it must be communicated to the patient. This is also valid for the purpose of scientific research (Appendix A, item 12). Whenever possible, data should be used anonymously. If this is not possible then the patient or a representative must give his/her informed consent.

An extract with more detailed access control and security issues that is specified in this recommendation is presented in Appendix A.

4.3.2.1 Healthcare professionals' responsibility

HCP's or individuals or bodies working on behalf of HCPs must be responsible for collecting and processing medical data. The latter must be subject to similar rules of confidentiality incumbent on HCP. More details in Appendix A, items 3, 4 and 7.

4.3.2.2 Patient rights and consent

The patient must be informed of all the information that exists in relation to his/her medical record as well as the identity of who is processing that information together with the purpose and type of data that is being collected.

In terms of accessing their medical records, every person shall be enabled to have access, either directly or through a HCP or, if permitted by domestic law, a person appointed by him/her. The information must be accessible in understandable form.

In defined situations, access to medical data from patients may not be allowed. If this is the case then it must be detailed why and in which circumstances this is being done. It must be possible for patients to correct data concerning him/her and, in case of refusal, he/she shall be able to appeal.

More details in Appendix A, items 5, 6 and 8.

4.3.2.3 Security and access control

Appropriate technical and organizational measures shall be taken to protect personal data against accidental or illegal destruction, loss, as well as against unauthorized access, alteration, communication or any other form of processing.

In order to ensure, in particular the confidentiality, integrity and accuracy of processed data as well as the protection of patients, measures must be implemented to ensure an appropriate level of security that conforms with the sensitive nature of medical data. More details in Appendix A, items 7 and 9.

Besides legislation enforcement, internal legislation as well as institutional rules and procedures must also be defined and applied in order to be adapted according to the healthcare institution needs and workflows.

4.3.3 Rec. No 17 (2004) – on the impact of information technologies on health care – the patient and Internet

The advantages and disadvantages of the Internet should be made clear to the patients, users and/or their carers. These must be aware that the Internet has many limitations and in itself does not produce any new medical evidence or any guarantee of data quality. Failure to make known these limitations is unethical and infringes the autonomy of the individual. In order to

protect the patients, education and other learning opportunities must be available by developers for the Internet users [74] (Appendix B, Items I and II).
An extract with more detailed access control and security issues that is specified in this recommendation is presented in Appendix B.

4.3.3.1 Healthcare professionals' responsibility

The correspondence between patients and health professionals must remain private and protected at all times. The providers or final owners of the information, communication and health services must be always identifiable.
More details in Appendix B, items 1-7, II and IV.

4.3.3.2 Patient rights and consent

Where necessary, policies, legislative and other measures necessary for developing a model framework for best practices regarding information technologies in health related matters should be adopted. The responsibility is becoming increasingly shared, with health professionals maintaining their responsibility, but patients taking on more responsibility for the choice of means, and of personal responsibility through self-care and self-management.
More details in Appendix B, items I, X and XI.

4.3.3.3 Security and access control

Policies, legislation and best practices must exist in order to restrict or control patient access to information and services via the Internet and other communications media. The measures to protect confidentiality and privacy should guarantee the right of citizens to self-determination and therefore provide a legal basis for data processing on the grounds of consent, contract or law. More details in Appendix B, items IV and XI.

4.3.4 Code of ethics for health information professionals

Apart from the deontological code that HCPs are bound to follow, for example, doctors have their own code [82], which advises them about ethical principles that regulate the privacy and dignity of the patients, the International Medical Informatics Association has created a code of ethics for health information professionals [83] in order:

1. to provide ethical guidance for the professionals themselves;
2. to furnish a set of principles against which the conduct of the professionals may be measured; and
3. to provide the public with a clear statement of the ethical considerations that should shape the behavior of the professionals themselves.

Unquestionably, the law provides the regulatory setting in which healthcare information professionals carry out their activities. However, ethical conduct frequently goes beyond what the law requires. On the other hand, a Code of Ethics for Healthcare Information Professionals is grounded in fundamental ethical principles as these applied to the types of situations that characterize the activities of the health informatics specialist. Some of the principles of this code are presented next.

4.3.4.1 Healthcare professionals' responsibility

Principle of Accountability: Any infringement of the privacy rights of the individual person, and of the right to control over person-relative data, must be justified to the affected person in good time and in an appropriate fashion.

4.3.4.2 Patient rights and consent

Principle of Information-Privacy and Disposition: All persons have a fundamental right to privacy, and hence to control over the collection, storage, access, use, communication, manipulation and disposition of data about themselves.

4.3.4.3 Security and access control

Principle of Security: Data that have been legitimately collected about a person should be protected by all reasonable and appropriate measures against loss, degradation, unauthorized destruction, access, use, manipulation, modification or communication.

Principle of Access: The subject of an electronic record has the right of access to that record and the right to correct the record with respect to its accurateness, completeness and relevance.

Principle of Legitimate Infringement: The fundamental right of control over the collection, storage, access, use, manipulation, communication and disposition of personal data is conditioned only by the legitimate, appropriate and relevant data-needs of a free, responsible and democratic society, and by the equal and competing rights of other persons.

4.4 Legislative access control rules

Legislation and regulations need to be put into practice. In order to include them within access control policies a list of legislative access control rules was extracted from the legislative recommendations (Section 4.3) and is presented below.

Although some are very generic, these rules constitute some of the access control rules and procedures that must be included within any final access control policy with the necessary adjusts according to the needs and workflows of the institution.

L.1 Patient consent must be sought where required.

L.2 Medical data collection and processing purposes must be defined before they are performed (it includes scientific research). Any changes in the original purposes mentioned must be communicated to the patient.

L.3 Medical data should only be collected and processed by HCPs or individuals or bodies working on behalf of HCPs.

L.4 Every person shall be enabled to have access to his/her medical data either directly or through a HCP.

L.5 If the domestic law permits, a patient may appoint a person to access his/her medical data on his/her behalf.

L.6 Patients may ask for their medical data to be corrected.

L.7 Access to medical data by patients may be refused, limited or delayed under some specific circumstances (i.e., defined by the HCPs).

L.8 Appropriate measures must be available to protect against unauthorized access.

L.9 It must be possible to prevent the unauthorised consultation of processed personal data.

L.10 It must be possible to prevent automated data processing systems from being used by unauthorised persons by means of data transmission equipment.

L.11 It must be possible to enable the separation of: identifiers and data relating to the identity of persons; administrative data; medical data; social data and genetic data (access control).

L.12 It must be possible to guarantee the possibility of checking and ascertaining to which persons or bodies personal data can be communicated by data transmission equipment.

L.13 It must be possible to guarantee that it is possible to check and establish a posteriori who has had access to the system and when.

L.14 Providers of information, communication and health services should under all circumstances be identifiable including final owner or provider.

L.15 There must exist policies, legislation and practices that fundamentally restrict, control or hamper patient access to information and services via the internet and other communication media.

L.16 Recommendations are made to also include internal legislation and institutional rules according to the healthcare institution.

4.5 Discussion

The healthcare environment is a very complex environment. It is not always possible to compare it to banking, commerce or even the government where data is also very sensitive. The healthcare environment deals with people's lives everyday, only occasionally do the other domains involve matters of life or death. Besides all the technological advances, healthcare is about humans taking care of and providing for other humans using medical data. It is difficult to control, enforce and ensure that all processes are as they should be and human lives should not be compromised by badly performing systems. Still, efforts must be made to ensure that rules are obeyed.

Legislation and regulations should be made closer to human processes and daily needs and not the other way around. In an evolving and always changing environment, an interdisciplinary approach is needed that includes generic healthcare standards, generic and specific security standards, legal requirements, as well as the specific needs of users. The understanding of all these parties will provide for a better and more secure way of dealing with medical data.

This chapter helps in pursuing this goal by providing access control rules derived from both American and European legislation and regulations that can be modelled into the healthcare practice.

5 APPLICATION OF MIXED METHODS

5.1 Introduction

In real healthcare environments, access controls are often bypassed by users. In one study where three EMR log data were analysed, it was found that around 10% of the logins and passwords were shared among the workers [84]. It is clear in this case that access control policies were either not enforced or failed to take into account the needs of users and workflow complexities regarding these three systems. Therefore, users either needed or found it more convenient to share their identities in order to work with the system on a daily basis.

In order to define access control policies with rules that are closer to users' needs and daily experiences and to overcome scenarios like the one described above, while taking into account the research presented in the previous chapters, the use of mixed methods should provide insights into the subject of study (Section 6.2).

This chapter presents the mixed methods that were used to gather information about HCPs (Section 5.2) and patients' (Section 5.3) needs and experiences regarding access control to EMR. It also presents the results obtained from the application of the mixed methods and discusses them.

5.2 Healthcare professionals' perspectives on access control

The mixed methods used to gather information relating to HCPs' attitudes and opinions were Focus Groups (FGs) (qualitative analysis) and structured questionnaires (quantitative analysis).

5.2.1 List of discussion topics

Using the information reviewed in the previous chapters, the following list of discussion topics about HCPs views regarding access control to EMR was created. This list is important because it helps defining the FGs line of discussion.

5.2.1.1 Healthcare professionals' generic views on EMR

1. EMR takes time and effort to learn and use
2. EMR requires changes to the existing workflows
3. EMR cannot be customized
4. Most of the times HCPs do not know what they need from the EMR
5. The relationship between HCPs and patients can be affected
6. EMR is usually introduced without HCPs collaboration in the process
7. HCPs do not see any benefits in the short term and will not support its introduction
8. There are security issues that HCPs do not fully understand, and make them mistrust the system

5.2.1.2 Healthcare professionals' views regarding access control to EMR

1. HCPs usually rely on someone else to do access control for them
2. How do HCPs think access control should be with regard to:
   - 2.1 different types of roles for accessing EMR information
   - 2.2 patients having full access to their medical records
   - 2.3 a need for an override policy (e.g., BTG)
3. How would HCPs feel about a specific patient access control scenario

5.2.2 Focus groups

Focus groups are described as a qualitative method used to explore attitudes, opinions, thoughts and experiences of a specific group of people. They can be used at the beginning of a study in order to generate new hypotheses or theories about a theme, or they can be applied after other evaluation methods to focus on a specific issue that needs to be further analysed. When used at the beginning of a study, once the problem is defined, FGs can be useful to better prepare other subsequent studies such as observation or interviewing in order to solve the problem. Hence the key characteristic which distinguishes FGs from other evaluation methods is the insight and data produced by the interaction between participants of each group [85].

The use of FGs in research is not new. Merton and Kendall's [86] influential article on the focused interview set the parameters for the development of FGs. These were: ensuring that participants have a specific experience of or opinion about the topic under investigation; that an explicit interview guide is used; and that the subjective experiences of participants are explored in relation to a predetermined line of discussion.
FGs have a long history in market research [52], and in medical research [87].
As a source of knowledge, FG sessions are helpful in answering questions about how people behave and in particular why people behave as they do. The groups' situation may encourage participants to disclose behaviour and attitudes that they might not consciously reveal in a one-to-one interview situation. They may feel more comfortable in the presence of people who share similar opinions, attitudes and behaviour.

The need for qualitative methods such as FGs relies on the fact that public organizations are more aware that exclusive reliance on statistical information sometimes yields insufficient returns in terms of the effort invested to achieve socially desirable forms of behaviour. Furthermore, qualitative research is considered an important input for quantitative research [88]. FGs are a cost-effective and quick empirical research method that provides qualitative insight and feedback. It must however be used with sufficient empirical rigor [89].

Quantitative methods are also needed because FG data is not capable of producing typical or projectable information for the whole universe under study.

In conclusion, FGs should not be used as a stand alone evaluation method but need to be applied under a multiple method approach that comprises both qualitative and quantitative methods since every research method has its own limitations and advantages. A multiple methods approach is more capable of disclosing diverse dimensions of behaviour and attitudes [88].

5.2.2.1 Objective

The aim of this section is to apply FGs in order to evaluate the attitudes, experiences and needs of HCPs regarding access control to EMR. The literature review (Section 3.4.1) showed that FGs are commonly used to evaluate similar issues with good results, especially in medical research. However, no published material was found relating specifically to the study of access control issues in order to improve the definition of access control policies in the healthcare area. Consequently, this is a new area to apply this kind of methodology. The goal is ultimately to improve the development and implementation of access control to EMR, a key goal of this research.

Best practise guidelines for reporting the research procedure are given in [52]. Following these would improve the quality of the FG research. The best practise suggest that the following information should be published along with the results: the context of research and set of questions applied throughout the project; the number of FGs conducted as well as their size; the groups' composition including background data on the participants; the session duration; if the groups are segmented then information on the sampling strategy and the number of groups per segment; the sources for locating participants and other information about recruitment procedures; summaries of the questions made; and information about the type of moderation – how many moderators were used and the training they had.

5.2.2.2 Population

For this research, there was no previous data to direct the sampling of the FG participants. Consequently the "convenience sampling" strategy was used [90]. This is where participants are chosen from a convenient group of people. In this case, the selection of participants was made from postgraduate students at the Faculty of Medicine of the University of Porto. Students were chosen from the following Masters Courses: Medical Informatics; and Evidence and Decision in Healthcare; and from the Doctoral Program Clinical and Healthcare Services Research. Both HCPs and informatics' professionals are enrolled on the Masters courses, but only HCPs were selected and put into groups according to their

professional background. One of these groups however had HCPs with mixed backgrounds. The doctoral program only enrolls medical doctors and so these comprised one of the groups. The reason for grouping participants according to their professional backgrounds (i.e., segmentation) is that facilitates discussions because all the participants in a group have similar experiences and backgrounds, usually at the same level [52].

The HCPs were contacted and selected at the beginning of their courses (during their first lectures). They were gathered in a room without knowing that they were going to participate in a FG or what the topic of discussion was going to be.

5.2.2.3 Line of discussion

The list below presents the line of discussion that was followed by the moderator:

1. The participants were given the main theme to discuss and other information regarding the process that would be followed during the course of the FG.
   Each participant was asked to give their consent to participating.
2. Each participant was initially asked to give details about their profession and work location, as well as the use of EMR within their practice.
3. The participants were then asked to discuss the following amongst themselves:
   a. the use of paper records or EMR, what are the advantages or disadvantages of each
   b. access control issues in general
   c. access control mechanisms they use on a daily basis when accessing any system
   d. the problems and benefits of giving different access levels to different groups of users
   e. access control policies to EMR: who defines them, what should be improved

At the end of the session the participants were asked to give their opinions about the best access control solutions they think should be used in EMR.

5.2.2.4 Data collection and analysis

Data was collected by audio recording the whole conversations while the conversations of the third and fourth groups were also recorded with a video camera (Table 5.1).

Table 5.1 – Description of each FG data collection.

FG	Segmentation	Date & Time	Recording	Audio	Video	Moderators
FG1	Yes	11/01/2008 18h:20m	44m:28s	Y	N	2
FG2	Yes	11/01/2008 19h:20m	37m:22s	Y	N	2
FG3	No	21/02/2008 19h:00m	54m:44s	Y	Y	1
FG4	Yes	26/06/2008 19h:00m	40m:16s	Y	Y	1

Analysis was only done by one person. The discussions from each FG were transcribed into four separate word documents. Each document was then divided into smaller ones, containing only the dialogues belonging to each one of the participants, so that the data could be more easily related to a specific participant.

All documents were input into the qualitative analysis software, QSR NVivo 7 [91] and the coding was done using this tool to register and structure data in a more automatic way. The coding started after each FG document was generated and was done separately for each group. Discussion topics, categories and sub-categories that were generated from each group were not only used in the categorisation of subsequent group discussions but were also back categorised to the previous ones (where applicable).

The data analysis was based on the GT approach and performed in four phases (Figure 5.1). In the first phase, codes were generated from the data itself (in vivo coding), using a line-by-line coding strategy. This strategy consists in reading the whole text, line by line, identifying and underlining the key term phrases that are encountered. These codes comprise the core ideas that were found within the text: line-by-line coding (1) helps to identify gaps, define actions and explicate both actions and meanings, it also leads to developing categories [92]; shorter code phrases were developed from *in vivo* codes to capture the main ideas of the participants (2); code phrases were grouped together to create clusters (3); and clusters were labelled and grouped to create categories (4).

In a second phase, a more focused and structured coding was done and the codes were grouped into categories and sub-categories (5).

The third phase was based on axial coding where relations between categories and sub-categories became more visible and so they were organized as such (Figure 5.2): categories and sub-categories were sorted into a hierarchical tree (6); and core categories were identified (7). Phase 4 was customized and oriented to the objectives of this research and consisted in the generation of access control rules that could be integrated in an access control model. This phase included: the reduction of all categories to the most discussed sub-categories (8); the generation of insight sheets based on obtained support notes [90] for all FGs categories (9); and the generation of access control rules (10). In the end, these access

control rules are reduced to rules based on RBAC to be included in an Access Control Policy. Figure 5.1 represents the GT line of analysis for the FG data.

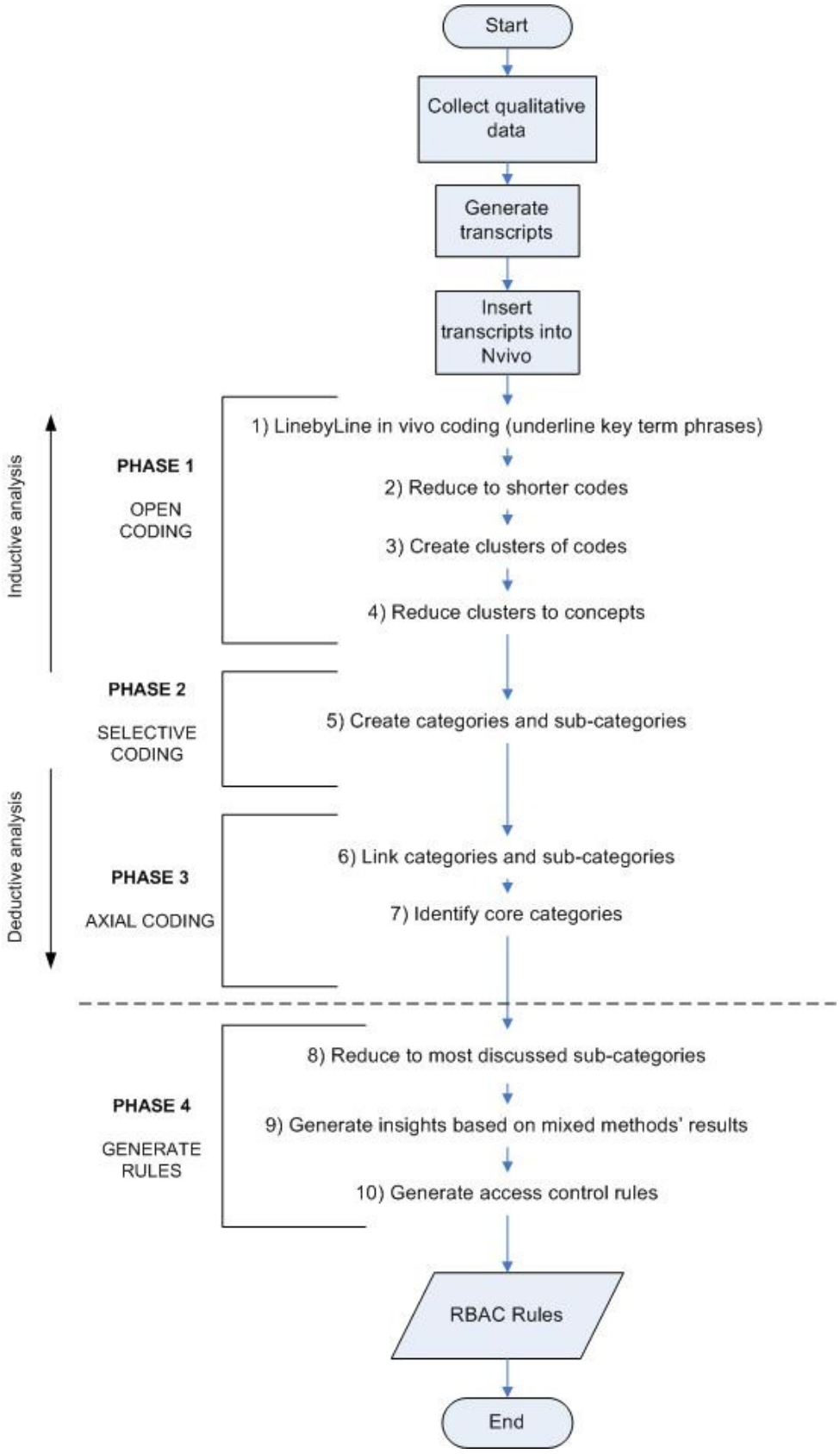

Figure 5.1 – Phases of the grounded theory data analysis for the focus groups.

Theoretical sampling was not incorporated in this study due to time and resources constraints so the GT approach used in this study was applied to data analysis and not to data collection.

5.2.2.5 Results

Four FGs were arranged with a total of 26 participants: one group with 4 nurses (FG1), one group with 5 health technicians (FG2) (3 radiologists, 1 pharmacist and 1 neurophysiologist), another group with 7 people from mixed backgrounds (FG3) (1 doctor, 3 nurses and 3 health technicians) and the last group with 10 medical doctors (FG4). Table 5.2 shows the type of institution they worked for.

Table 5.2 – Healthcare institutions for the FG participants.

FG	University hospital	Hospital centre[2]	Hospital	Health centre	Private clinic
FG1	1		2	1	
FG2	2	1	2		
FG3	1	1	3	1	1
FG4	4	4	1	1	
TOTAL	**8**	**6**	**8**	**3**	**1**

Figure 5.2 presents the categories/sub-categories generated from the qualitative data collected from each FG. Newly generated categories from the different FGs are marked. The 8 core categories represented in Figure 5.2 (from step 7 of the analysis) are: system access; access control roles; access by patients; access in emergency situations; security; system access solutions; access control policies and paper vs digital (the main categories are identified with a ✻).

[2] Organizations that integrate more than 2 hospitals.

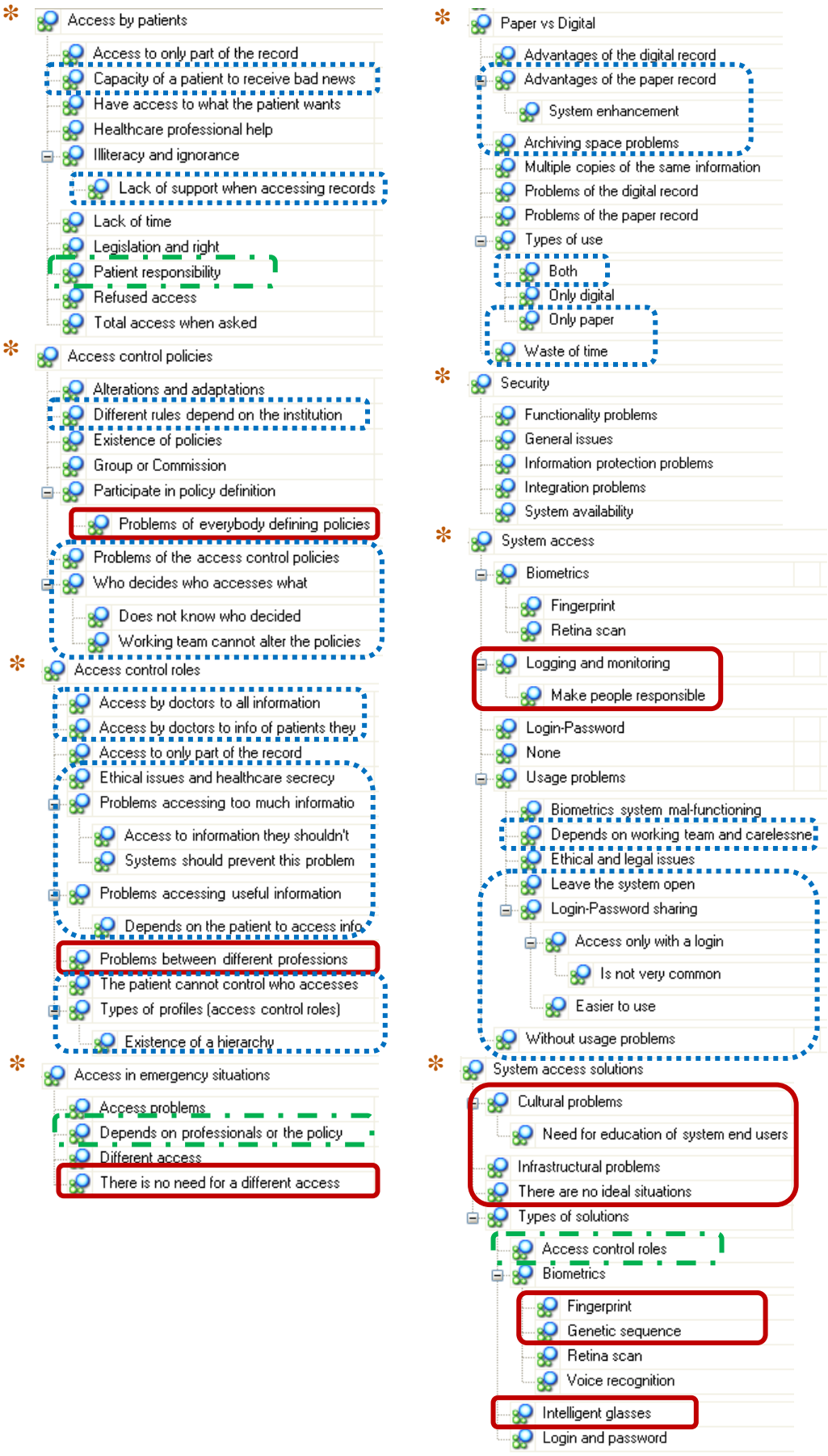

Figure 5.2 – Generated categories: FG1 are not marked; FG2 ——, FG3 ·····; FG4 — ·

Table 5.3 shows the categories with the most references, and therefore most mentioned by the FGs participants (step 8 of Figure 5.1).

Table 5.4 analyses in more detail the demographics of the participants in relation to the responses they gave concerning the most discussed sub-categories.

Table 5.3 – Most mentioned sub-categories on the course of the 4 FGs (n=26).
(TR - total no of references for a category; PP - No of different people that discussed a sub-category).

Main categories	TR	Most mentioned sub-categories	PP
System access	146	Login-password	18
		Usage problems	18
		Login-Password sharing	16
Access control policies	125	Problems with the policies	16
		Alterations and adaptations	12
		Participate in the policy definition and give opinion	14
Paper vs Digital records	100	Problems with the digital records	11
		Problems with the paper records	10
		Types of use	10
Access control roles	99	Problems of accessing useful information	11
		Access to only parts of the record	9
		Problems of accessing too much information	8
Access by patients	98	Require HCP support	9
		Illiteracy and ignorance	11
		Legislation and rights	11
Security	86	Functionality problems	13
		Information protection problems	6
		General issues	8
System access solutions	70	Types of solutions	11
		Biometrics	11
		Fingerprint	6
Access in emergency situations	11	Requires different access	4

Table 5.4 – Demographics of the participants of the most discussed sub-categories: by sex (F=16;M=10), professional category (N-nurses=7; T-technicians=8; D-doctors=11) and type of institution (Hc-health center=4; PH-public hospital=13; PrH-private hospital=3, PrCl-private clinic=3; HoC-hospital center=3).
(PP - No of different people that discussed a sub-category).

Most discussed sub-categories	F	M	N	T	D	Hc	PH	PrH	PrCl	HoC	Total PP
Login-password	12	6	4	6	8	4	6	3	2	3	**18**
Usage problems	10	8	6	5	7	3	8	2	2	3	**18**
Login-Password sharing	8	8	6	3	7	3	8	1	1	3	**16**
Problems with the policies	8	8	4	7	5	3	9	1	2	1	**16**
Participate in the policy definition and give opinion	7	7	4	6	4	2	7	2	2	1	**14**
Functionality problems	7	6	4	5	4	2	8	1	1	1	**13**
Alterations and adaptations	8	4	4	6	2	3	7	1	-	1	**12**
Types of solutions	6	5	4	6	1	1	5	2	3	-	**11**
Biometrics	6	5	4	5	2	1	5	2	3	-	**11**
Illiteracy and ignorance	7	4	2	5	4	1	3	3	3	1	**11**
Problems of accessing useful information	7	4	3	5	3	2	5	2	2	-	**11**
Legislation and rights	5	6	3	4	4	1	4	1	2	3	**11**
Problems of the digital record	7	4	4	1	6	2	4	1	1	3	**11**
Problems of the paper record	6	4	4	5	1	1	5	2	1	1	**10**
Types of use	8	2	5	4	1	2	3	2	3	-	**10**
Require HCP support	4	5	2	5	2		3	2	3	1	**9**
Access to only parts of the record	6	3	4	5		1	5	2	1	-	**9**
Problems of accessing too much information	4	4	4	1	3	-	3	1	3	1	**8**
General issues	3	5	3	1	4	2	4	-	1	1	**8**
Information protection problems	2	4	3	2	1	1	4	-	-	1	**6**
Fingerprint	4	2	1	4	1	-	1	2	3	-	**6**
Requires different access	2	2	1	1	2	-	2	1	1	-	**4**

5.2.3 Structured questionnaires

These are questionnaires containing different sets of questions, organized in a specific order. A sample of the population is selected and the questions are applied either face to face or people are left to complete them in their own time. The questionnaires can be oriented to focus on specific information. They can, for instance, be based on previously obtained information such as from FG discussions, as they were in this specific study.

The data is analysed quantitatively. Access control rules are generated according to Phase 4 of Figure 5.1.

5.2.3.1 Objective

The aim of this section is to apply structured questionnaires to HCPs so that some of the categories and sub-categories that came up during the course of the FGs can be further explored as well as complemented with the use of quantitative methods.

5.2.3.2 Construction of the questionnaire

The questionnaire comprises four sections. Section 1 contained 9 generic questions regarding EMR; Section 2 had 11 questions regarding access control to EMR; Section 3 had 4 questions about a fictitious scenario of patients using an Automated Teller Machine (ATM) to access their medical records; and Section 4 had 7 demographic questions (Appendix C). The questions comprising the first three sections were constructed based directly on the categories and sub-categories resulting from the FGs (Table 5.5).

Table 5.5 – Mapping the questionnaire sections and questions to the generated categories/sub-categories within the FGs.

QUESTION TOPIC	RELATED CATEGORIES/SUB-CATEGORIES	Questions
Generic EMR (Section 1)	• Usage problems • Paper vs digital records • Security • Alterations & adaptations	{1,2,3,5} {4} {6} {7,8,9}
Access control to EMR (Section 2)	• System access • Access control roles • Access control policy definition • System access solutions • Access in emergency situations	{12,13} {14,15,16,17,18} {19} {10,11} {20}
ATM patients' access (Section 3)	• Access by patients	{21,22,23,24}

5.2.3.3 Population

Questionnaires were tested and corrected with 5 different people from different backgrounds before they were applied to the population in the study.

HCPs from different healthcare institutions and backgrounds were approached in a random fashion at their working place during working hours. They were asked to answer the questionnaire and they could either refuse to do it, do it immediately or do it later in their own time. From the 30 HCPs that were approached, 29 agreed to answer the questionnaire but only 27 valid questionnaires were received and analysed.

5.2.3.4 Data collection and analysis

Data was collected from the respondents, who were completely unaided in this. The data was subsequently analysed and summarized by the SPSS statistical analysis software.

5.2.3.5 Results

27 valid questionnaires were received and analyzed. 12 (45%) questionnaires were received from medical doctors, 6 (22%) from nurses and 9 (33%) from HCPs. From the 25 participants that answered the last demographic question, 15 (60%) participants were female while 10 (40%) were male. 14 (52%) participants worked in a hospital, 5 (18%) in a health centre, 1(4%) in a laboratory, 2(7%) in an academic institution, 1 (4%) in a public healthcare institution and 4 (15%) in a private healthcare institution. In terms of academic education, 23 (85%) respondents had a BSc and 4 (15%) had an MSc. Also, 16 (59%) had some informatics' proficiency, 7 (26%) had had some informatics' education and 3 (11%) had had none (1 respondent did not answer this question).
A summary of the analysed results is presented next.

The answers obtained from Section 1 of the questionnaire were that 21 (78%) HCP had used EMR during the course of their work while 6 (22%) respondents never had. From the 21 respondents that had used EMR, 17 (81%) used the EMR daily or almost everyday while 3 (14%) used EMR 1 to 3 times per week (1 respondent did not know the frequency). The most common uses were: data input - 18; consultation - 15; prescription - 11; emergency or intensive care – 8; and decision support - 5; (the respondents could select more than one option to this question).
From the 26 valid answers about the importance of EMR, 1 (4%) respondent considered that EMR was a necessary evil, 14 (54%) agreed that EMR was very important for their work whilst 8 (31%) thought it was indispensable (3 respondents had no opinion). Although there are many participants that access EMR on a daily basis there are still many problems with its use. Table 5.6 presents some of the problems mentioned by the participants (more than one problem could be chosen by each respondent).

Table 5.6 – Number of respondents for the question about EMR problems (n=27).

EMR problems	n (%)
Required previous education or training	18 (67%)
EMR allows too easy sharing of sensitive information	17 (63%)
Access control can hinder access to the system	15 (56%)
Required change in tasks HCP need to perform	13 (48%)
EMR can allow too much/easy distributed online access	7 (26%)
They are not secure	6 (22%)
May affect doctor-patient relationship	5 (19%)
Do not trust the system	5 (19%)
Waste of time	4 (15%)
No opinion	3 (11%)

In response to the question about participating in the development of EMR, 22 (82%) respondents said they had never participated in this whilst 5 (18%) said they had. When asked if they thought HCP should participate in the development of EMR, 22 (82%) respondents said they should, 3 (11%) said they should not while 2 (7%) did not know. When asked which parts of the development they ought to participate in, 21 said they would like to participate in the conceptualization phase; 16 in the testing process; 15 in the implementation; 14 in the definition of access control policies; and 2 did not know (the respondents could select more than one option to this question).

For the second set of questions (Section 2) regarding access to EMR, 22 (82%) respondents said they logged in using a password (4 of them together with biometrics), 1 (3,5%) respondent used biometrics alone, 1 (3,5%) did not use any kind of mechanism, and 3 (11%) did not know what mechanisms they used.

From the 26 respondents that answered the question about login/password, 17 (65%) said they easily accessed the EMR system with this authentication mechanism; 4 (15%) said they normally share their password; and 3 (12%) agreed that they very often forget their passwords (2 respondents had no opinion).

Seven respondents (26%) said that it took too long to access the EMR, while 16 (59%) said it did not (4 did not know).

When asked if they had difficulties while accessing the EMR, the respondents answers were the ones presented in Figure 5.3.

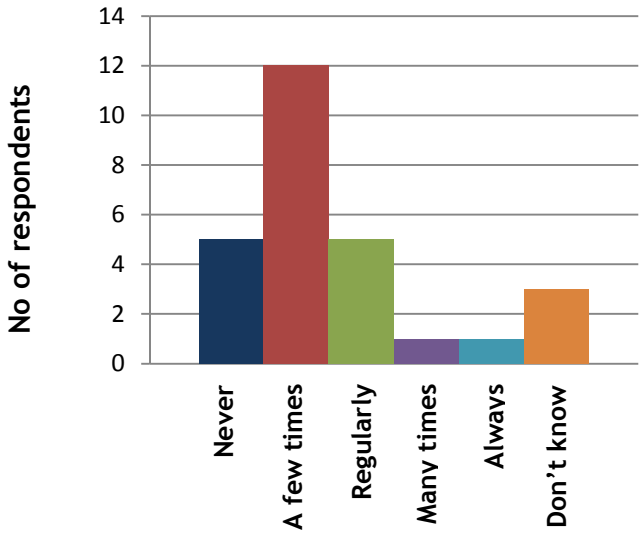

Figure 5.3 – No of respondents vs. the difficulties they have when accessing an EMR.

Now about access control roles, 13 (48%) respondents agreed with the existence of access control roles in general, while 12 (44%) agreed with this but only for some information. 2 (8%) participants did not agree with the existence of access control roles. With the EMR they use, respondents said that 16 (59%) have access control roles, 6 (22%) do not have and 5 (19%) did not know. Further, for the ones that answered yes to the previous question (n=16), 9 (56%) respondents said they were not the correct access control roles, 5 (31%) said they were and 2 respondents did not answer this question. 1 (4%) of the respondents said they had participated in the definition of the access control roles while 25 (92%) said they had not (1 respondent did not have an opinion).

Table 5.7 presents the responses for the types of access control roles that the participants think should be used versus what they use on a regular basis (respondents could select more than one option).

Table 5.7 – Types of access control roles that exist or should exist.

Access control roles defined by	Used regularly	Think should be used
Professional category	13	19
Type of information (more/less sensitive)	2	15
The dept where the HCP works	6	11
The patients	0	4
Does not know	2	2

Finally, a question was asked about providing HCP with access to patient information in emergency situations: 9 (33%) respondents agreed but only for those professionals participating in the emergency care; 8 (30%) respondents answered yes depending on the emergency situation; 3 (11%) respondents answered yes for everybody; 2 (7%) respondents

said yes as long as the HCP or the team that is assisting the patient at that moment has authorization; and 4 (15%) respondents said no (1 respondent did not answer).

Section 3 of the questionnaire related to a fictitious scenario of patients accessing their medical records via an ATM machine (Table 5.8).

Table 5.8 – Access to EMR via an ATM.

	Yes	**No**	**No opinion**
Agree with access to EMR by the patients via an ATM?	6 (22%)	17 (63%)	4 (15%)
Is it a secure system?	7 (26%)	18 (67%)	2 (7%)
	Daily/everyday	**1-3 times/week**	**Never**
How often do you use an ATM to perform banking operations? (n=26)	4 (15%)	21 (81%)	1 (4%)

Although 21 respondents said they accessed a normal ATM 1 to 3 times per week and 4 participants said daily or almost everyday, from the 18 respondents that answered that an ATM is not a secure system, 13 said that the main problems envisaged with this type of access to patients' healthcare information were that it raises ethical questions and 13 that is not secure enough (the respondents could select more than one option to this question).

5.3 Patients' perspectives on access control

Due to time constraints, it was not possible to perform FGs with patients. For this reason, the data used in this section was extracted from the FGs that were applied to the HCPs. Data was selected concerning HCP views on patients' access to their medical records and then structured telephone interviews were applied to the patients to confront the HCPs' views with the patient views and then extract the access control rules from this data.

5.3.1 List of discussion topics

Similarly to Section 5.2.1 of this chapter and according to all the information reviewed in the previous sections, a list of discussion topics about patients' views regarding access control to EMR was built. This list helps to summarize the information obtained until now from the reviews performed in previous chapters and can be integrated in the development of the structured telephone interviews.

5.3.1.1 Patient generic views on EMR

1. Most patients do not know or understand about EMR
2. Patients may think their relationship with their HCP can be affected by the use of EMR during consultation

3. Patients do not know how or if they want to access their records
4. Patients may not trust or not know about EMR security

5.3.1.2 Patient views regarding access control to EMR

1. What if they could access their EMR via an ATM with their card:
    1.1 Would they find that secure enough?
    1.2 Would it be easy enough to use and access?
    1.3 Would they use it on a regular basis?

5.3.2 Views from the focus groups

The participants of the four FGs presented in Section 5.2.2 discussed the subject of patients accessing their medical records. Using the transcription and analysis of the dialogues, the core category ***Access by patients*** comprised 10 sub-categories. These sub-categories refer to the most mentioned subjects during the discussions. Table 5.9 shows the number of times each of the sub-categories was discussed by the participants of each FG.

Table 5.9 – Number of different people discussing each of the subcategories that relate to patients' accessing their medical records (PP). It also includes the total number of references (TR).

Subtopic	FG1	FG2	FG3	FG4	PP	TR
1. Access helped by a healthcare professional	1	2	5	1	**9**	**23**
2. Legislation and right to access the medical record	2	3	3	3	**11**	**18**
3. Problems of ignorance and illiteracy	2	2	4	3	**11**	**18**
4. Have access to what the patient wants	3	3	3	1	**10**	**13**
5. Lack of time from the healthcare professional	-	1	3	1	**5**	**6**
6. Access to only part of the medical record	-	1	3	1	**5**	**6**
7. Access to the whole record as soon as it is requested	-	1	2	-	**3**	**5**
8. Access to the medical record should be denied	-	-	3	-	**3**	**4**
9. The capacity of the patient to deal with bad news	-	-	2	-	**2**	**2**
10. Patient responsibility	-	-	-	1	**1**	**2**

It is clear from Table 5.9 that most participants discussed subcategories relating to the right that patients have to access their medical data. It is defined within the legislation and they should be able to do it whenever they want to (2^{nd} and 4^{th} sub-categories). However, in contrast, sub-categories 1 and 3 also stress the need for a patient to have assistance when accessing their medical records, due to any problems they might encounter. The information that is registered may include medical terms that the ordinary citizen is usually not familiar

with. This can create a lot of unnecessary apprehension that can easily be avoided if a HCP explains to the patient what the record means. This is why so many HCPs feel that it is important to mention the ignorance and illiteracy that patients may have in understanding their medical records. Furthermore, they also mention the lack of time to help the patients with this task (5th subcategory).

It is important to draw attention to the contradiction between the points 2 & 4 and the points 1 & 3, since it highlights the gap that exists between legislation and patient rights on the one hand and the practical difficulties of making medical records available to patients on the other hand.

5.3.3 Structured telephone interviews

Structured telephone interviews are similar to structured questionnaires differing only in the way the questionnaires are applied. In telephone interviews, these are applied over the telephone to people's households. Although this saves time and money to the researcher, unlisted numbers can be a problem when trying to get a random sample. Random digit dialling tries to avoid this problem [93]. This technique dials numbers in a random fashion. Pre-selecting the numbers increases the proportion of reached households [94]. Advantages of telephone interviews include: a) a reduction in the number of omitted items (participants are bound to answer more questions than if they had to fill in a questionnaire on their own); b) skip patterns are followed by the interviewer instead of the respondent; c) open-ended questions can be asked; d) interviewer can ask if the respondent is having problems understanding the questions. Disadvantages of this technique include: a) someone pretending to be the respondent, there is no assurance on who the person at the other side is; b) the sample may be biased by the time when the call is made; c) difficulty with questions that require the person to choose among various options due to excessive memory requirements; d) repeated calls may be needed to reach a desired household [94].

5.3.3.1 Objective

The aim of this section is to apply structured telephone interviews to the population that use the Portuguese National Health Service. The goal is to obtain their opinions regarding the use and access control to EMR. These views will confront and/or complement the categories that came up during the course of the FGs analysis in relation to the patients as detailed in Section 5.3.2.

5.3.3.2 Construction of the interview

The interviews were divided into 5 sections. They were designed to explore further some of the issues that are more relevant to this study regarding patients' access to their medical records. Section 1 included 3 generic questions about an EMR and its usage, Section 2 contained 7 questions on access to patients' EMR by the patients themselves; Section 3 contained 4 questions about access control measures; Section 4 had 6 questions about a fictitious scenario of patients using an ATM to access their medical records; and Section 5 included 6 demographic questions (Appendix D).

The questions comprising the first four parts of the interview were constructed based directly on the categories and sub-categories resulting from the FGs (Table 5.5).

Table 5.10 – Mapping the interviews' sections and questions to the generated categories/sub-categories within the FGs.

QUESTION TOPIC	RELATED CATEGORIES/SUB-CATEGORIES	Questions
Generic EMR	• Usage problems	{1,2,3}
Access to EMR by patients	• Access by patients • Legislation and rights • Security	{5,6,7,10} {4} {8,9}
Access control measures	• System access • Access control roles • Access control policies • Access in emergency situations	{11} {12} {13} {14}
ATM patients' access	• Access by patients • System access solutions • Security	{18,19} {15,16,20} {17}

5.3.3.3 Population

People were selected from the region within and around the second biggest city in Portugal, Porto. The calls were made only to landline numbers and limited to the 22 prefix, which is the prefix for Porto. 14000 phone numbers from this region were randomly generated. Numbers were contacted from the list until a total of 200 valid interviews were performed. For each residence that was contacted, all the residents aged 18 years or over were asked to answer the interview. More than one telephone contact could be made to the same residence in order to interview all residents.

5.3.3.4 Data collection and analysis

The structured interviews were applied with the use of the simple Random Digit Dialling algorithm [93]. The method is described in Figure 5.4.

Data was collected on paper by the interviewer and some extra information (postal code, location, sex, number called, etc) was also recorded.

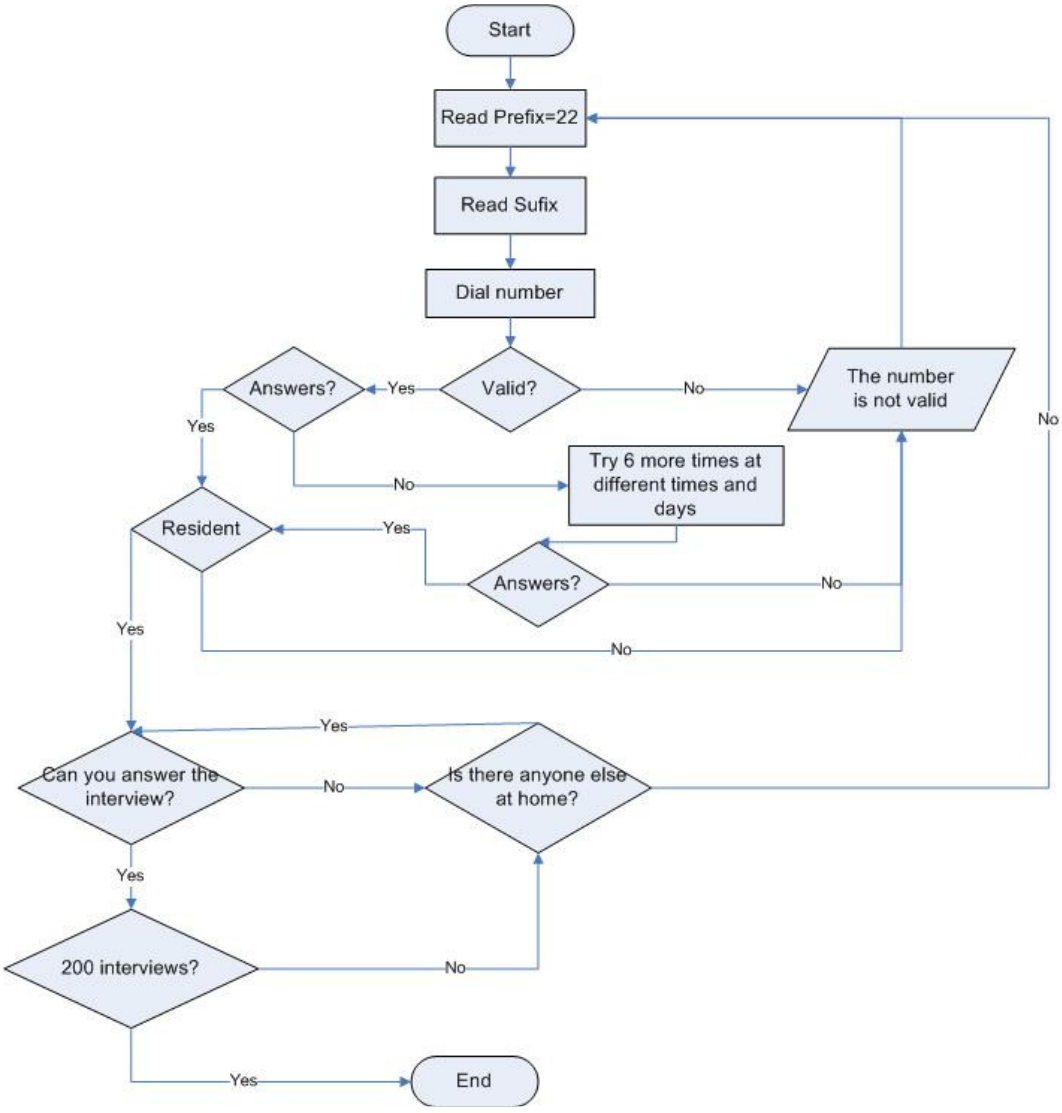

Figure 5.4 – The Random Digit Dialling algorithm used to perform the structured telephone interviews to the patients.

5.3.3.5 Results

A total of 200 valid telephone interviews were performed. From these, 130 (65%) interviewees were from female participants and 72 (36%) had a chronic disease. The age of the interviewees that revealed their age (n=198) had an average of 51 years (standard deviation of 16 years) and was normally distributed. In terms of academic proficiency (n=199), 5 (2%) had never been to school, 100 (50%) had finished primary school, 56 (28%) finished high school, 35 (18%) had a BSc, 2 (1%) a master degree while 1 (1%) had a PhD. In informatics (n=199), 75 (38%) had no proficiency at all, 70 (35%) had some proficiency while 54 (27%) were well acquainted with computers.

A summary of the analysed results is presented next.

The answers obtained from Section 1 of the interview revealed that, from the 200 valid interviews, 124 (62%) interviewees did not know what an EMR was while 76 (38%) said they did. From those that knew what an EMR is, 56 (77%) thought that EMR are used in Portugal, 10 (14%) thought they were not, 7 (10%) did not know and 3 did not answer. Respondents said EMR are used mostly for: consultation 52 (72%); communication, data transmission and information sharing 35 (48%); data input 18 (25%); research 7 (10%); decision support 2 (3%); and 2 (3%) did not know (respondents could select more than one option to this question).

For the second set of questions regarding patients' access to their medical records, 58 (29%) respondents said they know that it is within the legislation that they can access their medical data when required. Table 5.11 presents results from the questions regarding patients' accessing their EMR.

Table 5.11 – Results to the questions about patients' accessing their EMR.

	YES			**NO**
Would you like to access your EMR when required	131 (65%)			68 (34%)
	YES	**NO**	**Don't know**	
With the help of a healthcare professional	102(77%)	28(21%)	1(1%)	
With the use of a computer	102(77%)	29(22%)	-	

164 (82%) respondents also mentioned that they wanted their medical records to be available 24/7, 26 (13%) said they would not want their records to be available 24/7 while 10 (5%) did not know.

Regarding the questions about security of medical data from Section 2 of the interview, from the 198 valid responses, 152 (76%) respondents believed that access to their medical data would not influence the trust that they have in their doctor, 32 (16%) said it could affect their trust while 14 (7%) did not know. 82 (41%) respondents said that accessing their medical data with a computer would not affect data security, 85 (42%) thought that it might while 33 (17%) did not know. From the 85 respondents that said it might affect the security of their medical data, 71 (83%) said it would affect their confidentiality, 13 (15%) said that security is not provided, 2 (2%) others that there may be a virus or integrity problem while 1 (1%) respondent mentioned the problem of how easy it is to share medical data with the EMR system (the interviewees could select more than one option).

For the questions about access control measures in Section 3, from the valid 197 answers, 45 (23%) respondents thought that there are proper means to provide for access control to EMR, 82 (42%) thought there are not while 70 (35%) did not know. About the existence of access control roles, of the 198 respondents who answered this question, 141 (71%) said that access control roles should be provided to protect medical data, 25 (13%) said there is no need for that while 32 (16%) said they did not know. From the 141 that said that access control roles must be provided, 1 did not specify what type of roles should be provided while 2 did not know. Table 5.12 presents the types of access control roles that the 141 respondents thought should be provided (the respondents could select more than one option).

Table 5.12 – Results from the questions about access control roles.

Access control roles	n (%)
Defined by professional category	83 (60%)
Defined by the patients	34 (25%)
Defined in other ways (doctor with the patient, family members, only the family doctor, etc)	25 (18%)
Only for more sensitive information	4 (3%)

From 199 valid answers, 142 (71%) respondents said that they would like to define who should access their medical records, 52 (26%) said that they would not while 5 (3%) said they did not know. 195 interviewees answered the question relating to emergency access to their medical records. 191 (97%) said that mechanisms should be available to allow any HCP to access patient medical records in an emergency situation, 3 (2%) said that those mechanisms must not be provided while 1 did not know. For the respondents that agreed that emergency mechanisms should be available, 140 (73%) said that in emergency situations, any HCP should access their medical records, 47 (25%) said that only some emergency HCPs should have access, 1 said that only doctors should have access, while 1 said that any professional should have access as long as he/she had an authorization from the patient or a family member (2 did not answer this question).

Section 4 of the interview related to a fictitious scenario of patients accessing their medical records via an AMT machine (Table 5.13).

Table 5.13 – Answers to the questions about patients' accessing their medical records via an ATM machine.

	YES	NO	Do not know
Would you like to access your medical records via an ATM (n=199)	83 (42%)	112 (56%)	4 (2%)
Is it a secure way to access your medical data (n=81)	55 (68%)	13 (16%)	13(16%)
Type of data to access (n=80)	Exam: 64 (80%) Consultation: 40 (50%) Medication: 33 (41%) Others: 27 (34%)		
How frequently would you like to access your medical data this way (n=81)	1 to 3 times per week: 3 (4%) 1 to 3 times per month: 30 (37%) Less than 1 per month: 47 (58%) Never: 1 (1%)		

When asked how often they would access an ATM to perform bank operations, from the 188 valid responses, 104 (55%) respondents said that they do it more than 3 times per week while 17 (9%) said they do it daily or almost everyday. 38 (20%) respondents said that they did it less than 3 times per week and 26 (14%) said they have never accessed an ATM machine (3 respondents did not answer this question).

5.4 Discussion

This chapter presents, in some detail, the results from the application of the mixed methods (qualitative and quantitative), both to HCPs and patients. It also illustrates the integration of the results from the principal method (qualitative) to the subsequent secondary method (quantitative).

The analysis of the results obtained from the FGs shows that some of the generated categories/sub-categories that were most discussed by the participants needed further exploration. These were: usage problems, alterations and adaptations (relating to access control policies), access control roles, system access solutions, access in emergency situations and access by patients. In order to further investigate these issues, the quantitative methods were subsequently applied to the FG results.

The quantitative methods revealed that for HCP, the most common usage problems were that EMR require previous education or training and the HCP needed to change their workflows in order to use them. Also, a vast majority of HCP agreed that they did not participate in the design and development of EMR systems as well as their access control policies, something which they should be able to do more often. These results are consistent with what was discovered during the access control literature review (Chapter 2). There are in practice some barriers that impede

the successful integration of EMR. These results justify even further the importance of this research work.

This research also discovered that not many patients are aware that they have the right, according to law, to access their medical records. This may explain why patients are still not much involved with the process of accessing their medical information and do not press their Government for easier and better ways to do it. EMR systems rarely include the patients as another user. When patients are asked about these matters, the majority said they would like to access their medical records when needed, possibly with a computer, and most of them with the help of a HCP. In addition, both HCP and patients agreed that, in emergency situations, HCP should be able to access everything by overriding the access control rules that were previously defined. This requirement has never been provided by an access control model.

Regarding access control roles, the majority of both HCP and patients agree that EMR systems should include these mechanisms, although HCP think they are usually wrongly defined. While HCP feel that access control roles should be defined according to professional category, followed by the type of information (more/less sensitive) and then a very small percentage mentioned that patients should also be able to define them; patients agreed that professional category should be used more often, followed by around a quarter of them answering they should be able to do it themselves. And when asked, in a separate question, if they would like to define who can access what regarding their medical records, a big majority of respondents have the same opinion that they should be able to do it. Again, there is a general feeling that when asked for their opinion, patients actually think they should be more interested and in control of their medical records access and usage.

Analysing now the scenario about patients accessing their medical records with a machine similar to an ATM, it is interesting to see that a similar number of HCP and patients do not agree with the existence of this method to access medical records. However, a vast majority of HCP think that this method is not secure while about the same numbers of patients think it is. So their reasons are different for not wanting this type of scenario to work in practice. Further, it is important to note that a big percentage of HCP and patients access an ATM machine on a regular basis to perform bank operations. So an ATM machine with the provision of access control and securities that most people recognize and trust on a regular basis is good enough to keep their money and financial information but is not good enough to protect their medical information.

This chapter shows that it is possible to integrate several methods into the same study. The use of mixed methods helps to select the best features of every method, complementing and

improving research results. As long as they are well defined, and with objective steps, the methods presented here can be reproduced by other researchers with similar objectives and can integrate a wider range of knowledge and experiences.

6 ACCESS CONTROL RULES' EXTRACTION

6.1 Introduction

This chapter describes the process of extracting the access control rules from the results obtained with the application of the mixed methods presented in Chapter 5. This process includes the definition of insight sheets [90] that are then transformed into generic access control rules. An insight sheet contains insights and support notes from the discussion and then the design ideas from the insight, which in this case are the rules extracted from the insights.

The information provided for the support notes is based on quotations from the FGs' participants. The insight sheets are then obtained from those support notes or from the summarized results attained from the structured questionnaires and the structured telephone interviews. Several insight sheets and corresponding access control rules are provided for each one of the applied methods (i.e., FGs, structured questionnaires and structured telephone interviews) and for the applicable categories and/or sub-categories. Most rules are directly translated from the insights. The rules that are not are further explained.

In order to define and present the list of access control rules in a more standardized way that can be easily modelled this list is transformed into a list of rules that include RBAC fundamental building blocks.

6.2 Access control rules

The access control rules are separated into three different sets: legislative, standards and mixed methods. For each set there is a list of access control rules focused on the HCP and another one focused on the patients and the rules are numbered with a corresponding initial (L – Legislative; M – Mixed methods) and a number. As the standard rules are translated directly into final rules (Table 6.4), these do not need to be previously numbered.

There can be similar rules in each set. Some of these have the same numbering while others, which cannot be detected so easily, will be merged later in the chapter (Section 6.3) into a unique list of all the access control rules.

6.2.1 Legislative and standard rules

6.2.1.1 Healthcare professionals

The legislative access control rules for HCP are the rules L.1 to L.3 and L.8 to L.14 presented in Section 4.4, with the exception of rules L.15 and L.16 that cannot be translated into proper access control rules.

The standard rules for HCP are presented in Section 6.3.2, Table 6.4, rules 26 to 33.

6.2.1.2 Patients

The legislative access control rules for the patients are the rules L.4 to L.7 presented in Section 4.4.

The standard rules for the patients are presented in Section 6.3.2, Table 6.4, rules 34 and 35.

6.2.2 Mixed methods – insight sheets and rules from the focus groups

6.2.2.1 Healthcare professionals

Category: ***Access in emergency situations***

Sub-category: *Require different access*;

Insight: There is the need to provide for access in emergency situations and for the emergency doctor to access patients' information in those situations;

Support notes from the discussions: "…specific controls in the emergency room must be provided to access[3] information from those patients…different access to the doctor that is assisting in an emergency room…I'm talking about those that are not his/her patients…" (Quotation from a technician) ; "...we, in the emergency profile, must have [different] access..." (Quotation from a nurse);

Access control rules:

M.1 Specific roles must be able to BTG and access (read only) information in emergency situations.

M.2 Logging and audit must be provided at all times (this rule was included to further complement the BTG features that integrate rule M.1).

Category: ***System access (authentication)***

Sub-category: *Usage problems – login and password, biometrics;*

Insight: Sharing usernames and passwords is very common and auxiliary personnel can finds out quite easily usernames and passwords; some people cannot authenticate with the biometrics fingerprint;

Support notes from the discussions: "It is common practice to use each others' logins…specially in the integration of clinicians in electronic environments…is bad…very bad…" (Quotation from a technician); "When they bring passwords they leave them in a written paper…or sometimes they [auxiliary personnel] see us writing them on the

[3] The term "access" in Portuguese means "read only" while in English can include anything from write or update. The terms "insert" or "alter" would be used in Portuguese in order to mean any alteration to the data. So for this specific access control rule, "access" means "read only".

keyboard…" (Quotation from nurse1); "And who puts a login and password underneath the arm of auxiliary personnel?? Everything is there [paper record]!" (Quotation from a technician); "There are generic passwords in some places…" (Quotation from doctor1); "Sometimes we just need the person ID number to access a system…" (Quotation from nurse2); "We have to ask a colleague to login so that we can insert our observations, because we had some induction to system X but they didn't give us the fingerprint to access it afterwards...so we could not enter the system…" (Quotation from doctor2);

Access control rule:

M.3 Different types of authentication mechanisms must be available to be adapted according to user needs (most common are login/password + biometrics).

Sub-category: *Logging and monitoring;*

Insight: Systems must permanently log all the actions and provide mechanisms to block the screen after some inactivity time (it must be easy to log in again without much effort).

Support notes from the discussions: "It is more important that people have access to what they need on their daily work and that their access is logged and what type of information was accessed…" (Quotation from a doctor); "Login and password is annoying…we need something to log what a person does but it disrupts normal workflow and processes! Permanent records must be available…the system must have some mechanism to make the screen blank where the information is displayed but that will allow easily access to it again…to remember it without closing again...doctors go mad with this!" (Quotation from a technician);

Access control rules:

M.4 Audit must be available and secured at all times.

M.5 Necessary to provide means (e.g., alert features) to avoid problems with the authentication mechanisms.

Category: *Access control roles*

Sub-categories: *Types of roles & Access to only parts of the record;*

Insight: Systems must provide for appropriate access control roles;

Support notes from the discussions: "…if the doctor does not make relevant patient data available in a written form (I cannot access the doctors' system) I cannot see anything…I think that is wrong!" (Quotation from a technician). "Access roles are usually not correct…" (Quotation from a doctor).

Access control rule:

M.6 Access control roles must be provided.

Sub-category: *Problems of accessing too much information;*

Insight: It is currently easy to access all EMR information about a patient not related to the treatment;

Support notes from the discussions: "Who wants to be nosy and curious can easily with a click do that and access all the information he/she wants…" (Quotation from a nurse); "I've known of some cases where people went looking for information about other people…not everyone is so ethical…" (Quotation from a technician); "We find people that access lab information 800 or 900 times per week!" (Quotation from a doctor).

Access control rules:

M.7 It must be possible to define alerts for the number of accesses (defined on a temporal basis) based on specific users or roles.

M.7.1 The responsible person must be alerted if someone or some role reaches that limit (both if person has authorisation or not to access that information).

Sub-category: *Problems of accessing useful information;*

Insight: Cannot access EMR information that is useful to perform the daily work and the department is responsible for providing proper access control roles management;

Support notes from the discussions: "Some fields are not available for us…it depends on the department…" (Quotation from a nurse);

Access control rules:

M.8 The definition of access control roles must be fine-grained.

M.8.1 Exceptions to roles must exist so that people can have more or less permissions than the role assigned to them.

M.8.2 The head of the department (or responsible role) must be able to assign one or more people the right to alter some access permissions for some roles (can be associated with constraints).

M.8.3 Provided that all this is logged and properly audited (this rule was added to secure better the changes that are made by the responsible parties).

Category: *Access control policies*

Sub-category: *Participate in the policy definition and give opinion;*

Insight: HCP should participate in the definition of access control policies;

Support notes from the discussions: "…is frustrating that no one listens to us…that no one listens to our opinion…" (Quotation from nurse1); "I had a practical experience once…very positive…everybody participated...and there was always an improvement in real time…" (Quotation from nurse2);

Access control rules: not applicable for this sub-category.

Sub-category: *Who decides who accesses what;*

Insight: A team, representing the department, should define access control policies;

Support notes from the discussions: "…if there was a multidisciplinary team with all professional categories of a hospital and ask the responsible parties what they think…in relation to what tasks they need to perform…would be much better than implement equal [policies] for all places…" (Quotation from a technician);

Access control rule:

M.9 There must be a representative for each role who can define or change the policies for that role.

Sub-categories: *Problems with the policies & Alterations and adaptations;*

Insight: Roles should be able to be changed/dynamic/adaptable; Need for the informatics' department or administrator to change the policy;

Support notes from the discussions: "…I could not do it [alter some functionalities] because my profile did not allow it…" (Quotation from a nurse); "…it does not make sense HCPs not having access to the information for the normal performance of their tasks…healthcare information that is needed, any of us must be able to access it…" (Quotation from technician1); "I think [it] is not sensible to limit access to read information…people will end up accessing it anyway…" (Quotation from technician2);

Access control rules:

M.10 Roles must be able to change and adapt accordingly.

M.10.1 Permission to modify a role must be provided for specific circumstances.

M.10.2 All this must be logged and registered with conditions similar to BTG processes (someone gets a message of changes and revises its appropriateness).

Category: *System access solutions*

Sub-category: *Types of solutions;*

Insight: Biometrics: fingerprint, retina, voice recognition, genetic sequence, intelligent glasses (medical information would appear in the glasses to be read by the person that owns the glasses); Biometrics + passwords; and access control roles with auditing of what is done;

Support notes from the discussions: "...access control roles and auditing of what was accessed..." (Quotation from doctor1); "…with so many passwords we have to remember…we older people start to have loss of memory…I think that any biometrics system is easier for me…" (Quotation from doctor2);

Access control rule:

M.11 There is the need to provide for access control roles and logging features.

Category: *Security*

Sub-categories: *System availability & functionality problems;*

Insight: The need for better and more available support at a technical level (24/7);

Support notes from the discussions: "It happened at the new year's eve when the server was unavailable and we called to the informatics department and no one was there…sometimes saturday we also call…and then we stay the whole weekend…At the hospital where I work we have the laptops stored in the vault because the wireless antennas do not work properly and we cannot get connected while we are in the infirmaries…" (Quotation from a nurse);

Access control rule:

M.12 Necessary to provide alert features for the different services on a system (to prevent and detect downtime in a faster way).

Category: *Paper vs Digital records*

Sub-category: *Problems with the digital record;*

Insight: Once you access the digital record you can access everything about a patient;

Support notes from the discussions: "At this moment the paper record is more secure…you need to go there and make a request to take it with you...with digital record I can just print it out and take it home with me..." (Quotation from a doctor);

Access control rules: not applicable for this sub-category.

Sub-category: *Problems with the paper record;*

Insight: It is easier to correct/change paper records;

Support notes from the discussions: "…I think it [digital record] is more secure than the paper one where the administrative personnel and everybody can just grab it...at least [with the digital record] there is an auditing of who accessed what and when...with the paper no one knows who accessed and saw it..." (Quotation from a technician);

Access control rules: not applicable for this sub-category.

Sub-category: *Problems of the digital record;*

Insight: With electronic records more and more paper is spent and accessing electronic information should be more longitudinal;

Support notes from the discussions: "…paper records I cannot take home while electronic records I can print and take home…" (Quotation from doctor1); "Information systems are an

annoying aspect…whoever hasn't started working while they were young, does not like…to design a proper information system everything must be done with a proper discussion in the departments…we don't have proper informatics departments…" (Quotation from doctor2);

Access control rules: not applicable for this sub-category.

Sub-category: *Types of use;*

Insight: Only one type of record should be available, not a mixture of both;

Support notes from the discussions: "What happens now is that there is not only one or the other…" [paper and electronic records] (Quotation from a nurse);

Access control rules: not applicable for this sub-category.

6.2.2.2 Patients

Category: ***Access by patients***

Sub-category: *Require HCP support*;

Insight: Access with the help of a professional is needed;

Support notes from the discussions: "…ideally would be to have always a healthcare professional to help" (Quotation from a technician) ; "...accessing information with a professional and explaining them any doubts they may have can make a big difference..." (Quotation from a doctor);

Access control rule:

M.13.1 Patients must be able to access their record, either paper or electronically, with the help of a HCP.

(This rule and the following two include any kind of format, the law does not specify that the access must be done with paper or electronically).

Sub-category: *Illiteracy and ignorance*;

Insight: Access to the record not as it is but in a way patients will understand because they may not have the capacity to understand;

Support notes from the discussions: "...they [patients] cannot interpret it [medical record] and it can be very complicated..." (Quotation from a nurse); "...there are patients that cannot understand the technical terms and if the person reads that [record] it will not understand what it means..." (Quotation from a technician); "...I think they will not understand anything...they have no capacity..." (Quotation from a doctor);

Access control rule:

M.13.2 Patients must be able to access their record, either paper or electronically, as a summarized/simpler record.

Sub-category: *Access to what the patient wants;*

Insight: It is appropriate, if the information is only about that patient;

Support notes from the discussions: "I think the record should not be available to the patients. If they want to access it they have the right but those who do not want will end up seeing it as well if it is available to everybody." (Quotation from a nurse).

Sub-category: *Legislation and rights;*

Insight: It is appropriate [to access the medical record], if the information is only about that patient;

Support notes from the discussions: "It is in the law that they [patients] must have access..." (Quotation from a nurse); "The record belongs to the patients so they must have access to everything." (Quotation from a doctor).

Access control rule:

M.13.3 Patients must be able to access their record, either in paper form or electronically, without any modifications.
(This rule was extracted from the last 2 sub-categories: *Access to what the patient wants* and *Legislation and rights*).

6.2.3 Mixed methods – insight sheets and rules from the structured questionnaires

This section describes the insights that arose from a more detailed analysis of the structured questionnaires. These insights refer to most of the main categories presented in Table 5.5. The support notes in this case are the data obtained from the structured questionnaires.

6.2.3.1 Healthcare professionals

Category: ***Access in emergency situations***

Insight: A majority of respondents 20 (81%) agreed with the existence of providing access in emergency situations depending on the situation and on the HCPs;

Access control rules:

M.1.1 Specific roles must be able to BTG and access (read only) information in emergency, or any other unanticipated extreme situations.

M.1.2 It must be possible to define a fine-grained BTG (i.e., it may depend on the roles as well as time, location and other restrictions).

(In this rule it was added not only the type of situation but other constraints that can be useful to define depending on the environment and goals of the institution or department, such as time, location, even task, etc).

Category: *System access (authentication)*

Insight: Most respondents use login and password as authentication mechanisms 22 (82%), 4 of them together with biometrics (e.g., fingerprint):

- 17 (65%) participants answered that they access the EMR easily with login and password mechanisms although 4 (15%) said they share logins and passwords;

Access control rule:

M.3 Different types of authentication mechanisms must be available to be adapted according to the user needs (most common are login/password + biometrics).

Category: *Access control roles*

Insights:

- 25 (92%) respondents agreed with the existence of access control roles in order to access EMR by professional category (n=19), by the type of information (n=15), by the department where they work (n=11), while 4 said that patients should be the ones to define the access control roles (respondents could choose more than 1 option);
- While 16 (59%) people use access control roles (13 according to the professional category) in the EMR they usually work with, 9 (56%) said the roles are not adequate, 5 (31%) said they are and 6 (37,5%) had no opinion;
- 25 (92%) respondents said that they did not participate in the definition/choice of these access control roles;

Access control rule:

M.14 Access control roles must exist depending on the professional category and/or type of information.

Category: *Access control policies*

Insights:

- Most respondents stated they never participated in the definition of access control policies 22 (82%) while 5 (18%) said they did;

- The same number of people 22 (82%) said they should be able to participate in that definition (21 in the idea and conceptualization, 14 in defining the policies, 15 in the implementation and 16 in the testing) while 3 said no (respondents could choose more than 1 option);

Access control rules: not applicable for this category.

Category: *System access solutions*

Insight: HCP said that using an ATM is not a solution for patient access to their medical records;

Access control rules: not applicable for this category.

Category: *Security*

Insight: EMR security problems: most respondents said that EMR allows easy sharing of sensitive information 17 (63%), access control can be a security problem 15 (56%), EMR is not secure in general 6 (22%) and they do not trust it 5 (19%);

Access control rules:

M.15 IT support roles must exist in order to deal with problems more rapidly and efficiently (e.g., logged time responses, alert to responsible people when time is expired, etc).

6.2.3.2 Patients

Category: *Access by patients*

Insight: Regarding the access by patients to their medical records using an ATM:

- 17 (63%) respondents said they do not agree, 6 (22%) answered they do while 4 (15%) had no opinion;
- 18 (67%) remarked that this system was not secure: most problems are related with ethical issues (n=13) and the feeling that is not secure enough (n=13) (respondents could choose more than 1 option); while 7 (26%) said it was;
- 21 (81%) respondents said they access an ATM to withdraw money on a regular basis and 4 (15%) of them every day.

Access control rules: not applicable for this category.

Category: ***Access control roles***

Insight:

- 25 (92%) respondents agreed with the existence of access control roles in order to access EMR:
  - by professional category (n=19)
  - by the type of information (n=15)
  - by the department where they work (n=11)
  - while 4 said that patients should be the ones to define the access control roles (respondents could choose more than 1 option);

Access control rule:

M.16 There must exist the option for patients to define access control roles in some situations.

6.2.4 Mixed methods – insight sheets and rules from the structured telephone interviews

This section describes the insights that came up in a more detailed analysis of the structured telephone interviews. These insights refer to most of the main categories presented in Table 5.10. The support notes in this case are the data obtained from the structured telephone interviews.

6.2.4.1 Healthcare professionals

Category: ***Access in emergency situations***

Insight: A vast majority of respondents 195 (97%) agreed that mechanisms should be available to allow any HCP to access patient medical records in an emergency situation;

Access control rule:

M.1 Specific roles must be able to BTG and access (read only) information in emergency situations.

Category: ***Access control roles***

Insights:

- Most respondents 141 (71%) said that access control roles should be provided to protect medical data;
- The three main ways to do this should be:
  - By professional category (60% - 83);
  - Defined by the patients (25% - 34);

- Defined in other ways (doctor with patient, family members, only family doctor, etc) (18% - 25);

Access control rule:

M.14 Access control roles must exist depending on the professional category and/or type of information.

Category: *System access solutions*

Insights:

- When asked about a system access solution such as an ATM machine, most respondents said they would not like to use it to access their medical records 112 (56%);
- For the ones that said they would 83 (42%), the most frequent accesses would be:
  - 1 to 3 times per month 30 (37%);
  - less than once per month 47 (58%);

Access control rules: not applicable for this category.

Category: *Security*

Insight: There is a balance between the feeling of security within the EMR, 82 (41%) respondents said that medical data within a computer does not affect its security, while 85 (42%) think that it might;

- most respondents were worried about the confidentiality of the records;
- about the security of accessing medical records via an ATM, the majority of respondents said it is secure 55 (68%);

Access control rules: not applicable for this category.

6.2.4.2 Patients

Category: *Access control policies*

Insight: From 199 valid answers, 142 (71%) respondents said that they would like to define who should access their medical records;

Access control rule:

M.16 There must exist the option for patients to define access control roles in some situations.

Category: *Access by patients*

Insights:

- Most respondents would like to access their medical records 131 (65%) whenever they wanted:
  - with the help of a HCP 102 (77%);
  - with the use of a computer 102 (77%);
- Most respondents agreed that their medical records should be available 24/7 164 (82%);

Access control rule:

M.17 Patients must be able to access their record as in rules M.13.1, M.13.2 & M.13.3 with the use of a computer.

Category: *Access control roles*

Insights:

- Most respondents 141 (71%) said that access control roles should be provided to protect medical data;
- The three main ways to do this should be:
  - By professional category 83 (60%);
  - Defined by the patients 34 (25%);
  - Defined in other ways (doctor with patient, family members, only family doctor, etc) 25 (18%);

Access control rules:

M.16 There must exist the option for patients to define access control roles in some situations.

M.18 There must exist the option of defining access control roles for several different cases. For example, groups of people that could define those access control roles could be: a doctor with a patient, a doctor with a family member (when a patient cannot do it), only the family assisting doctor, etc.

Category: *System access (authentication)*

Access control rules: not applicable for this category.

6.3 Role based access control rules

The list of preliminary access control rules defined in the previous section (Section 6.2) must be refined as there are similar rules that need to be merged as well as some rules that are not directly related to access control. Figure 6.1 presents the method used to refine and achieve the final list of RBAC rules. An example of how these rules can be ultimately transformed into RBAC-Access Control Framework (ACF) [17] rules is presented in Section 6.3.3.

All the access control rules were defined in the positive, so they are all defined with an allow permission.

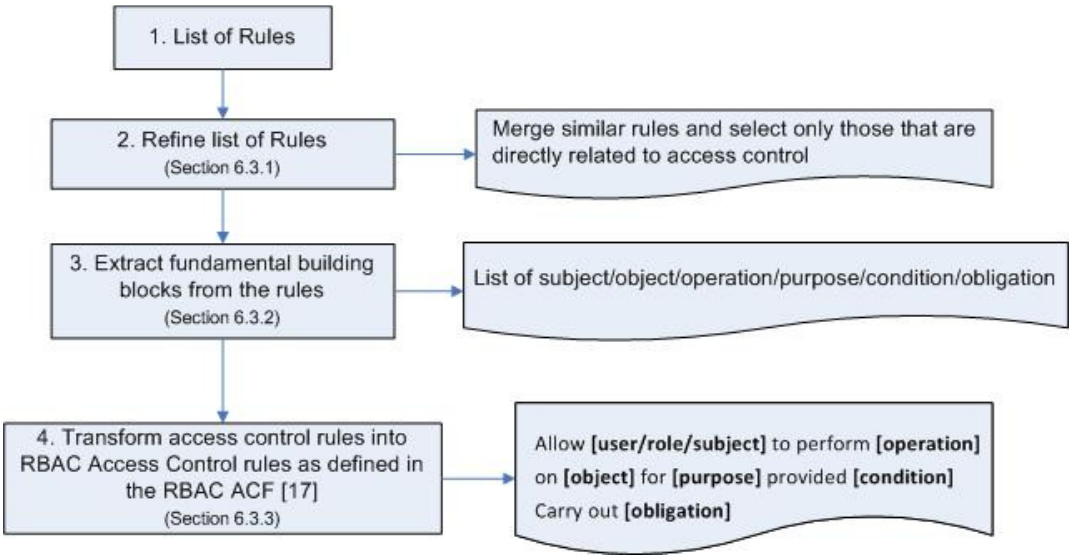

Figure 6.1 – Process of reaching a list of standardized RBAC rules.

6.3.1 Refined list of access control rules

Tables 6.1 and 6.2 present the lists of refined access control rules from both legislative and mixed methods.

6.3.1.1 Legislative rules

Table 6.1 – Numbered list of the legislative access control rules for HCP and patients.

Rule no	HCP Access control rules
L.1	*Patient consent must be sought where required.*
L.2	*Medical data collection and processing purposes must be defined before they are performed (it includes scientific research). Any changes in the original purposes mentioned must be communicated to the patient*
L.3	*Medical data should only be collected and processed by healthcare professionals or individuals or bodies working on behalf of healthcare professionals*
L.8	*Appropriate measures must be available to protect against unauthorized access*
L.9	*It must be possible to prevent the unauthorised consultation of processed personal data*
L.10	*It must be possible to prevent automated data processing systems from being used by unauthorised persons by means of data transmission equipment*
L.11	*It must be possible to enable the separation of: identifiers and data relating to the identity of persons; administrative data; medical data; social data and genetic data (access control)*
L.12	*It must be possible to guarantee the possibility of checking and ascertaining to which persons or bodies personal data can be communicated by data transmission equipment*
L.13	*It must be possible to guarantee that it is possible to check and establish a posteriori who has had access to the system and when*
L.14	*Providers of information, communication and health services should under all circumstances be identifiable including the final owner or provider*
	Patient Access control rules
L.4	**Integrated into rule M.14 of Table 6.2**
L.5	*If the domestic law permits the patient may appoint a person to access his/her medical data on his/her behalf*
L.6	*Patients may ask for their medical data to be corrected*
L.7	*Access to medical data by patients may be refused, limited or delayed under certain circumstances (i.e., defined by the HCPs)*

6.3.1.2 Mixed methods rules

Table 6.2 – Numbered list of the mixed methods access control rules for HCP and patients.

Rule no	HCP Access control rules
M.1	*Specific roles (with a fine-grained definition that may depend on roles, time, location and other restrictions) must be able to BTG and access (read only) information in emergency (or other unanticipated) situations; logging and audit must be provided at all times*
M.1.1	**Integrated into rule M.1**
M.1.2	**Integrated into rule M.1**
M.2	**Integrated into rule M.1**
M.3	**Not an access control rule**
M.4	**Integrated into rule M.1**
M.5	**Not an access control rule**
M.6	**Integrated into rule M.8**
M.7	**Obligation. Alert responsible person after a defined number of accesses.**
M.7.1	**Integrated into rule M.7**
M.8	*The definition of access control roles must be fine-grained and include exceptions to roles (users can have more or less permissions than the role assigned to them); logging and audit must be provided at all times*
M.8.1	**Integrated into rule M.8**
M.8.2	*The Head of Department (or responsible role) must be able to assign one or more people the right to alter some access permissions for some roles (these alterations can be associated with some constraints) and this must be logged and securely audited*
M.8.3	**Integrated into rules M.8 & M.8.2**
M.9	**Integrated into rule M.8.2**
M.10	**Integrated into rule M.8.2**
M.10.1	**Integrated into rule M.8.2**
M.10.2	**Integrated into rules M.8 & M.8.2**
M.11	**Integrated into rules M.8 & M.8.2**
M.12	**Similar as M.7**
M.14	*Access control roles must exist depending on the professional category and/or type of information*
M.15	*IT support roles must exist in order to deal with problems more rapidly and efficiently*
	Patient Access control rules
M.13.1	*Patients must be able to access their record in paper or electronically with the help of a healthcare professional*
M.13.2	*Patients must be able to access their record in paper or electronically as a summarized/simpler record*
M.13.3	*Patients must be able to access their record in paper or electronically as it is*
M.16	*There must exist the option for patients to define access control roles in some situations*
M.17	**Integrated into rules M.13.1, M.13.2 and M.13.3**
M.18	*There must exist the option of defining access control roles for several different cases. [For example, groups of people that could define those roles could be: a doctor with a patient, a doctor with a family member (when a patient cannot do it), only the family assisting doctor]*

6.3.2 Fundamental building blocks

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 (the effect) to a particular subject for a particular data object. For the rules defined here the effect is always GRANT or allow because they are all described in the positive. Therefore there is no need to repeat it in each rule. Obligations are additional actions to be performed when the access control rule is triggered. The purpose has usually two objectives: business or data purpose [17].

The fundamental building blocks used to perform step 3 of Figure 6.1 comprise the following concepts:

subject/object/operation/purpose/condition/obligation

Lists of legislative, standards and mixed methods access control rules for HCP and patients are presented in Tables 6.3, 6.4 and 6.5.

Table 6.3 – Fundamental building blocks for the list of legislative access control rules for both HCP and patients.

ID	Subject	Operation	Object	Purpose	Condition	Obligation	Related rules
1	HCP	Processing (reading & updating)	Medical data except patient personal ID data	Scientific research & other defined purposes		Record all details including User ID in audit trail	**L.2, L.3, L.8, L.9 L.10, L.12 L.13, L.14**
2	Individual(s)	Processing (reading & updating)	Medical data except patient personal ID data	Scientific research & other defined purposes	Working on behalf of HCP	Record all details including User ID in audit trail	
3	Member of organization X	Processing (reading & updating)	Medical data except patient personal ID data	Scientific research & other defined purposes	Organization X working on behalf of HCP	Record all details including User ID in audit trail	
4	HCP	Creation (collection)	All patient medical data	Defined purposes (e.g., treatment)		Tell the patient that a record has been created for defined purposes & Record all details including User ID in audit trail	**L.2, L.3, L.8, L.9, L.10, L.12, L.13, L.14**
5	Individual(s)	Creation (collection)	All patient medical data	Defined purposes (e.g., treatment)	Working on behalf of HCP	Tell the patient that a record has been created for defined purposes & Record all details including User ID in audit trail	
6	Member of organization X	Creation (collection)	All patient medical data	Defined purposes (e.g., treatment)	Organization X working on behalf of HCP	Tell the patient that a record has been created for defined purposes & Record all details including User ID in audit trail	
7	HCP	Update	Purpose of medical record			Tell the patient that the purpose had been changed & Record all details including User ID in audit trail	
8	Individual(s)	Update	Purpose of medical record		Working on behalf of HCP	Tell the patient that the purpose had been changed & Record all details including User ID in audit trail	

9	Member of organization X	Update	Purpose of medical record		Organization X working on behalf of HCP	Tell the patient that the purpose had been changed & Record all details including User ID in audit trail	
10	HCP	Processing (reading & updating)	Patient personal ID	Treating patient		Record all details including User ID in audit trail	**L.3, L.8, L.9, L.10, L.11, L.12, L.13**
11	Individual(s)	Processing (reading & updating)	Patient personal ID	Treating patient	Working on behalf of HCP	Record all details including User ID in audit trail	
12	Member of organization X	Processing (reading & updating)	Patient personal ID	Treating patient	Organization X working on behalf of HCP	Record all details including User ID in audit trail	
13	HCP	Processing (reading & updating)	Genetic data	Treating patient		Record all details including User ID in audit trail	
14	Individual(s)	Processing (reading & updating)	Genetic data	Treating patient	Working on behalf of HCP	Record all details including User ID in audit trail	
15	Member of organization X	Processing (reading & updating)	Genetic data	Treating patient	Organization X working on behalf of HCP	Record all details including User ID in audit trail	
16	HCP	Processing (reading & updating)	Social data	Treating patient		Record all details including User ID in audit trail	
17	Individual(s)	Processing (reading & updating)	Social data	Treating patient	Working on behalf of HCP	Record all details including User ID in audit trail	
18	Member of organization X	Processing (reading & updating)	Social data	Treating patient	Organization X working on behalf of HCP	Record all details including User ID in audit trail	
19	HCP	Processing (reading & updating)	Administrative data	Treating patient		Record all details including User ID in audit trail	
20	Individual(s)	Processing (reading & updating)	Administrative data	Treating patient	Working on behalf of HCP	Record all details including User ID in audit trail	
21	Member of organization X	Processing (reading & updating)	Administrative data	Treating patient	Organization X working on behalf of HCP	Record all details including User ID in audit trail	
22	HCP	All operations	Medical data & Patient personal ID	All purposes	With patient consent	Record all details including User ID in audit trail	**L.1, L.3, L.11, L.12, L.13, L.14**
23	Individual(s)	All operations	Medical data & Patient personal ID	All purposes	Working on behalf of HCP & With patient consent	Record all details including User ID in audit trail	**L.1, L.3, L.12, L.13, L.14**
24	Member of organization X	All operations	Medical data & Patient personal ID	All purposes	Organization X working on behalf of HCP & With patient consent	Record all details including User ID in audit trail	
25	Named Person (HCP/Individual)	Processing (reading & updating)	Medical data & Patient personal ID	(to be defined)	On behalf of the patient	Record all details including User ID in audit trail	**L.5, L.6, L.7, L.12, L.13, L.14**

Legislation can provide basic generic access control rules that define the minimum rules to integrate into any access control policy in the healthcare domain. However, these rules are too lax. They allow any HCP to access any identifiable patient medical record. More fine-grained rules are needed. Next, a table with access control rules extracted from the access control standard for healthcare - the EN 13606-4:2007 standard [69], described in Section 4.2.3, is presented in Table 6.4. The role hierarchy defined within the standard is as follows (Figure 6.2):

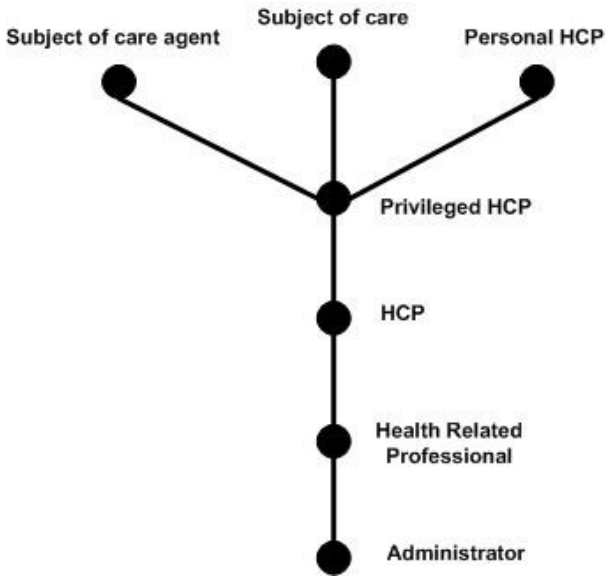

Figure 6.2 – Functional role hierarchy as defined in the CEN standard, EN 13606-4:2007 [69].

The standard rules 26 to 35 can easily translate rules M.1, M.8, M.13, M.14 and M.18 obtained from the mixed methods that are closely related to the definition and management of access control roles.

Although standards can define more specific rules than legislation, they are still too generic and deficient.

For example, in this case, the subject of care (patient) can update everything in the record. So there is the need for more control and closer to practice rules that can model access control actions within an EMR. Table 6.5 presents the fundamental building blocks that were created for the mixed methods access control rules that were not already covered by the previously specified rules (Tables 6.3 and 6.4). These access control rules complement the previous defined rules with more specific patient access control rules and other fine-grained rules for the already defined subjects.

Table 6.4 – Fundamental building blocks for the access control rules defined within the healthcare access control standard EN 13606-4:2007 [69].

ID	Subject	Operation	Object	Purpose	Condition	Obligation	Related rules
26	Administrator	Read & write	Care Management data		Include exceptions if needed (optional)	Record in audit trail	**M.8, M.14**
27	Health related professional	Read & write	Clinical Management data		Include exceptions if needed (optional)	Record in audit trail	
28	Health professional	Read & write	Clinical care data		Include exceptions if needed (optional)	Record in audit trail	
29	Privileged healthcare professional	Read & write	Privileged Care data		Include exceptions if needed (optional)	Record in audit trail	
30	Privileged healthcare professional	Break The Glass	Privileged Care data	Emergency care	(depending upon time/location)	Record in audit trail	**M.1**
31	Privileged healthcare professional	Read & write	Privileged Care data	Emergency care	If Glass is broken	Record in audit trail	
32	Privileged healthcare professional	Read & write	Personal Care data		If mandate granted	Record in audit trail	**M.8**
33	Personal healthcare professional	Read & write	Personal Care data		Include exceptions if needed (optional)	Record in audit trail	**M.8, M.14**
34	Subject of care agent	Read & write	Personal Care data			Record in audit trail	**M.14, M.18**
35	Subject of care	Read & write	Personal Care data		With help of an HCP (optional)	Record in audit trail	**M.13.1, M.13.2, M.13.3 M.14**

Table 6.5 – Fundamental building blocks for the HCP and patients' list of access control rules from the mixed methods research results.

ID	Subject	Operation	Object	Purpose	Condition	Obligation	Related rules
36	Patient	Update	Access control rules for own record	N/a	In defined situations	Record in audit trail	**M.16**
37	Head of Department	Update	Access control rules	N/a		Record in audit trail	**M.8.2**
38	Head of Department	Delegate modification	Access control rules	N/a	(to be defined)	Record in audit trail	
39	Patient	Read only	Medical data	All	If HCP agrees (optional)	Record in audit trail & create summarized record	**M.13.1, M.13.2, M.13.3**
40	Personal HCP	Update	Access control rules for patient record	N/a	(to be defined)	Record in audit trail	**M.18**
41	IT Personnel	Update	Access control rules	N/a	In defined situations & if mandate granted	Record in audit trail & ask for justification later	**M.15**

6.3.3 Role based access control framework rules

The RBAC model can be extended with additional entities and relationships to become a privacy-aware RBAC model. This model can support evaluation of privacy policies for practical application domains. As in authorization using RBAC Access Control Framework (ACF), the privacy rules are defined using the concepts presented in Section 6.3.2 [17]. The access control evaluation rules can be defined as (Step 4 of Figure 6.1):

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

The driving motivation for using the RBAC standard is to simplify security policy administration while facilitating the definition of flexible customized policies. Although RBAC is often considered a single access control and authorization model, it is in fact composed of a number of models each fit for a specific security management application [17].
One of the potential improvements of the RBAC standard is the augmentation of obligations, which are tasks and requirements to be fulfilled together with the enforcement of authorization decisions [95].
Each of the rows presented in Tables 6.3, 6.4, and 6.5 can be transformed into an RBAC-ACF rule of the form:

1. Allow **[HCP]** to perform **[processing (reading & updating)]**
   on **[medical data, except patient personal ID data]**
   for **[scientific research & other defined purposes]**
   Carry out **[record in audit trail]**

The rules presented in this chapter are now assessed to determine which can be modelled by the RBAC standard and which cannot. The result of this analysis showed that rules 30 and 31 cannot be modelled using the existing RBAC model. Therefore, the next step is to develop an access control model that can model all the access control rules that were generated and presented here. This access control model (the BTG-RBAC model) is presented in Chapter 7.

6.4 Summary of results

Figure 6.3 presents the results obtained from each step of the GT data analysis.

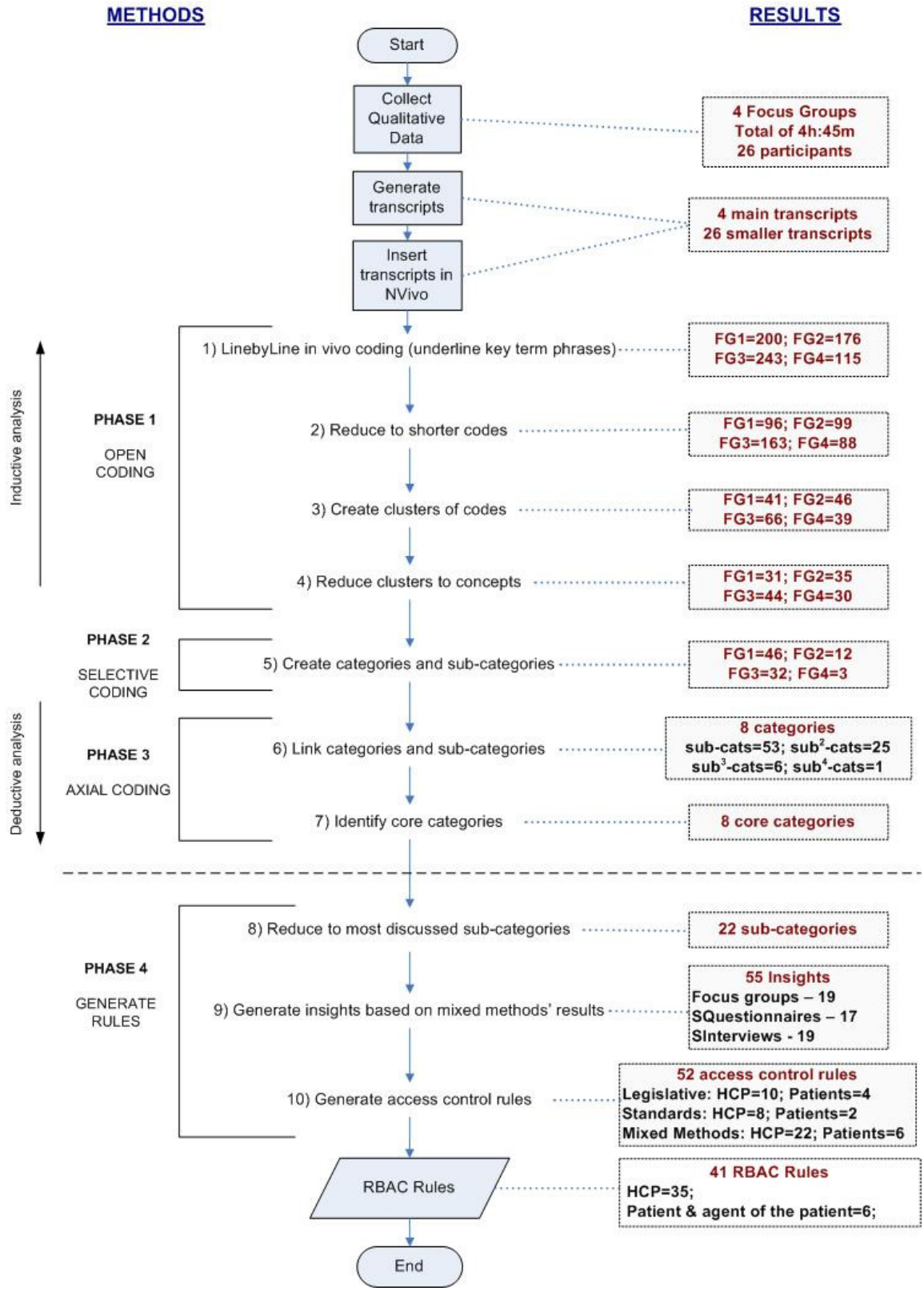

Figure 6.3 – Results from each step of the grounded theory data analysis.

6.5 Discussion

This chapter presents the access control rules that resulted from the application and analysis of mixed methods research that was described in Chapter 5 and describes, in detail, the process of extracting these rules from the insight sheets that were created for each of the applied methods. These are then combined with both legislative and standard rules that were generated in Chapter 4.

The list of access control rules that was generated (41 RBAC rules in total: 35 for HCP, 2 for an agent of the patient and 4 for the patients) integrate access control procedures, guidelines and definitions described within the healthcare legislation, standards and user needs. The reason for choosing an approach that integrates so many different issues for access control in healthcare is justified within this chapter. This justification starts to become visible when legislative rules start to appear. It is clear that, although they can comprise a minimum set of basic access control rules, these are too generic and too lax, for instance, for the HCP. In order to complement these rules, access control definitions from healthcare access control standards were included. These were mainly targeted for the definition of access control roles. However, these access control definitions are still too generic as they allow too much permission for the patients accessing their medical records. Again, there is the need to tighten up a bit more the access control rules in order to reflect users' needs closer to the healthcare practice. And this is where the access control rules resulting from the mixed methods can be used to further complement the final list of rules.

The final list of access control rules has therefore integrated the generic and specific issues that are needed to define a more complete access control policy for healthcare. Note however that this is still a generic list of rules that need to be adapted and refined for actual healthcare domains, for example, by specifying additional roles, additional subclasses of information, additional purposes and so on, that are applicable to the domain in question.

Finally, there are some resulting access control rules, which refer to the BTG operation that cannot be modelled by the existing access control models, including the RBAC model. The next step is to define an extension of the RBAC model that can include these rules to be modelled in a standardized fashion. This new model (BTG-RBAC model) is presented in detail in Chapter 7.

7 THE BTG-RBAC: PROPOSAL OF A NEW MODEL

7.1 Introduction

Most of the access control rules that were generated in Chapter 6 can be expressed as RBAC rules when the core RBAC model is augmented with obligations [95]. There are however exceptions: rules 30 and 31 where a BTG operation is mentioned (Section 6.3.2, Table 6.4). These rules cannot be expressed by the RBAC model because a BTG operation implies that the access control policy is "broken" or "breached" in a controlled manner for a certain period of time. For this to be achieved in a secure way, a new access control model must be defined. This new model is described in this chapter.

7.2 The BTG-RBAC model development

This section introduces and describes an extension of the Core RBAC model with obligations to include the BTG operation. This model is a new access control model and is named the BTG-RBAC model.

7.2.1 Break-The-Glass

Traditional access control policies are designed to be restrictive. The assumption is that users prefer to have unrestricted access to everything so they need to be strictly controlled. Consequently, access control implementations focus mainly on avoiding security breaches and consequently they do not always best serve the user's needs and purposes. Access control policies that are instead defined with maximum freedom of access and, at the same time, maximum user responsibility for any exceptional actions taken, are preferable to traditional ones. *Maximum freedom* means that the system must provide mechanisms for the users to access the requested information at all times, whenever it is needed. *Maximum user responsibility* means that the system must provide mechanisms to show the user (who takes an exceptional action) an alert message making him/her aware that he/she is trying to access information he/she is not normally authorized to access. This makes the user responsible for what he/she is doing and all the actions he/she may subsequently take; the system must provide mechanisms to notify automatically all responsible parties so that the user's actions can be justified afterwards to them [35].

As an example, an application domain where BTG is an essential feature is healthcare.
According to legislation, the HIPPA act specifies the need for BTG [96] as is described in [97]. BTG is needed when normal access controls to processes are insufficient and an emergency access control mechanism is required. Examples of emergency situations that

might require BTG could be account problems (e.g., a user has not been given the proper roles or permissions) or authorization problems (e.g., an emergency situation such as hurricane Katrina thrusts an individual into a role that lacks sufficient access rights to perform the needed actions). A similar concept is the one described in the National Health Service (NHS) documentation as *break the seal* on sealed documents [98]. The idea is that patients have the right to seal information. They can place access restrictions on parts of their medical records. An email alert is raised when the seal is "broken" and a privacy officer investigates if the action taken was justifiable or not. Moving from legislation to practice, [35] presents a good example of where BTG is needed and describes an access control policy that was defined by HCPs where BTG is included (mainly doctors who stated that BTG was a very important feature to be integrated within the policy and the system that was to be implemented).

BTG is a required aspect both in terms of generic and theoretical as well as practical issues, so it needs to be integrated in a transparent and modular way in the domain where it is needed and within the access control policy and model that is developed within any IS.

7.2.2 The core RBAC model

The American National Standards Institute (ANSI) standard Core RBAC model consists of five basic elements [16], which are the USERS, ROLES, OPS (operations), OBS (objects), and SESSIONS, and five relations, which are (Figure 7.1):

- **UA**: User-Assignment $\in$ USERS x ROLES, a many-to-many mapping user-to-role assignment relation;
- **PA**: Permission-Assignment $\subseteq$ PRMS x ROLES, a many-to-many mapping permission-to-role assignment relation;
- **U-S**: user_sessions (u: USERS) $\rightarrow$ $2^{SESSIONS}$, the mapping of user *u* onto a set of sessions;
- **S-R**: session_roles (s: SESSIONS) $\rightarrow$ 2^{ROLES}, the mapping of session *s* onto a set of roles;
- **PRMS**: $2^{(OPS \times OBS)}$, the set of permissions; Op(p: PRMS) $\rightarrow$ {op $\subseteq$ OPS}, the permission-to-operation mapping, which gives the set of operations associated with permission *p*; Ob(p: PRMS) $\rightarrow$ {ob $\subseteq$ OBS}, the permission-to-object mapping, which gives the set of objects associated with permission *p*.

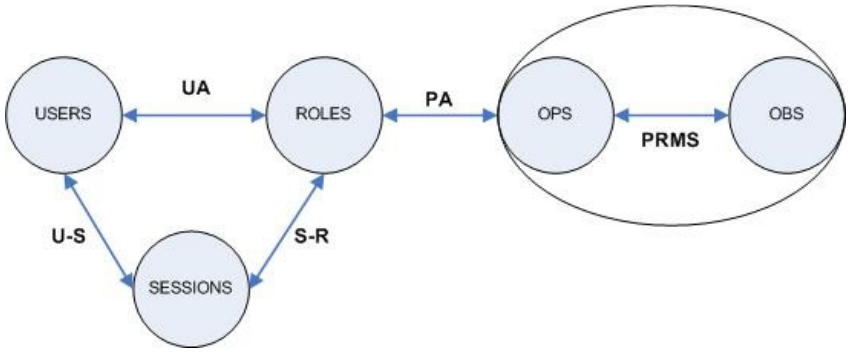

Figure 7.1 – The Core RBAC Model [99].

The authorization decision making function *CheckAccess* describes how a decision is made within the Core RBAC model by taking as inputs the current session, the requested operation and the target object and returns a Boolean value as a result to indicate whether the request is authorized or not.

$$\text{CheckAccess} : \text{SESSIONS} \times \text{OPS} \times \text{OBS} \longrightarrow \text{BOOL}$$

$$\text{CheckAccess(s,op,ob)} \;=\; (\exists r \in ROLES : r \in S - R(s) \wedge ((op, ob), r) \in PA)$$

The *CheckAccess* function checks if a role *r* can be mapped for the current session *s*, such that *r* has been allocated the permission to perform the operations *op* on the objects *ob*. If such a value exists, the function returns TRUE (GRANT) if not, FALSE (DENY) will be returned.

The steps to access a resource by a user with the Core RBAC model are as follows (Figure 7.2):

1. The user sends an *access application resource* request to the application;
2. The application contacts the authentication service to authenticate the user;
3. The authentication service returns the authenticated identity of the user to the Application;
   (If authentication fails, a reject message is sent from the application to the user and the request terminates here)
4. The application calls the RBAC policy engine passing the session details, the requested operation and requested object (*CheckAccess*);
5. The RBAC engine returns GRANT to the application;
   (or DENY, in which case a reject message is sent from the application to the user and the request terminates here)
6. The application makes the requested operation to the resource;
7. The resource returns the results to the application;
8. The application returns the results to the user.

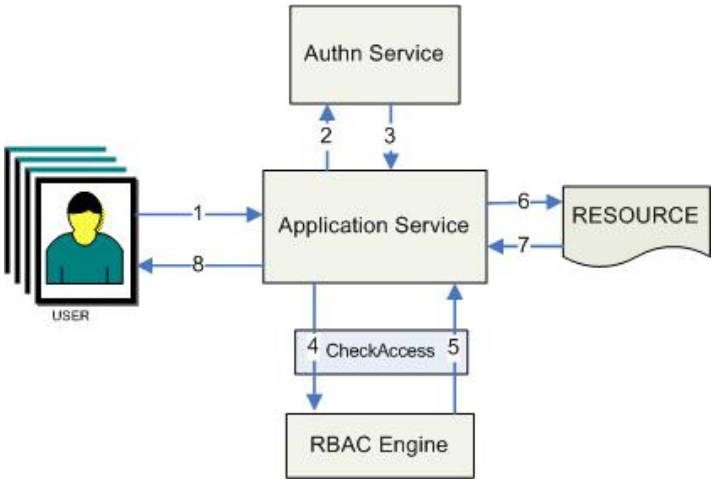

Figure 7.2 – Core RBAC interactions diagram.

7.2.3 The core RBAC model with obligations

In order to augment the Core RBAC model with obligations a new basic element OBLGS is introduced in [95], which is the set of valid obligations. The PRMS relation is replaced by a new relation OPRMS defined as:

$$OPRMS = PRMS \times 2^{OBLGS}$$

The PA relation is replaced by a new relation, the Permission-Obligation Assignment relation (POA) which is defined as follows:

$$POA \subseteq OPRMS \times ROLES$$

oprm ∈ OPRMS, and *oprm* is an obligation augmented permission: *oprm = (r,prm,oblgs).* This specifies that if the permission *prm* is granted to role *r* through *oprm* and is exercised by the role *r*, the set of obligations *oblgs* must be fulfilled (Figure 7.3). [95] also describes how the RBAC model can be augmented with obligations on DENY. In order to retrieve the obligations along with the authorization decisions, the *CheckAccess* function is enhanced to:

$$\text{CheckAccess: SESSIONS} \times \text{OPS} \times \text{OBS} \longrightarrow \text{BOOL} \times 2^{\text{OBLGS}}$$

The possible results from *CheckAccess* are now:

- (FALSE, Ø)→ DENY access to resource
- (FALSE, 2^{OBLGS})→ DENY access to resource AND perform Obligations on DENY
- (TRUE, Ø)→ GRANT access to resource
- (TRUE, 2^{OBLGS})→GRANT access to resource AND perform Obligations on GRANT

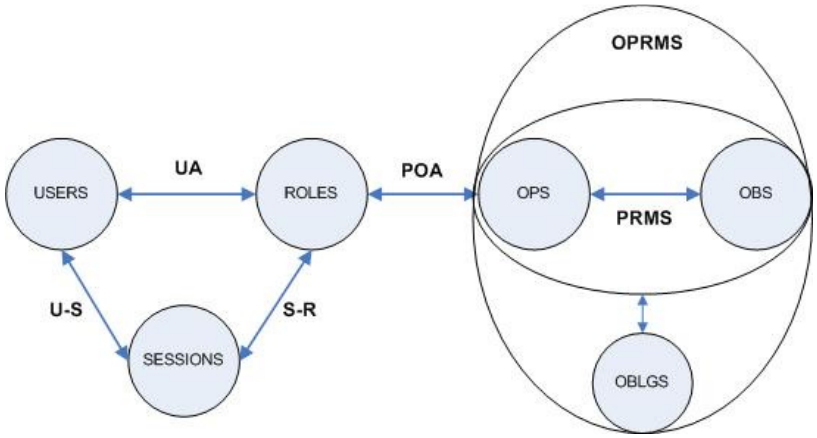

Figure 7.3 – The Core RBAC model with Obligations.

The steps to access a resource by a user with the Core RBAC augmented with obligations are the same as described in Core RBAC with the added step of retrieving and performing obligations, if they exist.

7.2.4 The simple BTG-RBAC model

The BTG-RBAC model includes the BTG functionality within the RBAC engine (Core RBAC model with BTG) assuming that a state based engine is available in order to alter the BTG state of a policy rule. With this assumption, the changes to be made to include BTG are minimal and are described below.

In order to integrate BTG within the Core RBAC model, the BTG-RBAC engine is introduced. This engine holds the BTG state of each permission in the system. Initially the BTG state of each permission is set to FALSE, but it can be set to TRUE if there is a policy rule that allows a user to perform the BTG operation O^{BTG} on a particular resource. BTG-RBAC is accessed via an enhanced *CheckAccess* procedure, which has been called *CheckBTGAccess*. It returns one of three decision values to the application: GRANT, DENY or $P^{BTG(r,op,ob)}$. The value $P^{BTG(r,op,ob)}$ grants the role *r* permission to BTG for the operation *op* on the object *ob*. The operation $O^{BTG(op)}$ refers to the BTG operation on a resource object for a defined operation *op*. The possible results for *CheckBTGAccess* are:

(GRANT)	**IF**	*there is a rule granting the user's active role either the necessary permission, or permission if the BTG state is TRUE and the BTG state is actually TRUE*
($P^{BTG(r,op,ob)}$)	**IF**	*there is a rule granting the user's active role permission if the BTG state is TRUE but the BTG state is FALSE*
(DENY)		*otherwise*

An example of how a simple BTG policy might be specified by a security administrator is presented in Table 7.1.

Table 7.1 – Example of a simple BTG-RBAC policy.

Role	Operation	Object	BTG
r1	read	obs1	-
r2	read	obs1	TRUE

The two policy rules described in Table 7.1 state that role *r1* is allowed to perform the *read* operation on the object *obs1*, and role *r2* is only allowed to perform the *read* operation on object *obs1* if the "glass is broken" i.e., the BTG state is TRUE. Implicit in this rule is the assumption that role *r2* is allowed to perform the BTG operation $O^{BTG(read)}$ on object *obs1*. This implicit rule does not need to be stated explicitly in the simple policy model. The model is easy to understand and the rules are simple to write. When *checkBTGAccess(r2,read,obs1)* is called and if the BTG state variable is TRUE, GRANT will be returned, else $P^{BTG(r2,read,obs1)}$ will be returned. If the user decides to take responsibility to BTG, when *CheckBTGAccess(r2, $O^{BTG(read)}$,obs1)* is called GRANT will be returned (as per the implicit rule) and the BTG state variable for the permission assignment will be set to TRUE by the RBAC engine.

However, there are a number of limitations with the simple policy model. The first limitation is the implied rule and its corresponding assumption that there is one BTG state variable for every permission assignment i.e., Role/Operation/Object combination. This is somewhat inflexible in practice, since it would not allow one role to BTG on a resource and thereby grant another role (or indeed all roles) access to the resource (as can happen when the "glass is broken" on a hotel fire door). Another limitation of the simple model is that the BTG-RBAC system does not know when or how to set the BTG state variable back to FALSE. A final limitation is that in most real life situations, when a subject does BTG, one would normally want to place some obligations on this action, such as notify the manager, write to an audit trail and so on. The following section will address the limitations of the simple model.

7.2.5 The complete BTG-RBAC model

Addressing the limitations that were mentioned previously leads us to a more complex model where:

a) new rules are added describing who is allowed to perform the $O^{BTG(op)}$ operation on a resource (this relaxes the enforced binding between the role that is allowed to BTG and the role that is allowed to access the resource if the "glass is broken");
b) obligations are added to the $O^{BTG(op)}$ permission, allowing administrators to define arbitrary actions that must be performed when the "glass is broken";

c) the granularity of the BTG state variable can be varied from the fixed one state per permission assignment i.e., Role/Operation/Object combination; and
d) rules can be added saying how the BTG state variable is reset to FALSE.

An example of the more sophisticated BTG-RBAC model is exhibited in the policy in Table 7.2.

Table 7.2 – Example of a complex BTG-RBAC policy.

Role	Operation	Object	BTG	Obligations
r1	read	obs1	-	-
r2	read	obs1	BTGi	-
r2	$O^{BTG(read)}$	obs1		oblgs2_btg [Notify Manager; Write to Audit; Reset BTGi to FALSE after 30 mins]
r3	read	obs1	BTGi	oblgs3_btg [Write to Audit]
r4	$reset^{BTG}$	BTGi	-	

BTGi is a state variable of n dimensions over role, operation, object and environment i.e., BTG(r,op,ob,env) and will be described more fully in Section 7.2.6. Table 7.2 states that role *r1* is allowed to *read obs1*, role *r2* is allowed to *read obs1* if the BTG variable *BTGi is TRUE*, role *r3* is allowed to *read obs1* if the BTG variable *BTGi is TRUE* but the system must perform one obligation (*oblgs3_btg*) simultaneously with granting access, role *r2* is allowed to BTG for *reading obs1* but the system must perform three obligations (*oblgs2_btg*) if *r2* does this, and role *r4* is allowed to set the *BTGi state variable to FALSE*. The function *CheckBTGAccess* will now return the results augmented with obligations:

$$\text{CheckBTGAccess:} \quad \text{SESSIONS}\times\text{OPS}\times\text{OBS}\longrightarrow\{\text{T,F},P^{BTG}\}\times 2^{\text{OBLGS}}$$

(GRANT, 2^{OBLGS})	**IF**	*there is a rule granting the user's active role either the necessary permission, or permission if the BTGi state is TRUE, and the BTGi state is actually TRUE*
(P^{BTG})	**IF**	*there is a rule granting the user's active role permission to BTG on the requested object*
(DENY, 2^{OBLGS})		*otherwise*

7.2.6 Resetting the BTGi state variable

After a successful GRANT decision is returned to $O^{BTG(op)}$ there is the need to set the BTGi state variable to TRUE (if it is not already set). The BTG-RBAC model is consequently state based as it needs to remember the state of the BTGi state variables. The writer of the BTG-

RBAC policy determines the dimensions of the BTGi state variables. They could be based on the user's roles, the operation, the object, or environmental parameters such as a time period, etc. An example of various BTGi state variables is given in Table 7.3.

Table 7.3 – Example of BTGi state variables.

Role	Operation	Object	Environment
r2	Read	obs1	30 minutes
*	*	obs2	Daily
*	Write	obs1	*

The first BTGi state variable is dependent upon all 4 dimensions, thus it is only applicable for role *r2* performing operation *Read* on object *obs1*. Because it is time dependent, the BTG-RBAC engine will automatically create a new state variable every 30 minutes. If desired, the administrator could define a different BTGi state variable for the same role (*r2*) performing a different operation (say Delete), on the same object, in the same time period. The second BTGi state variable is for all operations by all roles on object *obs2* on a daily basis i.e., there is a different state variable for each day. If any role has permission to BTG for any operation on *obs2*, it means that once this is done then the state *BTG(obs2)* will be set to TRUE so that any other role with any other BTG permission on *obs2* will have had the "glass broken" for them. The third BTGi state variable is for use by all roles with *Write* permission to object *obs1*. If a role breaks the glass for writing to obs1, this will not affect any role with permission to *Read* obs1. With the use of an *n* dimensional BTGi state array, BTG can be defined in a fine-grained way so that a user can perform BTG with a combination of roles, operations, objects and environmental parameters.

BTGi state variables require a service that can reset each BTGi state variable to FALSE. This can be done automatically, semi-automatically or manually. All three ways are needed. Automatic resetting means that the BTG-RBAC engine itself resets the BTGi state variable to FALSE after a specified event has occurred. The event must be specified by the administrator when creating the BTG-RBAC policy. Example events could be the expiration of a time period such as 30 minutes, or after a certain number of accesses have been made while the BTGi state was TRUE. Automatically resetting the BTGi state to FALSE controls the availability of a resource once the "glass has been broken", and requires a second breaking of the glass after the specified event has occurred, before additional accesses can be granted.
It is not dictated how these events should be specified for the BTG-RBAC engine, or which events should be supported by a BTG-RBAC engine. Each BTG-RBAC engine supplier can specify them.

Semi-automatic resetting of the BTG state is similar to automatic resetting, but it is carried out in a standardised way by a system component that is external to the BTG-RBAC engine. For this, a new function *resetBTGstate (BTGi)* was specified and it must be supported by the BTG-RBAC engine. Any system component may call this function to reset the BTGi variable to FALSE. In this proof of concept, an obligation's service is used as the external system component. Using obligations, the security administrator sets an obligation in the policy rule that describes when the BTG state is to be reset. The events for when this occurs can be similar to the ones for automatic resetting. For example, obligations could be defined as follows: *Obligation set BTGi to FALSE after 30 minutes* or *Obligation set BTGi to FALSE after 3 BTG accesses*. These obligations are returned within 2^{OBLGS_BTG} once the user chooses and is allowed to perform BTG. The obligations will be performed when the events that are defined occur ("after 30 minutes" or "after 3 BTG accesses"). The middle row of the example policy in Table 7.2 gives an example of an obligation that will reset the BTG state to FALSE 30 minutes after it is set to TRUE.

Manually resetting the state means that human intervention must occur before the BTG state is set to FALSE, and policy rules should specify who is allowed to reset the state. This requires a new operation for resetting the state, which has been defined as the $reset^{BTG}$ operation ($reset^{BTG} \in OPS$). This operates on the BTGi state variable as the resource object. The last row of the example policy in Table 7.2 gives an example of a policy rule for manually resetting the BTG state to FALSE. The BTG state will only be reset after the permitted role, *r4*, issues the $reset^{BTG}$ operation on the BTGi state variable.

7.3 The formal BTG-RBAC model and architecture

This section describes in more detail the formal definition of the BTG-RBAC model and presents a visual description of the model architecture. The new features included within the BTG-RBAC model are recorded within Figure 7.4 in italics and bold.

Defining now formally the new relations of BTG-RBAC from the Core RBAC model with obligations, the permission obligation assignment (POA) relation is modified to **POA_BTG** in the new BTG-RBAC model:

$$PRMS\_BTG = OPRMS \times 2^{BTG}$$

$$POA\_BTG = PRMS\_BTG \times ROLES$$

Again, the relation OPRMS is also used in the new model where:

$$OPRMS \subseteq OPRMS\_BTG \quad AND \quad OPRMS\_BTG \subseteq PRMS \times BTGS \times OBLGS$$

The relation POA_BTG for the policy in Table 7.2 would look like:

POA_BTG = {<r1, read, obs1, {}, {}> ; <r2, read, obs1, BTGi, {}> ;
<r2, $O^{BTG(read)}$, obs1, {}, oblgs2_btg> ; <r3, read, obs1, BTGi, oblgs3_btg> ;
<r4, $reset^{BTG}$, BTGi, {}, {}}.

The new BTG-RBAC model is presented in Figure 7.4.

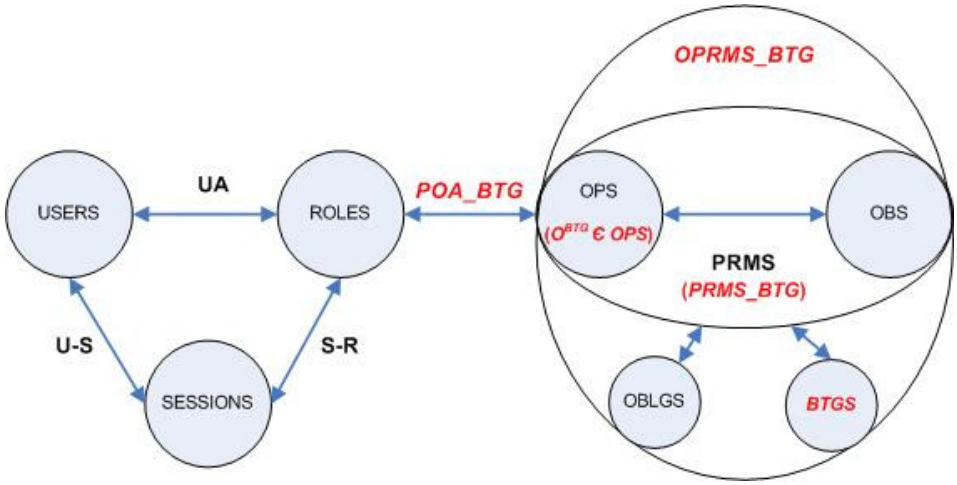

Figure 7.4 – The BTG-RBAC model.

Where BTGS holds the states of the various BTGi variables.

The necessary steps for a user to perform BTG within a resource in the new BTG-RBAC model, assuming that the BTG state is initially FALSE, are as follows (see Figure 7.5):

1. The user tries to access a resource he/she is not authorized to access;
2. The authentication service validates the user's log in credentials;
3. The authentication service returns the authenticated identity of the user;

   (In the case where the authentication service fails, a reject message is sent from the application to the user and the request terminates here)

4. If the user is authenticated, the application calls the BTG-RBAC policy engine passing the session details, the requested operation and requested object (*CheckBTGAccess*):

- In the case where *there is a policy rule granting access to the object*, *CheckBTGAccess* returns GRANT, so it goes to step 9;
- In the case where there is a policy rule granting access to the object if the BTGi state is TRUE, but the value is currently FALSE and the user has permission to $O^{BTG(op)}$, the BTG-RBAC engine returns P^{BTG} as the decision value;
- In all other cases CheckBTGAccess returns DENY and the request terminates here (NOTE: this does imply there may be some policies that grant the user access if the "glass is broken", but the user is not allowed to BTG);

5. The application can now ask the user if he/she wants to BTG on that resource. If the user chooses to BTG (giving a reason for it, if applicable) go to step 6;

(In the case where the user chooses not to BTG the original request terminates here)

6. The application calls the BTG-RBAC policy engine passing the session details, the requested operation ($O^{BTG(op)}$) and the requested object (*CheckBTGAccess*):

- The BTG-RBAC policy engine checks if there is a rule granting the user permissions to perform $O^{BTG(op)}$ on the object, and if so it sets the BTG_i state variable to TRUE and returns any obligations associated with the $O^{BTG(op)}$ operation to the application along with the GRANT response. Otherwise the user is denied permission to $O^{BTG(op)}$ and the process terminates here;

7. The application performs the returned obligations and the user is again shown the option to access the resource he requested and selects it;

8. The application calls the BTG-RBAC policy engine passing the session details, the original requested operation and object (*CheckBTGAccess*):

- *CheckBTGAccess* returns GRANT as the BTGi state variable is already set to TRUE;

9. The application makes the requested operation to the resource;

10 & 11. The resource returns the results to the application service, which gives them to the user.

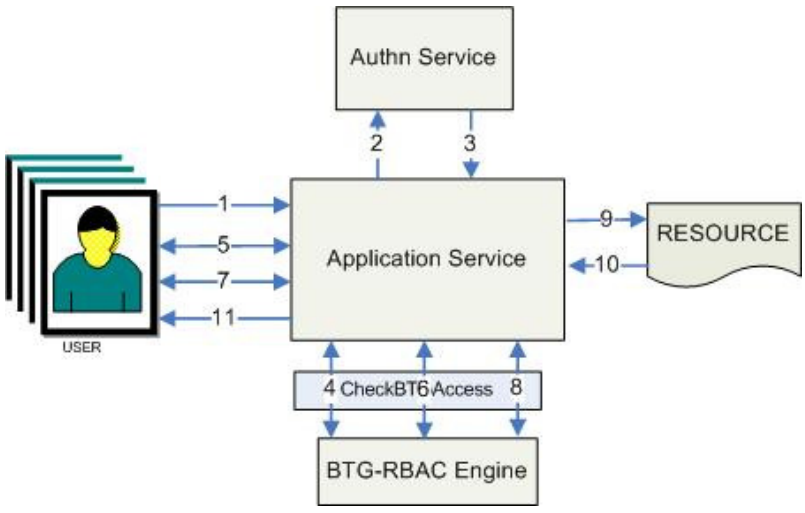

Figure 7.5 – The BTG-RBAC interaction diagram.

7.4 Discussion

This chapter presents the new BTG-RBAC model that easily integrates BTG features within the NIST/ANSI RBAC model in a secure, controlled and responsible way. The system is easy to use because the BTG-RBAC engine supplements the GRANT/DENY response with an additional "permission to BTG" response. This allows applications to converse easily with the user and to ask them if they would like to BTG. There are two alternative ways of specifying policy rules for BTG-RBAC policies, according to either the simple BTG-RBAC model or the complete BTG-RBAC model.

There is however one fact that must be stressed. This model requires that a responsible party audits the reasons why the BTG actions were performed within the system. If the justification that a subject states when breaking the glass is not justifiable enough, further justifications or disciplinary measures must be pursued by the responsible party. The responsible party might receive immediate or weekly notifications of the subjects that broke the glass and act accordingly. From the moment the subjects know that they are being audited and they know further actions will be taken, they are bound to lessen their unauthorized accesses to the required and justifiable ones only.

With this in mind, the BTG-RBAC is a secure and flexible model because it moulds emergency or unanticipated situations and allows the administrator/manager to add BTG policies in a controlled manner and the effects may be monitored closely through the provision of various obligations. The BTG-RBAC model allows subjects to act responsibly by giving them a choice whether to BTG or not, when they are initially denied access. The BTG-RBAC model can be implemented within any application and can shape a more flexible, dynamic and adaptable access control policy that will relate more closely with end users' needs, in complex settings.

8 THE BTG-RBAC: IMPLEMENTATION OF A PROTOTYPE

8.1 Introduction

The BTG-RBAC model was designed and developed as a theoretical concept during the research work presented in this thesis. This section describes the realization of this new access control model to demonstrate its feasibility and application within a specific domain. In order to achieve this goal the BTG-RBAC model was developed within the PERMIS (PrivilEge and Role Management Infrastructure Standards) authorisation platform [100], together with Apache, to protect an example website. A prototype was implemented so that the BTG-RBAC model could be tried and tested by real users simulating its use in real practice. This chapter describes this implementation.

8.2 Objectives

The main objectives of implementing a BTG-RBAC model prototype are to: build a proof of concept of the BTG-RBAC model; and test the feasibility of integrating the model within the PERMIS authorisation platform.

8.3 Methods

The software development method was to: design, implement and test a working prototype.
The PERMIS architecture was analyzed in order to decide where changes were needed so that the BTG-RBAC model could be integrated.
Generic development steps were defined at the beginning of the project and followed through.

The BTG-RBAC model requires a state based Policy Decision Point (PDP) but nearly all PDPs are currently stateless. Consequently, it was decided to put a state based wrapper around the PERMIS PDP and to define this wrapper in such a way that any stateless PDP could be used (Figure 8.1).

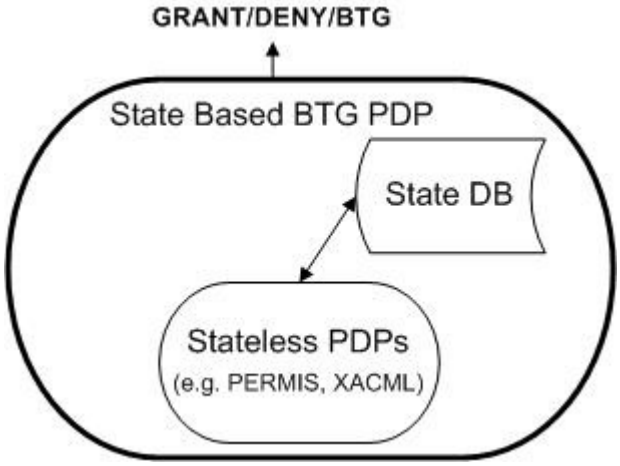

Figure 8.1 – BTG-RBAC PDP.

8.4 Design and implementation

The implementation of the BTG-RBAC model proof of concept with PERMIS had a duration of 3 months (between the 1st of September 2008 and the 30th of November 2008) and was funded by the Trusted Architecture for Securely Shared Services (TAS3) project [101]. The chosen scenario to implement the BTG-RBAC model proof of concept was the access to confidential student records within the University of Nottingham, one of the partners in the TAS3 project.
In summary, there are parts of the student records that are confidential, such as grades or other personal information that only professors are allowed to see. The lecturers that may need to access this confidential information will have to BTG on this information and therefore activate the BTG-RBAC model. All other roles are denied access to the confidential record. This scenario can be easily transposed to a healthcare scenario where a medical doctor can access genetic information while a nurse cannot, but in an emergency situation he/she can BTG to do it, justifying him/her action later on.

The steps that were defined to pursue the development of the BTG-RBAC model were to:

a. Install all the necessary components to get PERMIS up and running;
b. Create a simple static web site with two pages, one that is visible to a role lecturer, and the other that is visible to a role professor. The PERMIS policy should protect both pages;
c. Make the service publicly available on a testbed machine so that people can test it;
d. Add a MySQL database with different tables and dynamic web pages built from these tables using scripting and a PERMIS policy to protect the scripts. The role lecturer should be able to read student files but not student confidential files (only a professor can read those);

e. Add a BTG button (page) that is displayed to lecturers when an access is rejected (access to confidential file). Control over who is entitled to BTG will be in the PERMIS policy. Allow lecturers to BTG but not other roles. After BTG has been successfully selected, the confidential page should be displayed. When BTG is successful, the BTG state variable (Boolean) has to be set to TRUE and be stored somewhere for safe keeping (could be the MySQL database). The Boolean has to be passed to PERMIS in each decision request;
f. Add the obligation policy to the BTG operation. The obligation should be to send an email message to the role manager saying that the role lecturer has "broken the glass". Write the code that executes the returned obligation and sends off the email.

Figure 8.2 describes the architecture of the Apache PERMIS Shibboleth Apache Authorisation Module (SAAM) [102]. The PERMIS SAAM is a flexible RBAC authorisation module that integrates Shibboleth and Apache and is based on the PERMIS privilege management infrastructure. In the case of Apache PERMIS SAAM the authentication service is performed by *mod_auth_ldap* which is an Apache module located in the same target computer system as the PERMIS SAAM. The LDAP repository (used to store user credentials and other attributes) does not have to necessarily sit in the same computer as the Apache module or the PERMIS SAAM.

The interactions between SAAM, the authentication module (*mod_auth_ldap*) and the Apache server are as follows (Figure 8.2):

1. When a user contacts an Apache web server requesting access to a URL which is protected by *mod_auth_ldap* and *mod_permis*, the user is prompted by *mod_auth_ldap* to enter username and password in order to be authenticated;
2. *Mod_auth_ldap* authenticates the user by searching in the authentication LDAP server and locating the correct entry, which matches the username and password, retrieves and puts the user's DN (Distinguished Name) in the Apache HTTP header;
3. During the authorisation phase in the HTTP request handling process, *mod_permis* is invoked by the Apache server, and the user's DN is acquired by *mod_permis* through the HTTP header;
4. *Mod_permis* calls the Credential Validation Service (CVS) and passes the user's DN to it, the CVS retrieves the user's role attribute certificate from the configured LDAP server and validates it. The PDP then makes an authorisation decision based on the valid role attributes and this is returned back to *mod_permis*;
5. *Mod_permis* returns the decision result to the Apache server, and the user is granted or denied access to the target resource according to the decision result.

It can be seen that *mod_permis* is only capable of returning GRANT or DENY responses, and so the BTG-State handling has to be done in custom PHP code as described below.

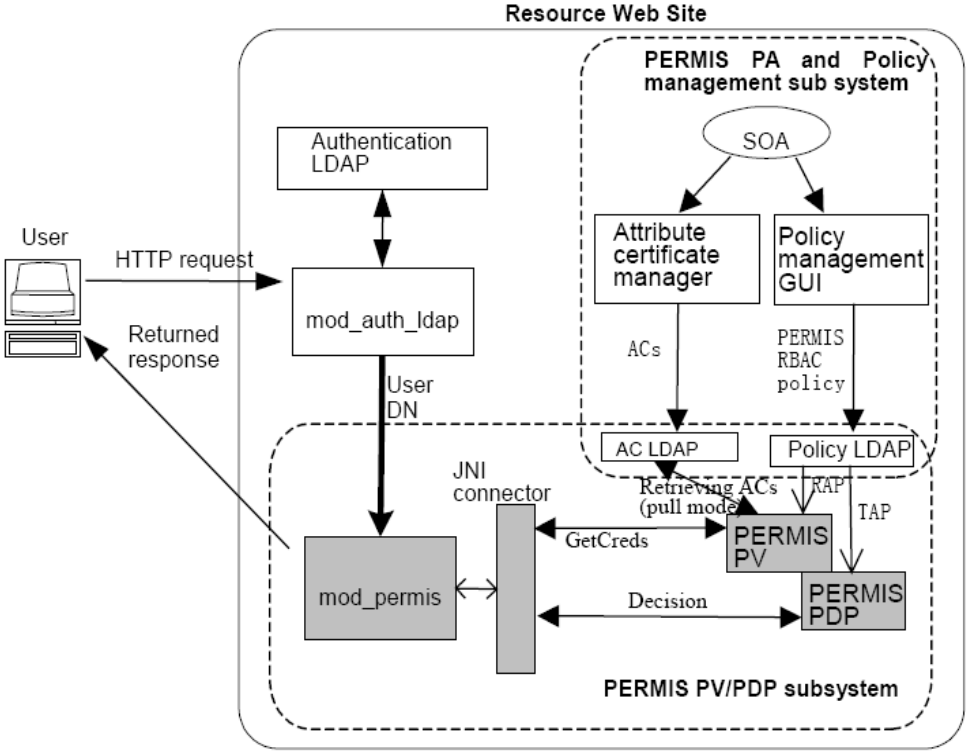

Figure 8.2 – Structure of Apache-PERMIS SAAM Integration [102].

The BTG-RBAC model was integrated within the PERMIS SAAM 4.0.0 authorisation infrastructure. Changes had to be made to the Apache configuration file and to the PERMIS access control XML policy. These changes are described below.

Table 8.1 describes the software that was used to implement the BTG-RBAC prototype while Figure 8.3 presents the web pages that integrated the same prototype.

Table 8.1– Software required to install Apache PERMIS SAAM 4.0.0.

Application	Version
Apache	2.0.63
OpenLdap	-
PHP	5.2.6
Mysql	-
Tomcat for Apache	5.5.27
Mod_auth_ldap	3.0
SAAM	4.0.0
Ubuntu Server Edition	8.0.4

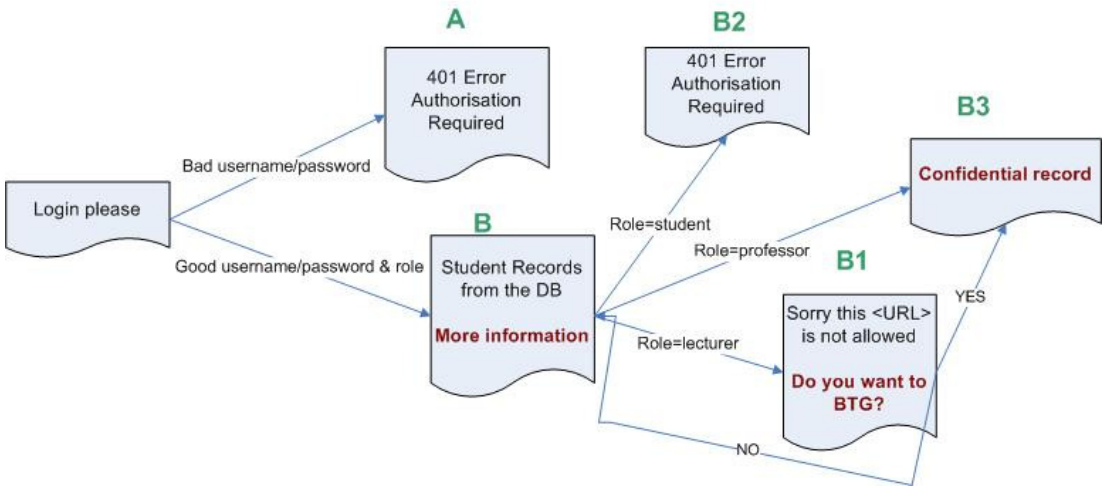

Figure 8.3 – Steps that represent the prototype interactions.

There is a need to make an extra authorisation decision request to the RBAC engine in order to check within the access control policy if the user that was denied access the first time can still perform BTG on that resource. If the RBAC engine returned DENY to the first question (can the user access the confidential resources?) as well as DENY to the second question (can the user perform BTG on the confidential resources?) then the BTG-RBAC engine would deny access to the user. If the RBAC engine returned DENY to the first question and returned GRANT to the second question then the BTG-RBAC engine would return BTG and the user is asked if he/she wants to BTG on the resource. This is done internally and transparently to the user who only sees the BTG page if he is allowed to perform BTG on the resource.
The access control policy to enforce this prototype is presented in Table 8.2.

Table 8.2 – Generic description of the access control policy to enforce.

User	Role	Student records (B)	BTG page (B1)	Confidential records (B3)
Ana	student	yes	no	no
Rui	lecturer	yes	yes	no (unless BTG)
David	professor	yes	N/a	yes

8.4.1 Experimental results and screenshots

The prototype has been available since December 2008; it has been shown to several parties within the ambit of the TAS3 European project presentations and can be tried at the following link: http://issrg-testbed-2.cs.kent.ac.uk/.
In more detail, the prototype performs the following steps:

I. The page in Figure 8.4 is publicly accessible. When the user selects the *Search Database* button the login screen in Figure 8.5 appears. The valid pair username/password together with a role defined in Table 8.2 will trigger the BTG-RBAC engine to check if the user can access the students' records page B shown in Figure 8.6. If granted, Figure 8.6 is displayed to the user showing the records with a *More Information* option.

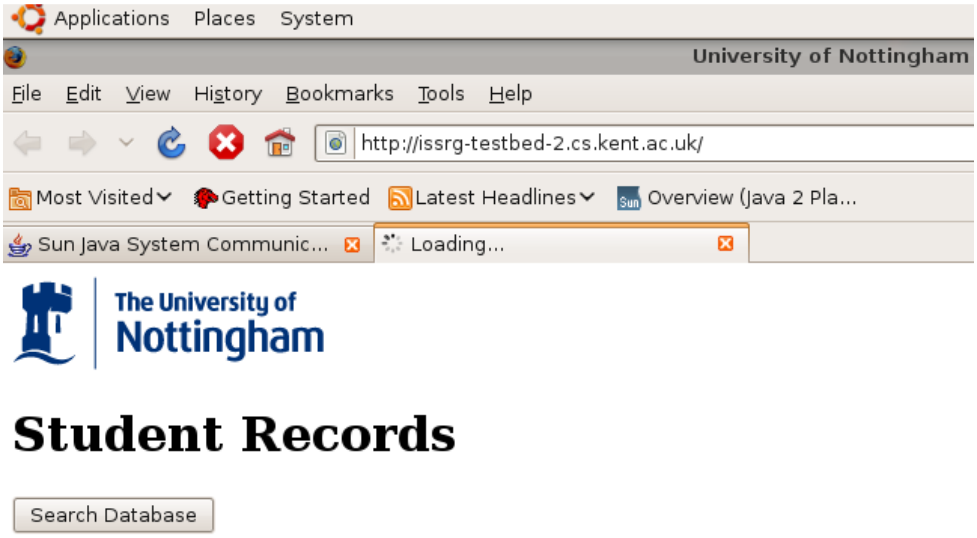

Figure 8.4 – The publicly accessible first page.

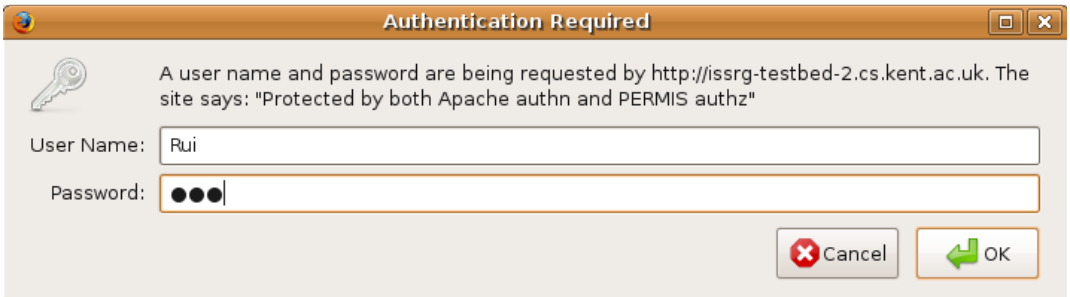

Figure 8.5 – Username/password screen.

II. If the user selects the *More Information* button then the BTG-RBAC engine checks if the user can access the student's confidential record (B3) and, if not, if the user can BTG on this <URL>. So one of three options is obtained: DENY, BTG or GRANT.

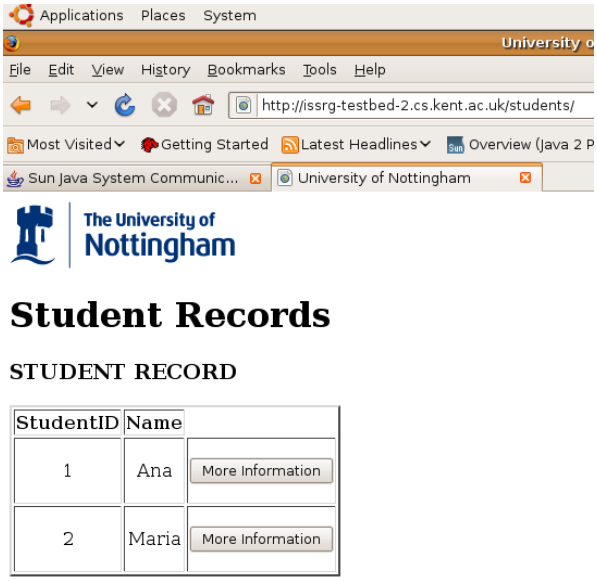

Figure 8.6 – The list of students' records **B**.

III. If GRANT is returned the confidential record B3 is displayed (Figure 8.7). This happens if David with role professor was the user to authenticate.

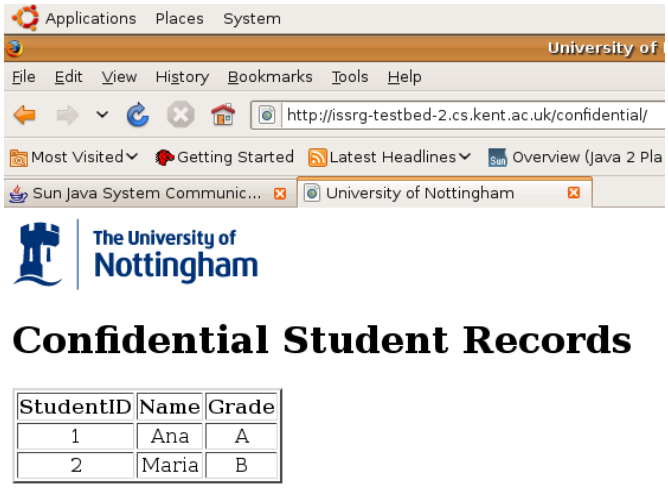

Figure 8.7 – The confidential record **B3**.

IV. If DENY is returned the *Not Authorised* Apache page is displayed - B2 (Figure 8.8). This happens if Ana with role student was the user to authenticate.

Figure 8.8 – Apache error page that is displayed when a user is not authorised to access the required web page.

V. If BTG is returned (this happens if the authenticated user was Rui with role lecturer), the BTG page B1 is displayed (Figure 8.9).

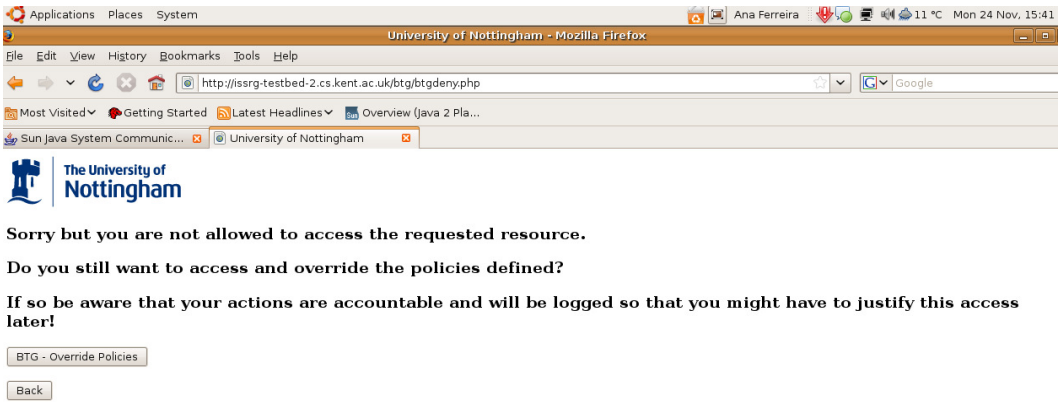

Figure 8.9 – The BTG page **B1**.

If the user carries out the BTG process by selecting the *BTG-Override Policies* button, the BTG-RBAC engine is asked if the user can BTG on that resource. If the answer is GRANT, a set of obligations is returned and the confidential record page is displayed (Figure 8.7). The obligations are: setting the BTG state variable to TRUE and sending an email to the responsible party alerting that a BTG action was performed by that user.

8.4.2 Platform to reset the BTG state variable

Two tables were created and stored in the database to hold information about users and student records. The users' table held information about the user identification, role, resources he/she can access and the BTG Boolean variable for each of these resources.

In order to reset the BTG Boolean variable state a management interface was created (Figure 8.10). This interface allows an authorised user to reset manually the BTG variables to FALSE within the database tables for a specific user that performed BTG.

Figure 8.10 – Management platform to manually reset the BTG variables to FALSE after BTG is performed.

However, in practice, this was found to be too tedious and so the public prototype was set to automatically reset the BTG variable to FALSE a few seconds after it was set to TRUE.

8.4.3 PERMIS XML access control policy

The PERMIS XML access control policy used for the access control policy described in Table 8.2, and used in this prototype, is presented below. To be consistent, the TargetDomains defined within the policy are referred as B, B1 and B3, to conform with the diagram presented in Figure 8.3.

Once the BTG state parameter "urn:uk:ac:kent:cs:issrg:attribute:btg" is returned from the state database, if the parameter is TRUE and the "permisRole=lecturer" then the target set within the policy is available for that user (B3). If the parameter is set to FALSE then, if the role of the user can BTG, the shown target will be B1. If the user chooses to BTG by clicking the *More information* button, the BTG parameter within the state database will be altered to TRUE (with the obligations) and he/she can then access the B3 (which corresponds to the confidential pages). The email obligations that are also returned will be performed together with the resources display (i.e., email obligation methods described below). In Table 8.3 the parts highlighted within the policy are the changes that were included for the BTG features to work.

Table 8.3 – XML Access control policy used for the BTG-RBAC model implementation with Apache PERMIS.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE X.509_PMI_RBAC_Policy>
<X.509_PMI_RBAC_Policy OID="1.2.826.0.1.3344810.6.0.0.11">

 <SubjectPolicy>
  <SubjectDomainSpec ID="SubjectDomain0">
   <Include LDAPDN="dc=kent,dc=ac,dc=uk"/>
  </SubjectDomainSpec>
 </SubjectPolicy>

  <RoleHierarchyPolicy>
  <RoleSpec OID="1.2.826.0.1.3344810.1.1.14" Type="permisRole">
   <SupRole Value="student" />
   <SupRole Value="lecturer" />
     <SubRole Value="student"/>
   </SupRole>
  <SupRole Value="professor" />
     <SubRole Value="lecturer"/>
  </SupRole>
  </RoleSpec>
  </RoleHierarchyPolicy>

 <SOAPolicy>
  <SOASpec ID="SOA0" LDAPDN="CN=A Permis Test User,dc=kent,dc=ac,dc=uk"/>
 </SOAPolicy>

 <RoleAssignmentPolicy>
  <RoleAssignment>
   <SubjectDomain ID="SubjectDomain0"/>
   <RoleList>
    <Role Type="permisRole" Value="student"/>
    <Role Type="permisRole" Value="lecturer"/>
    <Role Type="permisRole" Value="professor"/>
   </RoleList>
  <Delegate Depth="0"/>
   <SOA ID="SOA0"/>
   <Validity/>
  </RoleAssignment>
 </RoleAssignmentPolicy>

 <TargetPolicy>
  <TargetDomainSpec ID="B">
   <Include URL="http://*:0-65535/students"/>
   <Include URL="https://*:0-65535/students"/>
  </TargetDomainSpec>
  <TargetDomainSpec ID="B1">
   <Include URL="http://*:0-65535/btg"/>
   <Include URL="https://*:0-65535/btg"/>
  </TargetDomainSpec>
  <TargetDomainSpec ID="B3">
   <Include URL="http://*:0-65535/confidential"/>
   <Include URL="https://*:0-65535/confidential"/>
  </TargetDomainSpec>
  </TargetPolicy>

 <ActionPolicy>
  <Action ID="GET" Name="GET"/>
  <Action ID="POST" Name="POST"/>
  <Action ID="BTG" Name="BTG"/>
 </ActionPolicy>

<TargetAccessPolicy>
  <TargetAccess>
   <RoleList>
    <Role Type="permisRole" Value="student"/>
   </RoleList>
   <TargetList>
    <Target>
     <TargetDomain ID="B"/>
     <AllowedAction ID=”GET”/>
```

```
            </Target>
          </TargetList>
        </TargetAccess>

      <TargetAccess>
        <RoleList>
          <Role Type="permisRole" Value="lecturer"/>
        </RoleList>
        <TargetList>
          <Target>
            <TargetDomain ID="B1"/>
             <AllowedAction ID=”BTG”/>
          </Target>
        </TargetList>
      </TargetAccess>

        <Obligations>
          <Obligation FulfillOn="Permit" ObligationID=" urn:uk:ac:kent:cs:issrg:btg">
            <AttributeAssignment AttributeId=" urn:uk:ac:kent:cs:issrg:attribute:btg "
    DataType="http://www.w3.org/2001/XMLSchema#boolean">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean">true</AttributeValue>
            </AttributeAssignment>
          </Obligation>
      <Obligation FulfillOn="Permit" ObligationID="urn:oasis:names:tc:xacml:email">
            <AttributeAssignment AttributeId=" urn:uk:ac:kent:cs:issrg:attribute:mailto"
             DataType="http://www.w3.org/2001/XMLSchema#string">
           <AttributeValue
             DataType="http://www.w3.org/2001/XMLSchema#string">af84@kent.ac.uk</AttributeValue>
           </AttributeAssignment>
          <AttributeAssignment AttributeId=" urn:uk:ac:kent:cs:issrg:attribute:subject"
             DataType="http://www.w3.org/2001/XMLSchema#string">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">BTG</AttributeValue>
          </AttributeAssignment>
          <AttributeAssignment AttributeId=" urn:uk:ac:kent:cs:issrg:attribute:text"
             DataType="http://www.w3.org/2001/XMLSchema#string">
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">The Glass Has been broken
            in Nottingham</AttributeValue>
           </AttributeAssignment>
        </Obligation>
        </Obligations>
      </TargetAccess>

    <TargetAccess>
        <RoleList>
          <Role Type="permisRole" Value="lecturer"/>
        </RoleList>
        <TargetList>
          <Target>
            <TargetDomain ID="B3"/>
             <AllowedAction ID=”GET”/>
          </Target>
        </TargetList>

        <IF>
           <EQ>
             <Environment Parameter=" urn:uk:ac:kent:cs:issrg:attribute:btg" Type="Boolean"/>
             <Constant Type="Boolean" Value="true"/>
           </EQ>
        </IF>

      <TargetAccess>
        <RoleList>
          <Role Type="permisRole" Value="professor"/>
        </RoleList>
        <TargetList>
          <Target>
          <TargetDomain ID="B3"/>
         <AllowedAction ID=”GET”/>
          </Target>
        </TargetList>
      </TargetAccess>
     </TargetAccessPolicy>
</X.509_PMI_RBAC_Policy>
```

8.4.4 Changes in apache (httpd)

The changes performed in the Apache configuration file *httpd.conf* were the following.

For the web page **B** shown in Figure 8.6:

```
<Location /students>
 Options Indexes FollowSymLinks
 AllowOverride None
 order allow,deny
 allow from all
 PermisAuthorization
 PermisPullMode
 AuthName "Protected by both Apache authn and PERMIS authz"
 AuthType Basic
 LDAP_Server xxx.xxx.xxx.xxx
 LDAP_Port 389
 Base_DN "dc=xxx,dc=xxx,dc=xxx"
 UID_Attr uid
 require valid-user
</Location>
```

For the web page **B1** shown in Figure 8.9:

```
<Location /btg>
 Options Indexes FollowSymLinks
 AllowOverride None
 order allow,deny
 allow from all
 PermisAuthorization
 PermisPullMode
 AuthName "Protected by both Apache authn and PERMIS authz"
 AuthType Basic
 LDAP_Server xxx.xxx.xxx.xxx
 LDAP_Port 389
 Base_DN "dc=xxx,dc=xxx,dc=xxx"
 UID_Attr uid
 require valid-user
 </Location>
```

For the web page **B3** shown in Figure 8.7:

```
<Location /confidential>
 Options Indexes FollowSymLinks
 AllowOverride None
 order allow,deny
 allow from all
 PermisAuthorization
 PermisPullMode
 AuthName "Protected by both Apache authn and PERMIS authz"
 AuthType Basic
LDAP_Server xxx.xxx.xxx.xxx
 LDAP_Port 389
 Base_DN "dc=xxx,dc=xxx,dc=xxx"
UID_Attr uid
 require valid-user
</Location>
```

The code to connect to PERMIS was implemented using Java Server Pages (JSP) technology so that it could work with both Java and Apache but on the server side. In order to use JSP, Apache Tomcat was installed. Tomcat is an open source software of JSP technology [103]. The module *mod_jk* needed to be installed. This module is a plug-in that handles the communication between Tomcat and Apache. The configurations needed to work with Apache were (*httpd.conf*):

```
#Configure mod_jk
LoadModule jk_module modules/mod_jk.so
JkWorkersFile /usr/local/apache/conf/workers.properties
JkLogFile /usr/local/apache/logs/mod_jk.log
JkLogLevel info
JkMount /permis_web/* ajp13
```

In the file server.xml at the server side, these lines were included:

```
<!-- Define an AJP 1.3 Connector on port 8009 -->
  <Connector port="8009" enableLookups="false" redirectPort="8443" protocol="AJP/1.3" />
```

8.4.5 Main class BTGTestbed.jsp

The main class BTGTestbed.jsp is comprised of the following methods:

- *getCoordinationAttributes:* gets user attributes from the database;
- *updateCoordinationAttributes:* checks if the user is authorized to access the requested resource (webpage); updates BTG state variable in the database; and shows the user the result from the authorization procedure (either GRANT, DENY or BTG).

The code of these methods is presented in more detail in Appendix E – Part I.

8.4.6 Email obligation methods (JSP)

In order for the JSP to work there is the need for already built jar files to be set into its library directory. The location is: /WEB-INF/lib. The needed files were:
activation.jar; email-obligation.jar; iaik_jce.jar; issrg.jar; ldap.jar; log4j-1.2.13.jar; mail.jar; mysql-connector-java-5.1.6-bin.jar; opensaml-2.0-alpha1-jdk-1.5.jar; velocity-dep-1.5.jar; xalan-2.7.1.jar; xalan-2.7.1-serializer.jar; xerces-2.9.1-xercesImpl.jar; xerces-2.9.1-xml-apis.jar; xmlsec-1.4.1-commons-logging.jar; xmlsec-1.4.1.jar; xmltooling-1.0-alpha1-jdk-1.5.jar.

The email obligation is implemented by *EmailObligation.java* which parses the whole list of obligations and selects the email obligations to prepare and send them accordingly. *EmailObligation.java* comprises the following methods:

- *start*: prepares the obligation;
- *commit*: performs the obligation by calling *postMail* method;
- *rollback*: deletes the id of an obligation so that it will no longer be available next time round;
- *getEmailObligations*: parses each obligation from a list of obligations;
- *postMail*: sends an email message; this method can send an email message with or without authentication needed.

The code of these methods is presented in more detail in Appendix E – Part II.

EmailObject.java parses the XML code for the email obligation and constructs the corresponding email message to send. It comprises the following methods:

- *getFrom – getTo – getSubject - getBody*: returns each of the email fields (From, To, Subject and Body);
- *EmailObject*: returns the email address that was parsed from the obligation;
- *getAttributeValue*: returns each attribute for an obligation node (from the text that is included in the policy for an obligation).

The code of these methods is presented in more detail in Appendix E – Part III.

8.5 Discussion

This chapter showed that the implementation of the BTG-RBAC model requires only a few changes within an authorisation platform such as PERMIS. The proof of concept was successful because it was possible to build a prototype that is flexible and generic enough to be implemented in any domain. The use of a stateless PDP showed that it is possible to implement BTG with both stateless and state based PDPs. This prototype has been shown in several security conferences in the ambit of the TAS3 project.

However, the model did require a lot of custom code to handle the BTG state variable using PHP scripts, therefore the implementation is not trivial for web site developers. The next step will be to incorporate the state handler within the PDP so that no custom application code is needed. Unfortunately there was no time to achieve this during this research work[4].

Despite the successful proof of concept, the actual use of this model in a real setting will still require a justification process to show that it works properly and that follow up actions are taken when BTG actions are performed. Human intervention is crucial for the BTG process to work fully as stressed in Chapter 9.

[4] This has since been done by research assistants funded by the TAS3 project.

9 THE BTG-RBAC: PILOT CASE STUDY AND EVALUATION

9.1 Introduction

There are many references in the literature about the need for BTG features within access control policies whether in healthcare or other domains. Several of these references were introduced in Chapter 7. Among them was one where the definition and need for the BTG concept within access controls was defined by HCPs themselves [35]. They foresaw the need for this type of feature and so, as this concept is included within the main results of this research, the next step is to implement and evaluate a pilot case study that can integrate BTG features in its access control policy.

This opportunity arrived when the HCPs realized that they were using an EMR system where they could access genetic information without any restriction. This did not conform to the Portuguese legislation about personal health genetic data - Law 12/2005 [104] - which says that only a specific group of previously defined HCPs must have access to genetic data. So it was decided that BTG access control rules should be integrated with the EMR to enforce this legislation.

The EMR system (the VEPR) that was chosen to implement the BTG concept has been in use at the Hospital S. João (HSJ) since 2004 [9] [105]. Here, the HCPs had already defined the BTG feature they needed within the access control policy by the time the system was being designed [35] but it was not implemented at that time. This BTG feature was part of the policy generically but it was not defined at the time how or for what information this should be applied.

The core of the VEPR is composed of three modules (VIZ, MAID and CRep), which are presented in Figure 9.1. MAID collects clinical reports from various hospital departments (e.g., Dep A and Dep B), and stores them on a central repository (CRep) consisting of a database holding references to all the integrated clinical hospital data. After searching the database, users can access the integrated data of a particular patient through a web-based interface (VIZ). When selecting a specific report, its content is downloaded from the central repository file system to the browser.

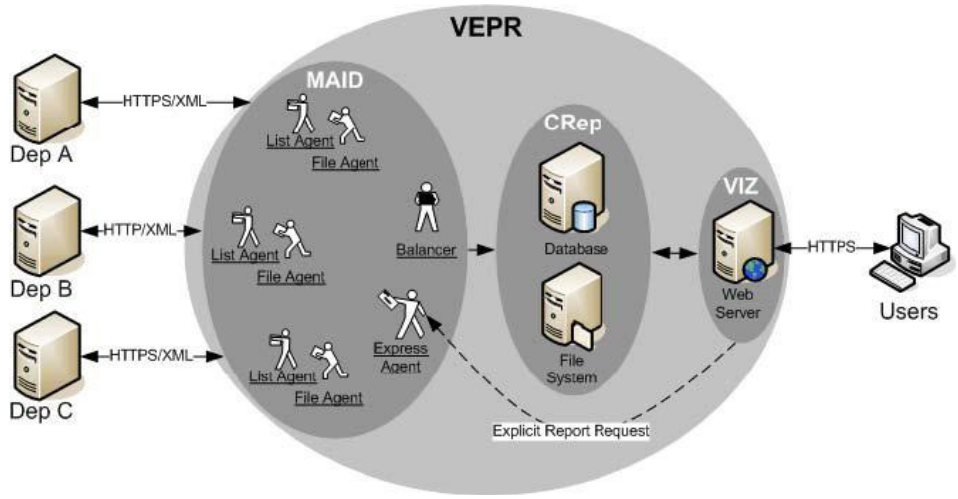

Figure 9.1 – General architecture of the EMR system showing the Multi-Agent system for Integration of Data (MAID), the Viewing (VIZ) and the Central Repository (CRep) modules.

Together with the VEPR, an access control management platform - the webcare - was implemented (Figures 9.2 and 9.3). An authentication procedure is used where the user is uniquely identified and associated with his/her profile, which holds the role or groups to which he/she belongs. These roles have privileges and permissions attached to them. To associate this profile to a user, an infrastructure to model the relationships between all the identities was created as part of the original VEPR.

This infrastructure integrated the RBAC model and included entities such as users, roles (which can include subroles), resources, access levels, actions, projects, the entity that includes the privileges and connects all of them (return_profile), and also the entity that does the same for the exception rules (return_exceptions).

This model implements all the necessary structures as well as the exceptions needed to generate the profile for a specific user at the time he/she authenticates to the system. To retrieve all this information there is a centralized feature, a database procedure, to search the whole infrastructure and collect all the privileges associated to the user.

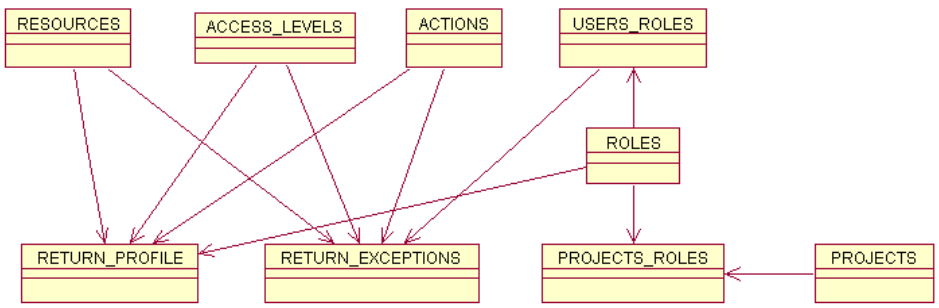

Figure 9.2 – Entity-relation model for the access control platform.

All accesses are registered in a specific database structure, separate from the one presented in Figure 9.2. The user, date and time as well as the errors that may occur during this session are recorded in this database. This is easy to do because the procedure itself can generate exceptions and insert error information according to the failed action. Figure 9.3 presents the platform used to associate access control privileges to the users of the VEPR.

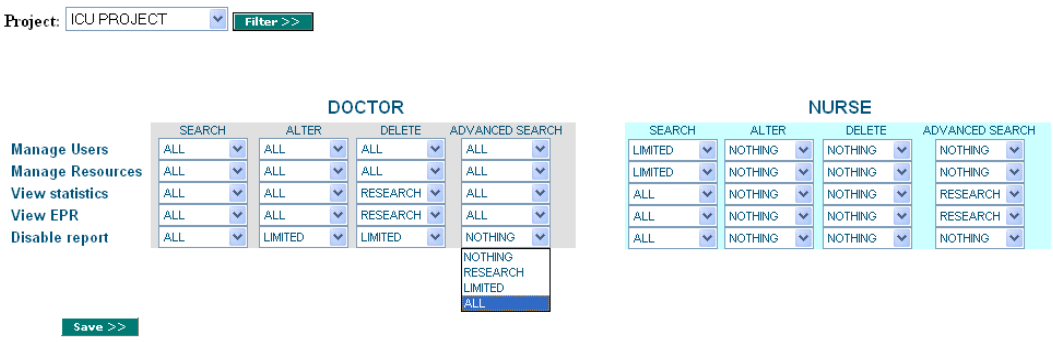

Figure 9.3 – Access control management platform.

As this platform does not handle BTG accesses some changes needed to be made to it.

The aim of this chapter is to describe the implementation of BTG within the VEPR described above and evaluate the impact that the BTG access control features have in the use and protection of genetic data.

9.2 Objectives

The users of the VEPR are currently medical doctors.

The objectives of implementing and evaluating a case study pilot of BTG access control rules within a real healthcare setting are: to enforce a National healthcare legislation; to test the implementation of the BTG access control rules within a real healthcare practice; to verify the impact on the security of genetic data (mainly its confidentiality) of the BTG pilot; to analyse the users' actions as they use this kind of system; and to evaluate the research process that was carried out from legislation to practice.

9.3 Methods

The methods used to design and implement the pilot for the BTG concept within a real setting are described in Figure 9.4.

A document with the Portuguese healthcare legislation was analyzed by three different parties - the researcher, a clinical department from a Portuguese hospital (the second biggest hospital in Portugal with more than 1300 beds, the HSJ) and the Ethics Commission from that same hospital.

The researcher followed the research process used within this thesis (Figure 1.1) and extracted a list of access control rules from the legal document (Figure 9.4). Further, the researcher selected the access control rules related to BTG that were generated from the mixed methods appliance (Chapters 5 & 6). The other two parties involved focused on enforcing the legislation as soon as possible within their healthcare institution. Once these two parties had the generic specification and processes defined to enforce the legislation, all the three parties got together several times in order to define the implementation strategy within the healthcare practice.

Within these meetings several procedures were defined for approval by the HSJ clinical board. When a consensus was reached regarding such procedures some more technical aspects concerning the actual implementation were defined and further approved. Once all these documents were finished the implementation process started.

The access control model for the VEPR was altered to include the new group of users, the CCADIG (HCPs authorized to access genetic information) group, and the coding was also altered accordingly to detect when a user tried to access a patient report containing genetic information. After the implementation of the BTG features described in this chapter, the user logs were analysed to see if the BTG system was working as expected and if the legislation was being enforced in a controlled and responsible manner. Furthermore, in order to evaluate the impact the BTG system had on the protection of confidentiality of patient genetic information, the access logs were analysed before and after the BTG feature got into production.

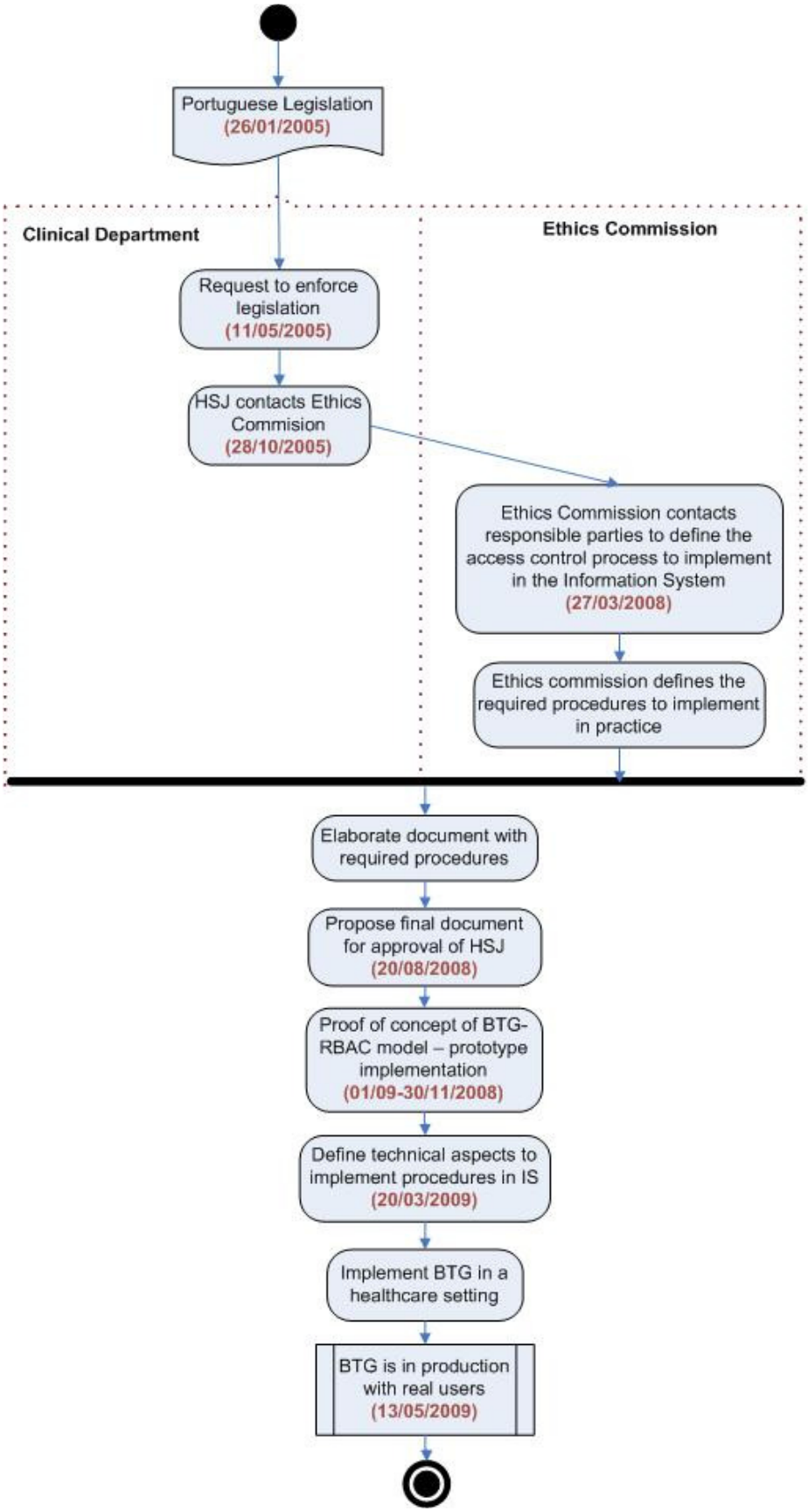

Figure 9.4 – Activity diagram describing the methods used during the research performed in this chapter.

9.4 Results

This section presents the results obtained for each step of the applied methodology.

The Portuguese legislation that was analysed was the Law 12/2005, whose main objective is: to enforce that genetic information must be the object of reinforced protection measures in terms of access, security and confidentiality (Article 6, nº 6).

9.4.1 Researcher

The results achieved by the methodology followed by the researcher are as follows.

9.4.1.1 Access control rules from the legislation

- The access to genetic information must be managed and accessed only by medical doctors from the genetic specialty (article 7, nº3 and article 9, nº 2)
- The number of HCPs that are authorized to access this information must be restricted in order to guarantee security as well as prevent losses, modification or destruction (article 19, nº 8 - DNA data and other biological products)

These two rules are in accordance and contained within access control rules 29 and 32 that were defined for privileged HCPs (Section 6.3.2).

9.4.1.2 Access control rules from the mixed methods

The access control rules that were generated from the mixed methods application that refer to the BTG concept are rules 30 and 31 (Section 6.3.2).

Rule 30:

Allow **[privileged healthcare professional]** to perform **[Break The Glass]**
on **[privileged care data]** for **[emergency care]**
provided **[time/location are set]**
Carry out **[record in audit trail]**

Rule 31:

Allow **[privileged healthcare professional]** to perform **[read & write]**
on **[privileged care data]** for **[emergency care]**
provided **[the Glass is broken]**
Carry out **[record in audit trail]**

Rules 30 and 31 can be modelled by the BTG-RBAC model, as explained in Chapter 7, while the other two rules (29 & 32) can be modelled by a generic RBAC model, and therefore, the BTG-RBAC model as well.

9.4.2 Clinical department and Ethics' Commission

The two main documents that started the process of enforcing the Law 12/2005 were the official request to enforce the legislation by the clinical department to both the HSJ clinical board and Ethics' Commission as well as the answer to this request.

Table 9.1 presents the extracts from these documents that relate directly with access control to genetic information.

Table 9.1 – Extracts from the request and answer documents for clarification of the Law 12/2005.

Article	Request	Clarification
Article 3, nº3	Will it be necessary to alter access to genetic information that is available within the EMR systems to only authorized professionals? Will exceptions in emergency situations be provided?	Already defined in the data protection Law nº67/98.
Article 6, nº4	Genetic information cannot be included within the patient record, will this information be separated from the rest?	Needs to be put into practice with the creation of a genetic file similar to an evaluated file for clinical trials (article 15 from the data protection Law enforces this)

9.4.3 All parties involved

The parties that were involved in the definition of the final document with the objective to enforce explicitly the legislation concerning genetic information were representatives from the HSJ: the Clinical Board, the Ethics Commission, the service of Immunohemotherapy, the service of Medical Genetics, the department of Information Systems and the Biostatistics and Medical Informatics department from the Faculty of Medicine of Porto.

The parties met regularly between the 27th March 2008 and the 20th March 2009. In these meetings it was defined who amongst the HCPs was authorized, according to their daily tasks, to access genetic information.

This section presents a summary of the results from the final document that was approved by all the representatives of the departments that participated in its development. The regulations that were approved and included within this document were the following:

1. To elaborate a list comprising all the medical doctors who fulfil all clinical and legal requirements to have authorized access to genetic information. These doctors will comprise a group, the CCADIG group;

2. Only medical doctors belonging to the CCADIG group can request studies related with genetics and are responsible for this request;
3. The results from genetic studies have to be properly coded by the laboratory that performs them;
4. There will be no clear distinction to a user accessing patient reports between the reports that contain genetic information from those that do not;
5. The management of the users that belong to the CCADIG group is done by the Information Systems department of the HSJ;
6. The users belonging to the CCADIG group have authorization to access genetic patient reports freely;
7. To the users that do not belong to the CCADIG group and wish to access a report that contains genetic information defined within the specifications of the Law 12/2005:
   a. A warning message explaining that the report they tried to access contains genetic information and that the user is not authorized to access it will be given to the user;
   b. The user will have to provide a reason for accessing that report (either a pre-defined one or another) if he/she still wants to access the information;
   c. Once the reason is set then a button to proceed with the access will be available;
   d. If the report is accessed then all these actions will be logged and registered for further perusal and justification;
8. A weekly email, with a reading acknowledgement to be recorded within a database, will be sent to the clinical board with the list of non authorized accesses to this information;
9. This regulatory document will be made available to all HSJ HCPs, together with the Law 12/2005.

9.4.4 Implementation results

The necessary steps for a user to perform BTG within the presented VEPR are the following (Figure 9.5):

1. The HCP tries to access a patient report within the VEPR application and that report contains genetic information;
2. The webcare platform validates the HCPs' credentials;
3. The webcare platform checks within the database if the pair login/password is correct; (In the case where the authentication fails, a reject message is sent from the application to the user and the request terminates here; if the user is privileged and can access the required report directly then the process is done)
4. The webcare platform sends back the user profile that states if the user can BTG or not to the VEPR application;

5. If the user can BTG, the VEPR application asks the HCP if he/she wants to BTG on that report, warning about the consequences of doing so (Figure 9.6);
6. If the user chooses to BTG (giving a reason for it) he/she just needs to press the appropriate button on the shown interface (Figure 9.6);
7. The VEPR application makes the requested operation to get the requested report;
8. The report is given to the VEPR application;
9. The VEPR application shows the report to the HCP.

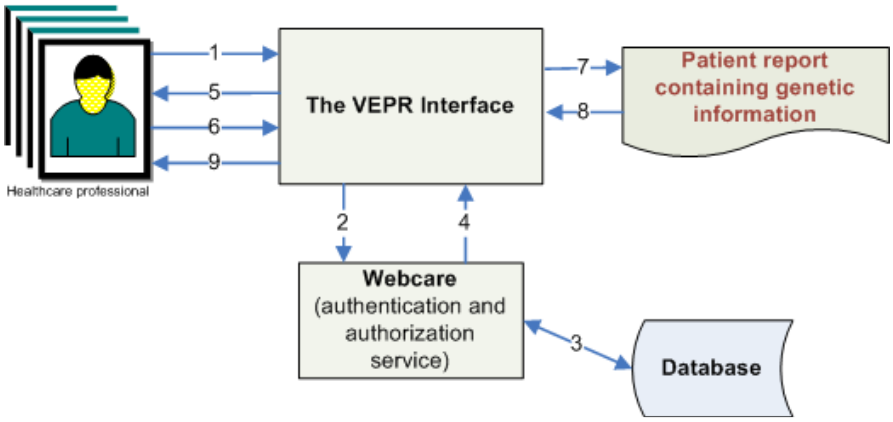

Figure 9.5 – BTG steps.

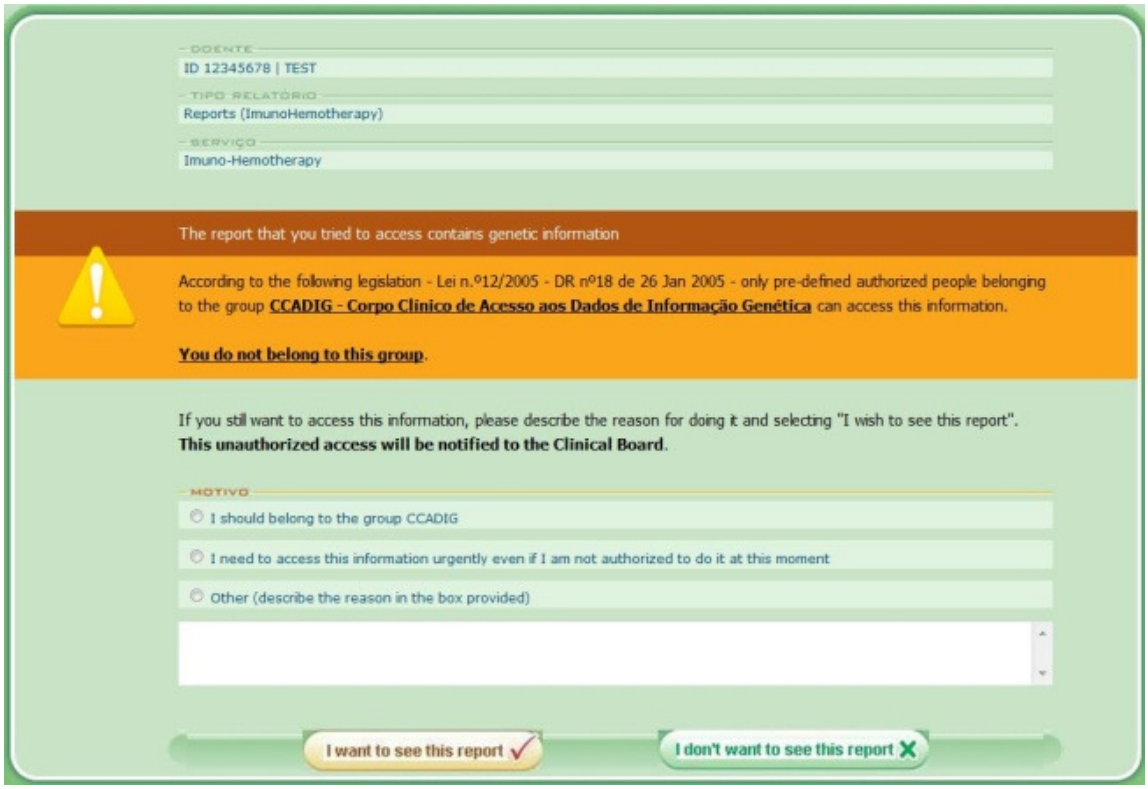

Figure 9.6 – BTG Interface.

Once the user chooses a report that contains genetic information, several actions are registered so that the user is accountable for this action afterwards. It is logged if the user just made a mistake, whether he/she carries on the BTG procedure or not, and if so, logging the reason he/she gives to BTG. Several procedures were altered within the webcare platform in order to integrate the BTG features. These included the creation of the following:

- a new group of users (11 medical doctors) that comprise the HCPs that are authorized to access patient reports that contain genetic information, according to the Ethics Commission official document;
- a new table within the database (BTG audit table) in order to register information about who is trying to access patient reports that contain genetic information.

This audit table contains the following information (Table 9.2):

Table 9.2 – Database table to audit user actions regarding BTG accesses.

Attribute name	Type	Description
Id	Integer	Unique identifier (primary key)
Timestamp	Date	Date & time the BTG popup warning occurred
Id_sessao	Integer	Session identifier
Id_relatorio	Integer	Report identifier the user tried to Access while BTG
Resposta	Integer	The final option chosen by the user (BTG or not)
Motivo_opc	Integer	The reason that was chosen for BTG
Motivo	String	Reason described by the user for BTG when the option “Other” is chosen

Besides this table, a new Boolean attribute, “genetics”, was created within another table that stores all the patient reports within the database. If the value for “genetics” is TRUE, the patient report contains genetic information otherwise the value is FALSE. This information is recorded automatically from the moment the patient report is collected and stored in the database.

At a coding level, a condition was introduced to check each user’s request, if the report contained genetic information or not, if the user belonged to the doctor’s role and if that user was a member of the group of medical doctors that is authorized to access this kind of report (the CCADIG group). Each time one of these reports is requested by a HCP, a new record is inserted within the BTG audit table with identifiers of the report and the HCP. All this is recorded whether the HCP chooses not to continue with the request or any BTG action the user makes. All this information is summarized and sent to the managerial role of those users by email, on a weekly basis. This makes sure that proper justification or any other disciplinary

action can be taken afterwards. It guarantees that BTG accesses are properly controlled and taken responsibility for.

The comparison period to analyze the BTG accesses in a real healthcare setting comprised 8 months of BTG use (between the 13th of May 2009 and 13th of January 2010) with the same period of time in the previous year, where no BTG features were available (between the 13th May 2008 and 13th of January 2009).

The patient reports started to be tagged with a genetic label (so that they could be identified) on the 27/11/2007, so the analysis was based on the total of genetic reports that were marked from this day onwards. The number of genetic reports that were marked on the period before the BTG features were available was 1909, while on the 13th of January 2010, this number had risen to 3979 (2070 more).

Table 9.3 – The percentage of accesses to reports containing genetic information.

Accesses to reports containing genetic information		
	Before BTG	**After BTG**
Total number of collected reports	**1909**	**3979**
% of accesses to genetic information	30%	29%
From within authorization group	5%	4%
Not within authorization group	25% (all successful)	25%:
	-	• 14% - successful
	-	• 11% - not successful

Table 9.4 shows the actions the users took once they were alerted they were not authorised to access the report they requested.

Table 9.4 – Comparison of BTG/NO BTG accesses to patient reports containing genetic information.

	BTG accesses	**NO BTG**
No of accesses	**562** (14%)	**448** (11%)
No of distinct users	135	182

Within the 448 that decided not to do BTG after trying to access a genetic report, 44 (10%) selected NO when asked if they wanted to BTG while 404 (90%) closed the browser without taking any further action. From the 562 users that selected to perform BTG, Table 9.5 describes the most common reasons the users gave to justify their accesses.

Table 9.5 – Most common reasons selected by the users to perform BTG (n=562).

Reasons to perform BTG	%	n
I have urgency in seeing the requested information although I'm not normally allowed to do it	41	232
Write own reason	33	184
I should belong to the group that can access genetic information	26	146

From the 184 users that wrote their own reason to perform BTG, Table 9.6 presents the most common mentioned reasons.

Table 9.6 – Most common reasons given by the users to perform BTG when they write their own reason (n=184).

Reasons written by the users	n
I'm the patient's assistant doctor	44
Study of the patient's problem and follow-up	43
I've requested this exam	30
Clarify studies in relation to pregnancy and infertility	26
I belong to the CCADIG group	19
Trombophilia studies	14
Autoimune disease consultation	4
Check for the IgG anti-D	3
I'm a member of the cerebral vascular diseases studies	1

9.5 Discussion

9.5.1 Interpretation of the results

The BTG concept was a relatively easy and fast process to implement in the VEPR because it was integrated within an EMR platform that was already in use in a healthcare practice that had been developed in a modular and flexible way. Although a long period was spent in defining the procedural regulations to be enforced when implementing the BTG concept only a short period was needed to implement them.

Now, in terms of the BTG accesses, the results of implementing and using the BTG feature in a real healthcare practice showed that there is a great decrease in the total percentage of accesses to genetic reports when the BTG feature was not available than when it is available

(30% → 18%), even when the number of genetic reports available is much higher than before. The same happens in the case of non authorized people accessing those reports (25% →14%). Furthermore, from the users who are not authorized to access genetic reports and try to do it, almost half of them decided not to go through with it. This means that the BTG features can filter these unauthorized accesses, which would not normally have been prevented. The expectation is that the tendency will be that only users who really need to access the reports, and have a valid reason, will go through with the process of BTG. The most common justification given by the users that perform BTG is that they have urgency to do it. This justification needs to be more detailed. Also, the justification process needs to complement the reasons given in an effective and coherent way.

9.5.2 Evaluation of the research process

The research process used during the course of this thesis was tested with the BTG case study and described in this chapter. This process is easy to use and apply and can in fact help in the definition and generation of access control rules from legislation to practice in any domain, not only in healthcare,.

The BTG-RBAC model can integrate a wide range of access control rules for the healthcare environment since any role can be given permission to BTG on any resource. The BTG-RBAC model is easy to integrate with other RBAC based authorisation platforms and this study shows that it can be even more secure and transparent to the end users than when it is not present.

Moreover, the impact of real use of the BTG concept is considerable and allows users to flexibly perform their tasks in a more controlled but transparent way. Nearly 50% of users decided not to access genetic data once the BTG feature was implemented.

However, the process of putting the legislation and regulations into practice should be quicker than was the case. The whole process described in Figure 9.4, from the healthcare legislation coming out to it being implemented and in production took 4 years and 4 months in total (Figure 9.7), with only a very low amount of this time being spent on design and implementation (2 months - tasks 6 & 7).
Figure 9.7 presents the main tasks for this case study implementation.

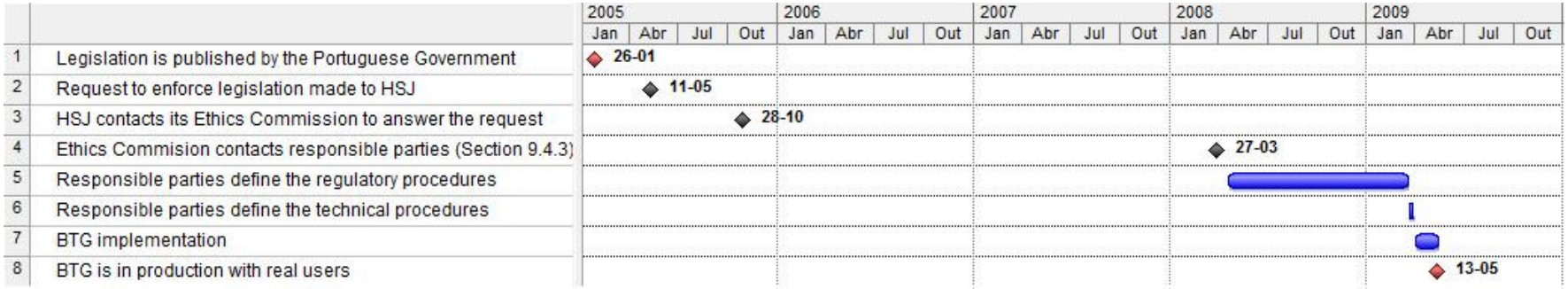

Figure 9.7 – Gantt diagram of the main tasks performed in the process from legislation to production.
Notice that the time elapsed[5] between tasks: 1 & 2 is 3 months and 2 weeks; 2 & 3 is 5 months and 2 weeks; and 3 & 4 is 2 years and 5 months.

[5] Time elapsed does not necessarily mean that it is a waiting time. It means that it cannot be further specified what processes were performed between the tasks during those times.

The process took most time between tasks 3 & 4 (2 years and 5 months), after the Ethics Commission is contacted to answer the request made to comply with the genetic legislation. It is not clear what was done between these two tasks, since only after 2 years and 5 months were the responsible parties (described in Section 9.4.3) contacted to participate in the process of defining legal and regulatory procedures (tasks 4 & 5). This process culminated with the definition of an official document approving the BTG implementation and the definition and implementation of the technical procedures (tasks 6 & 7). Tasks 4 to 7 took about 1 year and 2 months on the whole to be completed.

Tasks 2 & 3 are more procedural and should therefore be able to be accomplished in a swifter fashion. Although being probably the most hard to do, once it is understood what happened between tasks 3 & 4, this needs to be speeded up. It should be possible to hasten the whole process of translating legislation into regulations and procedures that can and should be implemented in an EMR. 4 years and 4 months to enforce legislation is a long time. The institutions and systems must be ready to do this in an easier and faster way. The whole process could have taken place in possibly half the time. Nevertheless, the results showed that enforcing a National healthcare legislation was, in this case, a successful process.

9.5.3 Limitations

The limitations of this study are that only a small amount of data is currently available as the system has only been in use in a real setting since May 2009.

Moreover, as the system was already in production at the time of this implementation, the definition of the IT procedures to be implemented had to take into account the software and technologies that were already in use in the system. So it was not an application independent pilot.

Also it should be considered that, at the moment, only medical doctors are using the VEPR system. Its use will need to be more scrutinised when other HCPs start to use it as well.

9.5.4 Future research

Future planned research to continue the improvement of this BTG system include: a thorough analysis of the justification process, to make sure accountability really works; and the enhancement of the system by the implementation of a more robust access control platform (e.g., PERMIS) instead of using a database to perform the authentication and authorization processes. Furthermore, there is the need to implement the BTG system into similar domains that require BTG features in order to conform to legislation or any other regulations and compare their results.

10 CONCLUSIONS

10.1 Research summary

At the beginning of this research it was identified, by means of a literature review, the main problems of EMR integration and use among HCPs regarding access control. These included educational and relational barriers that hinder EMR proper use and integration. These problems constituted the basis for the research questions to be explored and answered during the course of this thesis, having the following main objectives: to devise a more appropriate set of access control rules for which users were active participants and to define a new access control model that can model the aforementioned access control rules. To achieve this, the access control rules had to integrate both regulation/legislation (generic) and user needs (specific). These needs can be very complex to gather and integrate within an access control policy, but they are crucial nevertheless.

Research then proceeded to study the best way to achieve these objectives and how to select the best methodology to reach it. GT came up as an appropriate approach to gather end users' needs and became the main method to be applied. After the qualitative analysis, quantitative methods were necessary to complement or further explore specific issues in the data, and so this thesis used a mixed methods' approach in order to achieve this objective. Once this approach was defined and applied, it was possible to define access control rules to be integrated within an access control policy that included both generic and specific issues, in an objective and transparent way. As was expected, this access control policy was very heterogeneous and included some rules that had never been modelled before, such as the BTG rules.

The RBAC NIST standard model can easily integrate most of the access control rules that were generated (and it is commonly used in healthcare) but it could not, at this point, model BTG rules. So the next step was to develop a RBAC model that could integrate these new rules. The BTG-RBAC model was developed for this purpose. The new model included BTG as another response from a PDP (i.e GRANT, DENY or P^{BTG} – permission to perform BTG) and putting the user responsible for deciding if he would perform a BTG action. Some steps were also taken to test and evaluate the new model as well as the new BTG access control rules in a real setting.

10.2 Contributions

This section describes the contributions of this research work for each chapter of the thesis (Chapters 2 to 9).

Chapter 2 scientific contributions: (a) the application of systematic reviews (a method commonly used in medical research) to the information security research field, where this is rare; (b) the finding that access control is usually studied, modelled and theorized but is not implemented and tested in real settings, so that it is not properly adapted to real usage; (c) the finding that the definition and implementation of access control policies and models in healthcare is usually done without the insights from the most interested parties, the end users of the system; (d) the hypothesis that access control is a key component to improve EMR integration, usage and workflow; and (e) the finding that a vast majority of Portuguese patients are willing to access their medical records with a computer.
Part of this chapter was published in [32, 33, 38, 39] [106, 107].

Chapter 3 scientific contributions: (a) the selection and application of evaluation methods, such as GT and mixed methods that are usually used in social science research and medicine, in a research field where these kinds of methods and techniques are not commonly, if ever, used (i.e., access control systems in the healthcare environment); (b) the finding that currently used evaluation methods are not satisfactory in assessing access control needs but GT can be an approach that may help in this as well as improving the development of access control policies; and (c) a systematic approach to choose the mixed methods to apply in similar circumstances.
Part of this chapter was published in [106-109].

Chapter 4 scientific contributions: (a) the methods used to extract the access control rules from standards and legislation; and (b) the list of access control rules that were extracted from legislative and standards' documentation that can be used or adapted in the development of any access control model within the healthcare environment.

Chapter 5 scientific contributions: (a) the application of the chosen mixed methods in a systematic and transparent way within a subject (access control to EMR) where it has never been applied before; and (b) the results obtained from this appliance.
Part of this chapter was published in [84] [108].

Chapter 6 scientific contributions: (a) the methods to extract and define access control rules based on the results from mixed methods application to the end users of the healthcare domain (both HCP and patients) together with generic rules that resulted from legislation and standards' analysis; and (b) the list of RBAC rules for both HCP and patients, to be included within the new access control model. These rules can be applied generically in environments with similar requirements.
Part of this chapter was published in [108].

Chapter 7 scientific contribution: a formal definition and architecture of the new access control model – the BTG-RBAC model – in order to model the generated access control rules in the previous chapter, including the BTG access control rules.
Part of this chapter was published in [35] [110].

Chapter 8 scientific and technological contributions: the testing and evaluation of the BTG-RBAC model proof of concept.
The technological contribution of this chapter is: a prototype implementation that provides a proof of concept of the BTG-RBAC model that was implemented and tested using a free authentication and authorisation platform (Apache PERMIS - http://issrg-testbed-2.cs.kent.ac.uk)

Chapter 9 scientific and technological contributions: (a) the impact of implementing and evaluating the BTG concept in a real healthcare setting with the results from the experience of BTG usage, something that has never been referenced in the literature; and (b) the success of the application of the research process that has been developed during the whole research work (Figure 1.1) to translate access control from legislation into practice.
Part of this chapter was published in [35] [109-111].

10.3 Research limitations

There were some limitations during the course of this research that are worth mentioning. These relate to the fact that a wider GT and qualitative analysis could have been performed. During the first stage of research, observation and ethnographic studies could have been performed in order to bring this research even closer to end user experiences and needs.

Also, on the HCPs' side, the quantitative methods could have had a broader sample in that the structured questionnaires could have had a bigger and more varied selection of HCPs but this would have taken much longer than would have been possible for this research. HCPs have a very hectic life and it is very difficult to fit these kinds of studies in their timetables. This must be improved in future research.

On the patients' side, the application of GT and qualitative analysis could have been improved in order to include FGs with patients as participants. The integration of the results from the HCPs' FGs is not enough to describe the patients' needs and experiences in relation to access control to their medical records. The organization of FGs to patients was not possible to achieve due mainly to time constraints.

10.4 Recommendations and future work

According to the mentioned contributions, the main recommendations that researchers and developers should bear in mind when dealing with the study, development, implementation, evaluation and use of access control in healthcare are:

- to integrate both legislation and user needs in their research;
- to apply GT for access control (or information security) studies and development as this can be a more appropriate and complete methodology to apply;
- to use mixed methods as a mean to integrate wider and richer knowledge;
- to use FGs as a qualitative research approach in healthcare because they are less time consuming and generate more data in a short time span and so are more appropriate to this hectic environment;
- to always study the inclusion of BTG as an essential feature of any access control policy and model for healthcare systems' development and implementation;
- to reproduce the research process used in this work and compare the results obtained.

Although many issues within this work could be further studied and improved, the key factors that need further research and development are the following:

- testing and improving the access control rules that were generated within this research;
- further researching and evaluating the BTG usage in a real setting;
- implementing and testing a complete BTG-RBAC model in a real setting;
- perform patient FGs in similar research work;
- testing the research process that has been developed and used in this thesis in other domains and scenarios.

10.5 Conclusions

A new set of access control rules together with a new access control model – The BTG-RBAC model - have been developed. These integrate both the generic regulation needs as well as the specificities of the end users of the healthcare systems.

The BTG-RBAC model improved the existing access control models because it integrated the BTG feature that, as shown by this research, is essential in the healthcare domain. Furthermore, the generated access control rules together with the BTG-RBAC model can help reduce the time/costs, security and educational barriers that hinder the successful EMR integration within the healthcare practice. This was achieved with the collaboration of the end users into the access control definition. From this collaboration:

- *educational barriers* were reduced because if the users helped defining their interactions with the system, the complexity of the healthcare practice can be better translated into their daily workflows and needs and allow for a less problematic interaction with the EMR; it is therefore easier for the users to learn and understand how to use the system and will therefore need less education on these matters;

- *security and time/cost barriers* were reduced because unanticipated or emergency situations can be tackled in a controlled manner, reducing this way the healthcare professionals' downtime response to the situation at hand; unauthorized as well as non-recorded or non-justified accesses were also reduced due to the previous mentioned achievement; and finally, access controls closer to the user needs will be reflected in less time and costs wasted by the users to learn, use and alter the system.

The new BTG-RBAC model that integrates the access control rules generated during this research work, by reducing the described EMR integration barriers, can help to achieve a faster and safer patient treatment.

BIBLIOGRAPHY

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

[2] Gollman D. Computer Security. 1st ed.: John Wiley & Sons; 1999.

[3] Harris S. CISSP All-in-One Exam Guide. 2nd ed.: McGraw-Hill Osborne Media; 2003.

[4] International Standards Organisation. ISO 7498-2 - Information processing systems, Open Systems Interconnection, Basic Reference Model, Part 2: Security Architecture. ISO; 1989. p. 32.

[5] Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. 1st ed.: Wiley; 2001.

[6] Schneier B. Secrets and Lies: digital security in a networked world. 1st ed.: John Wiley &Sons; 2000.

[7] PriceWaterHouseCoopers. Information Security Breaches Survey. Technical report. Department of Trade and Industry; 2006.

[8] Waegemann C. EHR vs CPR vs EMR: whatever you call it, the vision is of superior care through uniform, accessible health records. Healthcare Informatics online. 2003.

[9] Cruz-Correia R, Vieira-Marques P, Costa P, Ferreira A, Oliveira-Palhares E, Araújo F, et al. Integration of Hospital data using Agent Technologies – a case study. AICommunications special issue of ECAI. 2005;18(3):191-200.

[10] Institute MR. 7th Annual survey of electronic health record trends and usage for 2005. Medical Records Institute; 2005.

[11] Bakker A. 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. 2004;73(3):267-70.

[12] Blobel B, Nordberg R, Davis JM, Pharow P. Modelling privilege management and access control. Int J Med Inform. 2006;75(8):597-623.

[13] International Organization for Standardization. ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management ISO; 2007.

[14] DoD National Computer Security Center. DoD 5200.28-STD. Department of Defense Trusted Computer Systems Evaluation Criteria. 1985.

[15] Thomas R, Sandhu R, editors. Towards a task-based paradigm for flexible and adaptable access control in distributed applications. New Security Paradigms Wrokshop; 1993. ACM.

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

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

[18] Hai-bo S, Fan H, editors. An attribute-based access control model for web services. 7th International Conference on Parallel and Distributed Computing, Applications and Technologies; 2006.

[19] Joshi J, Aref W, Ghafoor A, Spafford E. Security models for web-based applications: using traditional and emerging access control approaches to develop secure applications for the web. Communications of the ACM. 2001;44(2):38-44.

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

[21] Miller RH, Hillman JM, Given RS. Physician use of IT: results from the Deloitte Research Survey. J Healthc Inf Manag. 2004;18(1):72-80.

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

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

[24] Becker MY, Sewell P, editors. Cassandra: flexible trust management, applied to electronic health records; 2004.

[25] Lehoux P. The Problem of Health Technology: Policy Implications for Modern Health Care. 1st ed.: Routledge; 2006.

[26] Kling R. Computerization and social transformations. Science, Technology and Human Values. 1991;16(3):342-67.

[27] Lehoux P, Sicotte C, Denis J. Assessment of a computerized medical record system: disclosing scripts of use. Evaluation and Program Planning. 1999;22(4):439-53.

[28] Akrich M. Comment sortir de la dichotomie technique/société: Presentation des diverses sociologies de la technique. Latour B et Lemonnier P; 1994.

[29] Brown N, Webster A. New medical technologies and society: reordering life. Polity Press; 2004.

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

[31] Littlejohns P, Wyatt J, Garvican L. Evaluating computerised health information systems: hard lessons still to be learnt. BMJ. 2003;326:860-3.

[32] 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.

[33] Ferreira A, Chadwick DW, Antunes L, editors. Modelling access control for healthcare information systems: how to control access through policies, human processes and legislation. DCEIS - Proceedings of the 5th Doctoral Consortium; 2007.

[34] Andreas S, Jonathan M, Jeremy J, editors. The role-based access control system of a European bank: a case study and discussion. 6th ACM symposium on Access control models and technologies; 2001.

[35] Ferreira A, Cruz-Correia R, Antunes L, Farinha P, Oliveira-Palhares E, Chadwick DW, et al., editors. How to Break Access Control in a Controlled Manner. CBMS - Computer Based Medical Systems; 2006.

[36] Ross SE, Lin CT. The effects of promoting patient access to medical records: a review. J Am Med Inform Assoc. 2003;10(2):129-38.

[37] Mandl KD, Szolovits P, Kohane IS. Public standards and patients' control: how to keep electronic medical records accessible but private. BMJ. 2001;322(7281):283-7.

[38] Ferreira A, Cardoso A, Lima A, Pereira A, Silva A, Corte A, et al. Why facilitate patient access to medical records. Studies in Health Technology and Informatics. 2007;127:77-90.

[39] Ferreira A, Antunes L, Pinho C, Sá C, Mendes E, Santos E, et al., editors. Who should access electronic patient records. Proceedings of the International Conference on Health Informatics; 2008.

[40] Guerra A. Relatório de auditoria ao tratamento de informação de saúde nos hospitais Portugueses. Comissão Nacional de Protecção de Dados; 2004.

[41] Hackos J, Redish J. User and Task Analysis for Interface Design. 1st ed.: John Wiley & Sons; 1998.

[42] Brostoff S, Sasse MA, Chadwick D, Cunningham J, Mbanaso U, Otenko S. 'R-What?' Development of a Role-Based Access Control (RBAC) Policy-Writing Tool for e-Scientists. Software: Practice and Experience. 2005;35(9):835-56.

[43] Friedman C, Wyatt J. Evaluation Methods in Biomedical Informatics. 2nd ed.: Springer; 2005.

[44] Strauss A. Qualitative Analysis for Social Scientists. Cambridge University Press; 1987.

[45] Dey I. Grounded Theory. The SAGE handbook of Grounded Theory. Sage Publications Ltd; 2007.

[46] Marvasti A. Qualitative research in sociology: an introduction. London: Sage; 2004.

[47] Huston P, Rowan M. Qualitative Studies: their role in medical research. Canadian Family Physician. 1998;44:2453-8.

[48] Delamont S. Ethnography and participant observation. The Sage handbook of Grounded Theory. Sage; 2007.

[49] Bamberger M. Integrating qualitative and quantitative research in development projects. World Bank Publications; 2000.

[50] Borkan J. Mixed Methods Studies: a foundation for primary care research. annals of Family Medicine. 2004;2(1):4-6.

[51] Moffatt S, White M, Mackintosh J, Howel D. Using quantitative and qualitative data in health services research - what happens when mixed method findings conflict? BMC - Health Serv Res. 2006;6(28).

[52] Morgan DL. Practical Strategies for Combining Qualitative and Quantitative Methods: Applications to Health Research. Qualitative Health Research. 1998;8(3):362-76.

[53] Brewer J, Hunter A. The multimethod approach and its promise. Foundations of multimethod research. Sage Publications; 2005.

[54] Creswell J. Research Design: Qualitative, quantitative, and Mixed Methods Approaches. 3rd ed.: Sage Publications; 2008.

[55] Koppel R, Metlay J, Cohen A, Abaluck B, Localio A, Kimmel S, et al. Role of computerized physician order entry systems in facilitating medication errors. JAMA. 2005;293(10):1197-203.

[56] Lapelle N, Luckmann R, Simpson E, Martin E. Identifying strategies to improve access to credible and relevant information for public health professionals: a qualitative study. BMC Public Health. 2006;6.

[57] Porteous T, Bond C, Robertson R, Hannaford P, Reiter E. Electronic transfer of prescription-related information: comparing views of patients, general practitioners and pharmacists. British Journal of General Practice. 2003;53:204-9.

[58] Pyper C, Amery J, Watson M, Crook C. Patients' experiences when accessing their online electronic patient records in primary care. British Journal of General Practice. 2004;54:38-43.

[59] Robling M, Hood K, Houston H, Pill R, Fay J, Evans H. Public attitudes towards the use of primary care patient record data in medical research without consent: a qualitative study. Journal of Medical Ethics. 2004;30:104-9.

[60] Sciamanna C, Diaz J, Myne P. Patient attitudes toward using computers to improve health services delivery. BMC Health Services Research. 2002;2.

[61] Steele R, Secombe C, Brookes W, editors. Using wireless sensor networks for aged care: the patient's perspective. Pervasive Health Conference and Workshops; 2006.

[62] Winkelman W, Leonard K, Rossos P. Patient-perceived usefulness of online electronic medical records: employing grounded theory in the development of information and communication technologies for use by patients living with chronic illness. JAMIA. 2005;12(3):306-14.

[63] International Organization for Standardization. ISO/IEC 17799:2000 Information Technology - Code of Practice for Information Security Management. ISO; 2000.

[64] United Kingdom Government's Department of Trade and Industry. BS 7799. British Standards Institute; 1995.

[65] International Organization for Standardization. ISO 27799:2008 Health informatics - Information security management in health using ISO/IEC 27002. ISO; 2008.

[66] Union ECfSE. CEN/TC 251 - Health Informatics. Standardization in the field of Health Information and Communications Technology: CEN .

[67] ISO Technical Committee. ISO TC 215 Working Group 4, Health Informatics - Security. International Standards Organisation; 1998.

[68] CEN/TC 251. EN 12251 Health Informatics: Secure user identification for healthcare - management and security of authentication by passwords. CEN; 2004.

[69] CEN/TC 251. EN 13606 Health informatics - Electronic health record communication - Part 4: Security. CEN; 2007.

[70] International Organization for Standardization. ISO/IEC 10181-3:1996 - Information technology - Open Systems Interconnection - Security frameworks for open systems: Access control framework. ISO; 1996.

[71] International Organization for Standardization. ISO/TS 22600 - Health informatics -- Privilege management and access control ISO; 2006.

[72] Miller SoM. Health Insurance Portability and Accountability Act of 1996 (HIPAA). University of Miami; 2005; Available from: privacy.med.miami.edu/glossary/xd_hipaa.htm.

[73] Protection des Données Médicales, Comité des Ministres aux États Membres. (1997).

[74] On the impact of information technologies on health care – the patient and Internet Comité des Ministres aux États Membres. (2004).

[75] D'Alessandro D, Dosa N. Empowering Children and Families With Information Technology. Arch Pediatr Adolesc Med. 2001;155(10):1131-6.

[76] Ross-Lee B, Weiser M. Healthcare Regulation: past, present and future. Journal of the American Osteopathic Association. 1994;94(1):74-84.

[77] Anderson J. Social, ethical and legal barriers to e-health. Int J Med Inform. 2007;76(5-6):480-3.

[78] NHS Trust. Can I see my health records? Your quick and easy guide. In: Service CR, editor.: Communication Department; 2006.

[79] Fioriglio G, Szolovits P, editors. Copy Fees and patient's rights to obtain a copy of their medical records: from law to reality. AMIA Symposium; 2005.

[80] askSam eBooks & Databases. Health Insurance Portability and Accountability Act (HIPAA). Seaside Software Inc; 2008: http://www.asksam.com/ebooks/releases.asp?file=HIPAA.ask&b=TITLE%20I%2d%2dHEALTH%20CARE%20ACCESS%2c%20PORTABILITY%2c%20AND%20RENEWABILITY.

[81] Office for Civil Rights. The HIPAA privacy rule's right of access and health information technology. US Ddepartment of Health & Human Services; 2002 [updated 2002; cited 2009]; Available from: http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/eaccess.pdf.

[82] Ordem dos Médicos. Código Deontológico da Ordem dos Médicos: Diário da República; 2009. p. 1355-67.

[83] The International Medical Informatics Association. Code of ethics for health information professionals. IMIA; 2003 [updated 2003; cited 2010]; Available from: http://www.imia.org/pubdocs/Ethics_Eng.pdf.

[84] Ferreira A, Cruz-Correia R, Gomes R, Reis D, Santos H, Chadwick D, et al. Password Sharing and How to Reduce it. In: Chryssanthou A, editor. Certification and Security in Health-Related Web Applications : Concepts and Solutions: Medical Information Science Reference; 2010.

[85] Social Research Update. Sociology at Surrey. 1997 [updated 1997; cited 2008]; Available from: http://sru.soc.surrey.ac.uk/SRU19.html.

[86] Merton R, Kendall P. The Focused Interview. American Journal of Sociology. 1946;51:541-57.

[87] Powell RA, Single HM. Focus Groups. International Journal for Quality in Health Care. 1996;8(5):499-504.

[88] Folch-Lyon E, Trost J. Conducting Focus Groups Sessions. Studies in Family Planning. 1981;12(12): 443-9.

[89] Kontio J, Lehtola L, Bragge J, editors. Using the focus group method in software engineering: obtaining practitioner and user experiences. Proceedings of the International Symposium on Empirical Software Engineering; 2004.

[90] Charmaz K. Constructing Grounded Theory: A Practical Guide through Qualitative Analysis. 1st ed.: Sage Publications Ltd; 2006.

[91] International Q. NVIVO 7. 7 ed; 2006.

[92] Eaves Y. A synthesis technique for grounded theory data analysis. Journal of Advanced Nursing. 2001;35(5):654-63.

[93] Groves R, Biemer P, Lyberg L, Massey J, Nicholls II W, Waksberg J. Telephone Survey Methodology. Wiley-InterScience; 2001.

[94] Streiner D, Norman G. Health Measurement Scales: A practical guide to their development and use. 3rd ed.: Oxford University Press; 2003.

[95] Zhao G, Chadwick D, Otenko S., editors. Obligation for Role Based Access Control. International Symposium on Security in Networks and Distributed Systems (SSNDS07); 2007.

[96] Break Glass – Granting Emergency Access to Critical ePHI Systems – HIPAA Security. In: ACT PtpasohiHIPA, editor.; 2004.

[97] NEMA/COCIR/JIRA Security and Privacy Committee. Break-glass: An approach to granting emergency access to healthcare systems. 2004.

[98] NHS care records service – NHS Connecting for Health. 7869 2008 - A SCR Clinical User Guide. In: Health NCf, editor.; 2008.

[99] Information Technology – Role Based Access Control, ANSI/INCITS 359-2004. (2004).

[100] Chadwick D, Otenko A. The PERMIS X.509 Role Based Privilege Management Infrastructure. Future Generation Computer Systems. 2002;936:1-13.

[101] TAS3. Trusted Architecture for Securely Shared Services. European Funded Project; 2008.

[102] Wensheng Xu, David Chadwick, Otenko S, editors. Development of a Flexible PERMIS Authorisation Module for Shibboleth and Apache Server. 2nd EuroPKI Workshop; 2005.

[103] The Apache Software Foundation. Apache Tomcat. 1999 [updated 1999; cited 2010]; Available from: http://tomcat.apache.org/.

[104] Assembleia da República Portuguesa. Informação Genética Pessoal de Saúde. Diário da República I SÉRIE -A; 2005.

[105] Ferreira A, Cruz-Correia R, Costa-Pereira A, editors. Securing a Web-based EPR: An approach to secure a centralized EPR within a hospital. 6th International Conference on Enterprise Information Systems (ICEIS04); 2004.

[106] Ferreira A, Cruz-Correia R, Antunes L, Chadwick W D. Chapter III: Security of Electronic Medical Records. Handbook of Research on Distributed Medical Informatics and E-Health: Medical Information Science Reference: IGI Global; 2008.

[107] Ferreira A, Cruz-Correia R, Chadwick W D, Antunes L, editors. Improving the implementation of access control to electronic medical record. IEEE International Carnahan Conference on Security Technology; 2008.

[108] Ferreira A, Antunes L, Chadwick W D, Cruz-Correia R. Grounding Information Security in Healthcare. International Journal of Medical Informatics. 2010;79(4):268-83.

[109] Ferreira A, Cruz-Correia R, Chadwick W D, editors. Access Control in Healthcare: the methodology from legislation to practice. MEDINFO Congress; 2010. IOS Press; *(in press)*.

[110] Ferreira A, Chadwick W D, Zao G, Farinha P, Cruz-Correia R, Chilro R, et al., editors. How to securely break into RBAC: the BTG-RBAC model. 25th Annual Computer Security Applications Conference - ACSAC; 2009.

[111] Farinha P, Cruz-Correia R, Antunes L, Almeida F, Ferreira A, editors. From legislation to practice: a case study of break the glass in healthcare. Proceedings of the International Conference on Health Informatics - Healthinf; 2010. 114-120.

APPENDIX A

Council of Europe, Committee of Ministers, Recommendation No. R (97) 5 on the Protection of Medical Data 1997, (extract).

The Committee of Ministers, under the terms of Article 15.*b* of the Statute of the Council of Europe,
Considering that the aim of the Council of Europe is to achieve a greater unity between its members;
Recalling the general principles on data protection in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (European Treaty Series, No. 108) and in particular its Article 6 which stipulates that personal data concerning health may not be processed automatically unless domestic law provides appropriate safeguards;
Aware of the increasing use of automatic processing of medical data by information systems, not only for medical care, medical research, hospital management and public health but also outside the health-care sector;
Convinced of the importance of the quality, integrity and availability of medical data for the health of the data subject and his family;
Aware that progress in medical science is dependent to a great extent on the availability of medical data on individuals;
Convinced that it is desirable to regulate the collection and processing of medical data, to safeguard the confidentiality and security of personal data regarding health, and to ensure that they are used subject to the rights and fundamental freedoms of the individual, and in particular the right to privacy;
Aware that progress made in medical science and developments in information technology since 1981 have made it necessary to revise various provisions in Recommendation No. R (81) 1 on regulations for automated medical data banks,

Recommends that the governments of member states:

- take steps to ensure that the principles contained in the appendix to this recommendation are reflected in their law and practice;
- ensure wide circulation of the principles contained in the appendix to this recommendation among persons professionally involved in the collection and processing of medical data;

Decides that this recommendation will replace Recommendation No. R (81) 1 on regulations for automated medical data banks. Appendix to Recommendation No. R (97) 5

3. Respect for privacy

3.1. The respect of rights and fundamental freedoms, and in particular of the right to privacy, shall be guaranteed during the collection and processing of medical data.

3.2. Medical data may only be collected and processed if in accordance with appropriate safeguards which must be provided by domestic law.

In principle, medical data should be collected and processed only by health-care professionals, or by individuals or bodies working on behalf of health-care professionals. Individuals or bodies working on behalf of health-care professionals who collect and process medical data should be subject to the same rules of confidentiality incumbent on health-care professionals, or to comparable rules of confidentiality.

Controllers of files who are not health-care professionals should only collect and process medical data subject either to rules of confidentiality comparable to those incumbent upon a health-care professional or subject to equally effective safeguards provided for by domestic law.

4. Collection and processing of medical data

4.1. Medical data shall be collected and processed fairly and lawfully and only for specified purposes.

4.2. Medical data shall in principle be obtained from the data subject. They may only be obtained from other sources if in accordance with Principles 4, 6 and 7 of this recommendation and if this is necessary to achieve the purpose of the processing or if the data subject is not in a position to provide the data.

4.3. Medical data may be collected and processed:

a. if provided for by law for:
   i. public health reasons; or
   ii. subject to Principle 4.8, the prevention of a real danger or the suppression of a specific criminal offence; or
   iii. another important public interest; or

b. if permitted by law:
   i. for preventive medical purposes or for diagnostic or for therapeutic purposes with regard to the data subject or a relative in the genetic line; or
   ii. to safeguard the vital interests of the data subject or of a third person; or
   iii. for the fulfilment of specific contractual obligations; or
   iv. to establish, exercise or defend a legal claim; or

c. if the data subject or his/her legal representative or an authority or any person or body provided for by law has given his/her consent for one or more purposes, and in so far as domestic law does not provide otherwise.

4.4. If medical data have been collected for preventive medical purposes or for diagnostic or therapeutic purposes with regard to the data subject or a relative in the genetic line, they may also be processed for the management of a

medical service operating in the interest of the patient, in cases where the management is provided by the health-care professional who collected the data, or where the data are communicated in accordance with principles 7.2 and 7.3.

Unborn children

4.5. Medical data concerning unborn children should be considered as personal data and enjoy a protection comparable to the protection of the medical data of a minor.

4.6. Unless otherwise provided for by domestic law, the holder of parental responsibilities may act as the person legally entitled to act for the unborn child, the latter being a data subject.

Genetic data

4.7. Genetic data collected and processed for preventive treatment, diagnosis or treatment of the data subject or for scientific research should only be used for these purposes or to allow the data subject to take a free and informed decision on these matters.

4.8. Processing of genetic data for the purpose of a judicial procedure or a criminal investigation should be the subject of a specific law offering appropriate safeguards.

The data should only be used to establish whether there is a genetic link in the framework of adducing evidence, to prevent a real danger or to suppress a specific criminal offence. In no case should they be used to determine other characteristics which may be linked genetically.

4.9. For purposes other than those provided for in Principles 4.7 and 4.8, the collection and processing of genetic data should, in principle, only be permitted for health reasons and in particular to avoid any serious prejudice to the health of the data subject or third parties.

However, the collection and processing of genetic data in order to predict illness may be allowed for in cases of overriding interest and subject to appropriate safeguards defined by law.

5. Information of the data subject

5.1. The data subject shall be informed of the following elements:

a. the existence of a file containing his/her medical data and the type of data collected or to be collected;

b. the purpose or purposes for which they are or will be processed;

c. where applicable, the individuals or bodies from whom they are or will be collected;

d. the persons or bodies to whom and the purposes for which they may be communicated;

e. the possibility, if any, for the data subject to refuse his consent, to withdraw it and the consequences of such withdrawal;

f. the identity of the controller and of his/her representative, if any, as well as the conditions under which the rights of access and of rectification may be exercised.

5.2. The data subject should be informed at the latest at the moment of collection. However, when medical data are not collected from the data subject, the latter should be notified of the collection as soon as possible, as well as - in a suitable manner - of the information listed under Principle 5.1, unless this is clearly unreasonable or impracticable, or unless the data subject has already received the information.

5.3. Information for the data subject shall be appropriate and adapted to the circumstances. Information should preferably be given to each data subject individually.

5.4. Before a genetic analysis is carried out, the data subject should be informed about the objectives of the analysis and the possibility of unexpected findings.

Legally incapacitated persons

5.5. If the data subject is a legally incapacitated person, incapable of free decision and domestic law does not permit the data subject to act on his/her own behalf, the information shall be given to the person recognised as legally entitled to act in the interest of the data subject.

If a legally incapacitated person is capable of understanding, he/she should be informed before his/her data are collected or processed.

Derogations

5.6. Derogations from Principles 5.1, 5.2 and 5.3 may be made in the following cases:

a. information of the data subject may be restricted if the derogation is provided for by law and constitutes a necessary measure in a democratic society:

i. to prevent a real danger or to suppress a criminal offence.

ii. for public health reasons.

iii. to protect the data subject and the rights and freedoms of others;

b. in medical emergencies, data considered necessary for medical treatment may be collected prior to information.

6. Consent

6.1. Where the data subject is required to give his/her consent, this consent should be free, express and informed.

6.2. The results of any genetic analysis should be formulated within the limits of the objectives of the medical consultation, diagnosis or treatment for which consent was obtained.

6.3. Where it is intended to process medical data relating to a legally incapacitated person who is incapable of free decision, and when domestic law does not permit the data subject to act on his/her own behalf, consent is required of the person recognised as legally entitled to act in the interest of the data subject or of an authority or any person or body provided for by law.

If, in accordance with Principle 5.5 above, a legally incapacitated person has been informed of the intention to collect or process his/her medical data, his/her wishes should be taken into account, unless domestic law provides otherwise.

7. Communication

7.1. Medical data shall not be communicated, unless on the conditions set out in this principle and in Principle 12.

7.2. In particular, unless other appropriate safeguards are provided by domestic law, medical data may only be communicated to a person who is subject to the rules of confidentiality incumbent upon a health-care professional, or to comparable rules of confidentiality, and who complies with the provisions of this recommendation.

7.3. Medical data may be communicated if they are relevant and:

a. if the communication is provided for by law and constitutes a necessary measure in a democratic society for:
   i. public health reasons; or
   ii. the prevention of a real danger or the suppression of a specific criminal offence; or
   iii. another important public interest; or
   iv. the protection of the rights and freedoms of others; or

b. if the communication is permitted by law for the purpose of:
   i. the protection of the data subject or a relative in the genetic line;
   ii. safeguarding the vital interests of the data subject or a third person; or
   iii. the fulfilment of specific contractual obligations; or
   iv. establishing, exercising or defending a legal claim; or

c. if the data subject or his/her legal representative, or an authority, or any person or body provided for by law has given his/her consent for one or more purposes, and in so far as domestic law does not provide otherwise; or

d. provided that the data subject or his/her legal representative, or an authority, or any person or body provided for by law has not explicitly objected to any non-mandatory communication, if the data have been collected in a freely chosen preventive, diagnostic or therapeutic context, and if the purpose of the communication, in particular the provision of care to the patient or the management of a medical service operating in the interest of the patient, is not incompatible with the purpose of the processing for which they were collected.

8. Rights of the data subject

Rights of access and of rectification

8.1. Every person shall be enabled to have access to his/her medical data, either directly or through a health-care professional or, if permitted by domestic law, a person appointed by him/her. The information must be accessible in understandable form.

8.2. Access to medical data may be refused, limited or delayed only if the law provides for this and if:

a. this constitutes a necessary measure in a democratic society in the interests of protecting state security, public safety, or the suppression of criminal offences; or

b. knowledge of the information is likely to cause serious harm to the data subject's health; or

c. the information on the data subject also reveals information on third parties or if, with respect to genetic data, this information is likely to cause serious harm to consanguine or uterine kin or to a person who has a direct link with this genetic line; or

d. the data are used for statistical or for scientific research purposes where there is clearly no risk of an infringement of the privacy of the data subject, notably the possibility of using the data collected in support of decisions or measures regarding any particular individual.

8.3. The data subject may ask for rectification of erroneous data concerning him/her and, in case of refusal, he/she shall be able to appeal.

Unexpected findings

8.4. The person subjected to genetic analysis should be informed of unexpected findings if the following conditions are met:

a. domestic law does not prohibit the giving of such information;

b. the person himself has asked for this information;

c. the information is not likely to cause serious harm:
   i. to his/her health; or
   ii. to his/her consanguine or uterine kin, to a member of his/her social family, or to a person who has a direct link with his/her genetic line, unless domestic law provides other appropriate safeguards.

Subject to sub-paragraph *a*, the person should also be informed if this information is of direct importance to him/her for treatment or prevention.

9. Security

9.1. Appropriate technical and organisational measures shall be taken to protect personal data - processed in accordance with this recommendation - against accidental or illegal destruction, accidental loss, as well as against unauthorised access, alteration, communication or any other form of processing.

Such measures shall ensure an appropriate level of security taking account, on the one hand, of the technical state of the art and, on the other hand, of the sensitive nature of medical data and the evaluation of potential risks.

These measures shall be reviewed periodically.

9.2. In order to ensure in particular the confidentiality, integrity and accuracy of processed data, as well as the protection of patients, appropriate measures should be taken:

a. to prevent any unauthorised person from having access to installations used for processing personal data (control of the entrance to installations);

b. to prevent data media from being read, copied, altered or removed by unauthorised persons (control of data media);

c. to prevent the unauthorised entry of data into the information system, and any unauthorised consultation, modification or deletion of processed personal data (memory control);

d. to prevent automated data processing systems from being used by unauthorised persons by means of data transmission equipment (control of utilisation);
e. with a view to, on the one hand, selective access to data and, on the other hand, the security of the medical data, to ensure that the processing as a general rule is so designed as to enable the separation of:
- identifiers and data relating to the identity of persons;
- administrative data;
- medical data;
- social data;
- genetic data (access control);

f. to guarantee the possibility of checking and ascertaining to which persons or bodies personal data can be communicated by data transmission equipment (control of communication);
g. to guarantee that it is possible to check and establish *a posteriori* who has had access to the system and what personal data have been introduced into the information system, when and by whom (control of data introduction);
h. to prevent the unauthorised reading, copying, alteration or deletion of personal data during the communication of personal data and the transport of data media (control of transport);
i. to safeguard data by making security copies (availability control).
9.3. Controllers of medical files should, in accordance with domestic law, draw up appropriate internal regulations which respect the related principles in this recommendation.
9.4. Where necessary, controllers of files processing medical data should appoint an independent person responsible for security of information systems and data protection and competent for giving advice on these issues.

12. Scientific research
12.1. Whenever possible, medical data used for scientific research purposes should be anonymous. Professional and scientific organisations as well as public authorities should promote the development of techniques and procedures securing anonymity.
12.2. However, if such anonymisation would make a scientific research project impossible, and the project is to be carried out for legitimate purposes, it could be carried out with personal data on condition that:
a. the data subject has given his/her informed consent for one or more research purposes; or
b. when the data subject is a legally incapacitated person incapable of free decision, and domestic law does not permit the data subject to act on his/her own behalf, his/her legal representative or an authority, or any person or body provided for by law, has given his/her consent in the framework of a research project related to the medical condition or illness of the data subject; or
c. disclosure of data for the purpose of a defined scientific research project concerning an important public interest has been authorised by the body or bodies designated by domestic law, but only if:
i. the data subject has not expressly opposed disclosure; and
ii. despite reasonable efforts, it would be impracticable to contact the data subject to seek his consent; and
iii. the interests of the research project justify the authorisation; or

d. the scientific research is provided for by law and constitutes a necessary measure for public health reasons.
12.3. Subject to complementary provisions determined by domestic law, health-care professionals entitled to carry out their own medical research should be able to use the medical data which they hold as long as the data subject has been informed of this possibility and has not objected.
12.4. As regards any scientific research based on personal data, the incidental problems, including those of an ethical and scientific nature, raised by respect of the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data should also be examined in the light of other relevant instruments.
12.5. Personal data used for scientific research may not be published in a form which enables the data subjects to be identified, unless they have given their consent for the publication and publication is permitted by domestic law.

APPENDIX B

Recommendation 17 of the Committee of Ministers to member states on the impact of information technologies on health care – the patient and Internet, 2004, (extract).

(Adopted by the Committee of Ministers on 15 December 2004 at the 909th meeting of the Ministers' Deputies)

Recommends that the governments of member states:
1. adopt, where necessary, policies, legislative and other measures necessary for developing a model framework for best practices regarding information technologies in health related matters; in particular:
– by acknowledging the fundamental right of citizens to have access to information on health issues, and therefore ensuring that existing legislation and policies are conducive to this end;
– by reviewing existing policies, legislation and practices that fundamentally restrict, control or hamper patient access to information and services via the Internet and other communications media;
– by encouraging international organisations to develop a register of current legislation in all member states concerning national regulations with an impact on the Internet and patients or citizens;
– by creating an accessible database with a view to identifying all such legislation and policies which might conflict with the accepted fundamental values and principles;
– by ensuring that appropriate access to evidence-based practice on the use of the Internet for purposes of accessing information, enabling communication between patients and clinicians and delivery of health services, be reflected in the training of all health professional;
2. support and participate in preparing guidance tools for better practice of Internet users;
– by ensuring that appropriate evidence-based guidance is developed on new information communication technologies, such as the Internet, and that such guidance is integrally linked with the existing body of knowledge on educational practice guidance;
– by making educational tools available to developers of educational materials, courses and other learning opportunities, for patients, citizens, as well as health professionals;
3. promote international cooperation between organisations, research institutions and other agencies that are active in the health and Internet field in order to:
– develop international and collaborative arrangements to define and develop appropriate ways to exploit the Internet for optimal use by patients and citizens, including, but not limited to:
- quality of information provision;
- accreditation of health information services and providers;
- promoting the use of high quality legal standards in the cross-border exchange of health information between clinicians and patients;
- confidentiality, legal jurisdiction, fraud and misrepresentation by providers of information and services, and redress;
– allow the relevant organisations to review existing regulations, to ensure their compatibility with the Internet environment in respect of cross-border matters;
– avoid and solve potential conflicts between on the one hand existing data protection laws and on the other hand the freedom for patients to access health information and services in a cross-border environment;
– ensure better protection of human rights and ethical principles of the Council of Europe;
4. foresee a periodical reassessment of this Recommendation in light of the technological advances of the Internet and other existing and emergent information and communication technologies. Issues of the quality of health information and services, legal jurisdiction; and compatibility with existing Council of Europe documents and those of other bodies should be addressed;
5. take to this end, whenever feasible, the measures presented in the Appendix to this Recommendation, taking account of their respective national circumstances;
6. disseminate widely this Recommendation and its Appendix, where necessary accompanied by a translation;
7. bring these texts in particular to the attention of health authorities, the new communication and information industries and medical end-users, targeting the patient groups.

Appendix to Recommendation Rec(2004)17

I. GENERAL CONSIDERATIONS

1. The use of information technology in health care is of enormous potential to all citizens in improving information, communication and services supplied via Internet. However, the advantages and disadvantages of the Internet should be made clear to the patients-users and/or their carers. Governments should promote information about the fact that the Internet itself does not produce any new medical evidence or guarantee quality. The expectations of the benefits of new technologies should be mitigated by the latency period between the development and actual availability of new measures.
2. Governments and medical authorities should be aware of the limitations of the Internet as a source of information. Failure to make known these limitations is unethical and infringes the autonomy of the individual.
3. The responsibility is becoming increasingly shared, with health professionals maintaining their responsibility, but patients taking on more responsibility for the choice of means, and of personal responsibility through self-care and self-management.

4. The focus of this Recommendation is not only on patients, but also on all possible users, called "end-users" to avoid the more limiting connotation of the word "patient".
5. Taking a patient-oriented perspective, the three areas of end-user needs have been identified: 1. information, 2. communication and 3. services.
6. The field of information technology develops so quickly that the periodical reassessment and revision of this Recommendation should be foreseen.

II. GUIDING PRINCIPLES

1. Government policy should be based on values propounded by the Council of Europe: human rights and patients' rights, human dignity, social cohesion, democracy, equity, solidarity, equal gender opportunity, participation, freedom of choice – balanced by the obligation to help strengthen one's own health.
2. The state cannot be solely responsible for the Internet, since the Internet is unique in its forms of global governance, and operation, yet often falls within the jurisdiction of countries in virtue of the breadth of its applications. A shared approach to its development by all areas of society is necessary. This ensures that fundamental tenets of democratic society extend to the Internet and its applications
3. Governments should recognise that utilisation of the Internet is part of the fundamental freedom of choice people have in seeking information, communications and services in health.
4. Governments should promote public awareness of tools promoting quality, including systems for accrediting health information providers.
5. Governments should not apply an "Internet exceptionalism" approach; treating Internet as something fundamentally different, requiring new rules. It would just create barriers to the integration of the Internet into society.
6. Governments should ensure that regulations and laws are technology-neutral, to ensure that the legislative purpose is not invalidated by future technological innovations.
7. Health information should be in principle neither restricted nor censored. Some restrictions may be justified, for example when regulating Web advertising. However, concern about the quality of health information should be made a priority.
8. Correspondence between patients and health professionals should in all instances remain private and protected.
9. Individual member states should choose how and in what way to organise their health services to make use of the Internet.
10. Health policies are founded on the principle of universal access to health services and generally embrace active efforts to bridge social divides. The adoption of the Internet as a tool for health policy implementation is compatible with this approach.

IV. IMPACT OF THE INTERNET ON CONFIDENTIALITY AND RESPONSIBILITY IN THE MEDICAL SETTINGS

1. The services provided on the Internet could complement and enhance the traditional relationship between carers and the patient as well as the traditional model of consultation. In specific situations, they may replace traditional relationships only if potential shortcomings of online services could be neutralised by additional measures.
2. The measures to protect confidentiality and privacy should guarantee the right of citizens to self-determination and therefore provide a legal basis for data processing on the grounds of consent, contract or law. The influence of the free access of patients to electronic health records should be considered.
3. Individuals should not have to identify themselves except when it is important that their identity be known, e.g. to receive a health service or for medico-legal or reimbursement purposes. However, there are cases where anonymity might not be advisable, for example when communicating personal health data.
4. Providers of information, communication and health services should under all circumstances be identifiable, including the final owner or provider.
5. Internet care providers should be traceable and identifiable, so that security techniques, privacy policy and the identity of the individual in contact are known.
6. National governments and industry should establish nationally acceptable systems to enable the individual's personal privacy and security, in particular by encouraging the widespread availability of digital signatures and digital identities, with suitably secure communications.
7. Member states should promote the establishment of an authority or a committee, when not yet established or where necessary, which will be responsible for the development and updating of privacy and security standards.

VII. IMPACT ON QUALITY OF INFORMATION

1. A key challenge for governments is finding ways to enable consumers and health professionals to tell the difference between good and bad quality information. For that purpose, efforts are needed to create a trustworthy Internet environment for all users.
2. Properly regulated health information Internet sites, with suitable rules regarding identity of provider of information and provenance, should enable citizens, consumers, patients, and individuals generally to make up their own minds.
3. Self-regulation and the use of ethical codes should be promoted by governments and the relevant authorities. In this respect the accepted criteria of transparency and honesty, authority, privacy and data protection, updating of information, accountability and accessibility should be taken into account.
4. At a minimum, all Internet sites, whether providing information, communications or services should make explicit the following information:

– authorship of the content and who owns the site content;
– attribution of the content with specific information on who did the work;
– disclosure of what information is gathered and for what purposes the personal data are used, as well as whether they share that information and if so, with whom;
– disclosure of conflicts of interest, including any statements on the impartiality of the information. that includes sponsoring and hosting by third parties;
– the date of the content is provided or the date of latest revision, including references to sources providing additional authenticity.
5. Providers of information should be required to provide sufficient information to the public to permit identification of the sources of information, any intermediaries, and any other factors, which can offer evidence of the quality of the information. They must explicitly seek visitors' informed consent for specific data-gathering and data-sharing activities.
6. Governments should assess what quality-control system for providers of information is most appropriate for their circumstances. Governments should not necessarily undertake this role, but only ensure that a quality-control system exists. They should use existing regulations to establish quality standards for health information on Internet.

X. BEST PRACTICES
1. Each member state should decide upon the extent of information linkages, which will be considered legal and should establish the corresponding legal framework. Subject to the available technology, this framework should be enforceable.
2. Patients' organisations and NGOs should be encouraged to play an active role in the evaluation, the regulation and the accreditation of health information available through the Internet.
3. Governments should take all precautionary measures so that the rights of the patients are protected and respected, as in the traditional medical setting.
4. Member states should facilitate exchange of information regarding the types of fraud existing, the incidents reported and the policies, which has proved to be useful in similar cases.
5. Governments and health providers should ensure that they use information technologies as a way of reaching out to the public for consultation on important issues, in an active and committed manner.
6. Patients and consumers should be able to benefit from the use of the Internet when interacting with health providers, by being able to access health records, make payments, make appointments, or order medical products.
7. Public education is necessary to ensure that people feel they understand and are capable of participating fully. It is up to educational institutions (from primary school to university and beyond) and patients' groups, to help them set up support and communications programmes. Encouragement could range from favourable tax breaks for innovative non-profit services, to grants to institutions to enable public education programmes.
8. Third parties should be able to offer intermediary services to individuals to support them. The Internet has created the notion of “trusted third-parties” to ensure reliability in transactions between parties. The evolution of some into “trusted health intermediaries” may be appropriate and compatible with efforts to encourage individuals to use services, even if they do not do so directly themselves.

XI. ROLE OF DIFFERENT ACTORS
1. Government
Governments need to learn how to participate in this environment in a manner which is compatible with the innovative and accessible characteristics of the Internet.
Governments should promote specific development of the Internet and health by:
– encouraging cooperation between institutions, whether public or private;
– encouraging diversity in the provision of telecommunications services, including appropriately liberalised tariff structures to favour access and use to overcome potential social exclusion;
– promoting policies and procedures which are conducive to the development of health services, improve access, and enable uptake of services;
– promoting policies for good Internet use across the economy (public, private, voluntary sectors, individuals, patients) and which serve to enhance public knowledge through appropriate education in the use of the Internet;
– promoting policies to encourage pro-active development of health innovations through the Internet to benefit patients and citizens in the three priority areas of information, communications and services;
– protecting end-users from fraud, unethical or harmful practices, for example by:
● applying legislation on consumer rights to the Internet;
● applying legislation on patients' rights and data privacy to Internet transactions;
● applying legislation on professional misconduct, illicit practices and quackery to providers of services in Internet;
● applying legislation on drug sales to Internet.
***2.* Patients and citizens as end-users**
Individuals using the Internet should:
– exercise normal vigilance when accessing health information over the Internet to ensure that they are accessing information that is trustworthy;
– ensure they are informed consumers of health information and services.
3. Institutional health providers
Institutional health providers should:
– adopt models of service delivery over the Internet which are patient-centred;

– offer meaningful services, access to reliable information, and enable effective communications, including bringing more tele-health services into mainstream service;
– consider how the Internet can be a tool for rational service planning;
– adopt policies and evidence-based practices which actively reward or encourage innovations in the use of the Internet for health service delivery.

4. Health professionals

Health professionals should:
– be consumers informed of the Internet's potential to improve patient care, through access to reliable information, the offering of significant and substantial services and communications;
– be encouraged to develop entrepreneurial solutions to tele-health opportunities and be given the freedoms necessary to establish responsible organisations for the delivery of *evidence-based* tele-health services.

XII. RESEARCH AREAS

Research programmes should address the following issues:
– the needs of individual patients and citizens, through surveys and systematic study;
– the role of patient advocacy groups, and that of non-governmental bodies generally in health;
– the role of telecommunications companies and communications policies;
– the responsiveness of health professionals and health service providers to innovation and change;
– the role of the health economy more widely;
– the impact of the explosive growth in mobile telecommunication and its use in health care, health and new media (Internet, digital television, mobile telephones in particular);
– behaviour of patients and their use of new technologies;
– the scientific evidence on the effects of tele-health services.

APPENDIX C

Structured questionnaire to the healthcare professionals

Electronic Medical Record (EMR)

Section 1

Generic questions about the EMR

1. Have you ever used an EMR?
   (Choose only one option)

   a. ☐ No *(go to question 4)*
   b. ☐ Yes *(go to question 2)*
   c. ☐ Don't know *(go to question 4)*

2. How regularly do you use an EMR?
   (Choose only one option)

   a. ☐ Daily / almost everyday
   b. ☐ 1 to 3 times per week
   c. ☐ 1 to 3 times per month
   d. ☐ Don't know

3. What is (are) the objective(s) of that use?
   (Choose all necessary options)

   a. ☐ Consultation/search
   b. ☐ Data Input
   c. ☐ Decision Support
   d. ☐ Prescription
   e. ☐ Emergency / ICU
   f. ☐ Don't know

4. Do you think EMR is:
   (choose only one option)

   a. ☐ Not Useful
   b. ☐ Necessary evil
   c. ☐ Important for my work
   d. ☐ Indispensable
   e. ☐ Have no opinion

5. What are the problems of the EMR?
   (choose all necessary options)

   a. ☐ They have no problems
   b. ☐ They require education
   c. ☐ They require changing your tasks
   d. ☐ They are not secure
   e. ☐ Affect doctor/patient relationship
   f. ☐ They are a waste of time
   g. ☐ Have no opinion

6. What are EMR security problems?
   (choose all necessary options)

   a. ☐ Access control
   b. ☐ You do not trust the system
   c. ☐ Share sensitive information
   d. ☐ Distribute online access
   e. ☐ None
   f. ☐ No opinion

7. Did you ever participate in EMR development?
   (Choose one option)

   a. ☐ No
   b. ☐ Yes
   c. ☐ Don't know

8. Do you think you should participate in that process? *(choose one option)*

   a. ☐ No
   b. ☐ Yes
   c. ☐ No opinion

9. In which part of that process did you participate or would like to participate?
   (choose all necessary options)

   a. ☐ Idealization/conceptualization
   b. ☐ Define policies
   c. ☐ Implementation
   d. ☐ Test
   e. ☐ Don't know

Section 2

Questions about access control

10. Which mechanisms you normally use to access an EMR? *(choose one option)*

    a. ☐ It has no mechanisms
    b. ☐ Login / password
    c. ☐ Biometrics (fingerprint)
    d. ☐ Other _____
    e. ☐ Someone else accesses for me
    f. ☐ Don't know

11. If you use login / password:
    (choose all necessary options)

    a. ☐ You forget it many times
    b. ☐ You share your password
    c. ☐ Accesses the EMR easily
    d. ☐ Other _____
    e. ☐ No opinion

12. Do you take a long time to access the EMR?
    (choose one option)

    a. ☐ No
    b. ☐ Yes
    c. ☐ Don't know

13. Do you have difficulties accessing the EMR?
    (choose one option)

    a. ☐ Never
    b. ☐ A few times
    c. ☐ Regularly
    d. ☐ Many times
    e. ☐ Always
    f. ☐ Don't know

14. Do you agree with the existence of access control roles to access the EMR?
    (choose one option)

    a. ☐ No *(go to question 7)*
    b. ☐ Yes
    c. ☐ Yes for only some information
    d. ☐ No opinion

15. What type(s) of access control roles should there exist?
    (choose all necessary options)

    a. ☐ Professional category
    b. ☐ Defined by the patients
    c. ☐ Depending on the department where you work
    d. ☐ Type of information (+- sensitive)
    e. ☐ Others _____
    f. ☐ Don't know

16. Are there any access control roles in the EMR you normally use?
    (choose one option)

    a. ☐ No *(go to question 10)*
    b. ☐ Yes
    c. ☐ Don't know

17. Do you think those access control roles are adequate? *(choose one option)*

    a. ☐ No
    b. ☐ Yes
    c. ☐ No opinion

18. The access control roles within the EMR were implemented according to:
    (choose all necessary options)

    a. ☐ Professional category
    b. ☐ Defined by the patients
    c. ☐ The department where you work
    d. ☐ The type of information (+- sensitive)
    e. ☐ Others _____
    f. ☐ Don't know

19. Did you participate in the definition/choice of those access control roles? *(choose one option)*

    a. ☐ No
    b. ☐ Yes
    c. ☐ No opinion

20. Should there be mechanisms to allow any healthcare Professional to Access medical data in emergency situations?
    (choose one option and/or sub-option)

    a. ☐ No
    b. ☐ Yes
        1. ☐ everybody
        2. ☐ only professional in emergency
        3. ☐ depending on the emergency
        4. ☐ other _____
    c. ☐ No opinion

Section 3

Questions about ATM scenario

21. Do you agree with patients accessing their medical records through an ATM machine in the same way they access their bank account details?
    (choose one option)

    a. ☐ No
    b. ☐ Yes
    c. ☐ No opinion

22. Do you think ATM is a secure system?
    (choose one option)

    a. ☐ No *(go to question 3)*
    b. ☐ Yes *(go to question 4)*
    c. ☐ No opinion

23. Which are the problems of such a system (ATM)?
    (choose all necessary options)

    a. ☐ Don't know
    b. ☐ Raises ethical issues
    c. ☐ Is not secure enough
    d. ☐ Other_____
    e. ☐ No opinion

24. With what regularity do you access your bank details through an ATM machine?
    (choose one option)

    a. ☐ Daily or almost everyday
    b. ☐ 1 to 3 times per week
    c. ☐ 1 to 3 times per month
    d. ☐ Never
    e. ☐ Don't know

Section 4

Demographical questions

1. Professional category
   _____
2. Dept/Service
   _____
3. Healthcare Institution:

    a. ☐ Hospital
    b. ☐ Health Centre
    c. ☐ Laboratory
    d. ☐ Other _____
    e. ☐ Private sector
    f. ☐ Public sector

4. Working years _____

5. Academic proficiency:

   a. ☐ BSc
   b. ☐ MSc
   c. ☐ PhD
   d. ☐ Prof. Catedrático (a degree in the academic career that exists in Portugal)
   e. ☐ Other _____

6. Technical proficiency:

   a. ☐ None
   b. ☐ Some
   c. ☐ I have education
   d. ☐ Don't want to answer

7. Sex:

   a. ☐ Female
   b. ☐ Male

APPENDIX D

Structured telehone interview to the patients

Electronic Medical Record (EMR)

Section 1

General questions about EMR

1. Do you know what is an EMR?
   (choose one option)

   a. ☐ No *(go to Section 2)*
   b. ☐ Yes
   c. ☐ Does not answer

2. Do you think that the EMR is used in our country?
   (choose one option and/or sub-option)

   a. ☐ No
   b. ☐ Yes
      1. ☐ Daily or almost everyday
      2. ☐ 1 to 3 times per week
      3. ☐ 1 to 3 times per month
      4. ☐ Does not know
   c. ☐ Does not know
   d. ☐ Does not answer

3. Do you know what is(are) the objective(s) of the EMR?
   (choose all the necessary options)

   a. ☐ Consultation
   b. ☐ Search
   c. ☐ Data input
   d. ☐ Decision support
   e. ☐ Prescription
   f. ☐ Another _____
   g. ☐ Does not know

Section 2

Questions about accessing their medical records

4. Do you know that is stated in the legislation that you have the right to access your medical records whenever you need or wish?
   (choose one option)

   a. ☐ No
   b. ☐ Yes
   c. ☐ Does not answer

5. Would you like to access your medical records whenever you wanted?
   (choose one option)

   a. ☐ No *(go to question 5)*
   b. ☐ Yes
   c. ☐ Does not know
   d. ☐ Does not answer

6. Do you think you would need the help of a healthcare professional to explain you the contents of your medical records?
   (choose one option)

   a. ☐ No
   b. ☐ Yes
   c. ☐ Does not know
   d. ☐ Does not answer

7. Would you like to access your medical records with the use of a computer?
   (choose one option)

   a. ☐ No
   b. ☐ Yes
   c. ☐ Does not know
   d. ☐ Does not answer

8. Do you think that the access to your medical records can affect the confidence you have in your doctor?
   (choose one option)

   a. ☐ No
   b. ☐ Yes
   c. ☐ Does not know
   d. ☐ Does not answer

9. Do you think that the access to your medical records with the use of a computer can compromise your records' security?
(choose ont option and/or sub-options)

   a. ☐ No
   b. ☐ Yes
      1. ☐ confidentiality
      2. ☐ data sharing
      3. ☐ there is no security
      4. ☐ another _____
   c. ☐ Does not know
   d. ☐ Does not answer

10. Do you think your medical records must be available 24/7?
(choose one option)

   a. ☐ No
   b. ☐ Yes
   c. ☐ Does not know
   d. ☐ Does not answer

Section 3

Questions about access control

11. Do you think that the existing means to control access to medical information is adequate?
(choose one option)

   a. ☐ No
   b. ☐ Yes
   c. ☐ Does not know
   d. ☐ Does not answer

12. Do you think that access to medical records must be controlled with the use of access control roles?
(choose one option and/or sub-options)

   a. ☐ No
   b. ☐ Yes
      1. ☐ by professional category
      2. ☐ defined by the patients
      3. ☐ only for more sensitive information
      4. ☐ another _____
   c. ☐ Does not know
   d. ☐ Does not answer

13. Would you like to define who should access your medical records?
(choose one option)

   a. ☐ No
   b. ☐ Yes
   c. ☐ Does not know
   d. ☐ Does not answer

14. Do you think that there must be measures to allow any healthcare professional to access your medical records in an emergency situation?
(choose one option and/or sub-options)

   a. ☐ No
   b. ☐ Yes
      1. ☐ by everybody
      2. ☐ only by emergency professionals
      3. ☐ another _____
   c. ☐ Does not answer

Section 4

Questions about ATM scenario

15. Would you like to access your medical records using an ATM machine?
(choose one option)

   a. ☐ No *(go to question 6)*
   b. ☐ Yes
   c. ☐ Does not know
   d. ☐ Does not answer

16. Do you think this is an easy way to access your medical records using a card and a PIN number?
(choose one option)

a. ☐ No
b. ☐ Yes
c. ☐ Does not know
d. ☐ Does not answer

17. Do you think this is a secure way of accessing your medical records?
(choose one option)

a. ☐ No
b. ☐ Yes
c. ☐ Does not know
d. ☐ Does not answer

18. How frequently would you access your medical records using an ATM machine?
(choose one option)

a. ☐ Daily or almost everyday
b. ☐ 1 to 3 times per week
c. ☐ 1 to 3 times per month
d. ☐ Does not know
e. ☐ Never

19. What kind of medical data would you like to access more frequently?
(choose all the necessary options)

a. ☐ Exam results
b. ☐ Medication
c. ☐ Consultations
d. ☐ Another _____
e. ☐ Does not know

20. How frequently do you access and ATM machine to perform banking operations?
(choose one option)

a. ☐ Daily or almost everyday
b. ☐ 1 to 3 times per week
c. ☐ 1 to 3 times per month
d. ☐ Does not know
e. ☐ Never

Section 5

Demographical questions

1. Academic proficiency:

a. ☐ 1º to 4º cycle
b. ☐ Secondary School
c. ☐ BSc
d. ☐ MSc
e. ☐ PhD
f. ☐ Another _____

2. Informatics' Proficiency:

a. ☐ None
b. ☐ Some
c. ☐ A lot

3. Age: _____

4. Do you have a Chronic Disease?

a. ☐ Yes
b. ☐ No
c. ☐ Does not answer

5. Sex:

a. ☐ Female
b. ☐ Male

6. Healthcare Institution:

a. ☐ Hospital _____
b. ☐ Health Centre _____
c. ☐ Laboratory _____
d. ☐ Another _____

APPENDIX E

Part I

Code for the java methods: *getCoordinationAttributes* and *updateCoordinationAttributes*.

```
<%@ page import="java.io.*,issrg.simplePERMIS.*,issrg.utils.*"%>
<%@ page import="java.util.*"%>
<%@ page import="issrg.pba.*" %>
<%@ page import="issrg.pba.rbac.*" %>
<%@ page import="issrg.pba.rbac.x509.*" %>
<%@ page import="java.security.*" %>
<%@ page import="java.sql.*" %>
<%@ page import="javax.xml.parsers.*" %>
<%@ page import="javax.xml.xpath.*" %>
<%@ page import="org.w3c.dom.*" %>
<%@ page import="org.xml.sax.*" %>
<%@ page import="issrg.obligations.*" %>
<%@ page import="org.apache.log4j.Level" %>
<%@ page import="org.apache.log4j.Logger" %>
<%@ page import="org.apache.log4j.SimpleLayout" %>
<%@ page import="org.apache.log4j.FileAppender" %>
<%@ page import="org.apache.log4j.RollingFileAppender" %>
<%@ page import="org.apache.log4j.PropertyConfigurator" %>

<HTML>
<BODY>
<% Logger log = Logger.getLogger("BTGTestbed");
PropertyConfigurator.configure("/usr/local/apache-tomcat-
5.5.27/webapps/permis_web/WEB-INF/classes/log4j.properties");
%>
<%!
private static Logger logger = Logger.getLogger("BTGTestbed");
private PermisRBAC pba = null;

public boolean getCoordinationAttributes(String holder, String table) {
        boolean btgvar=false;
        try
         {
             // Load the JDBC driver
             String driverName = "com.mysql.jdbc.Driver";
            // MySQL MM JDBC driver
                        try {
                        Class.forName(driverName);
                        } catch(Exception e) {
                                e.printStackTrace();
                        System.out.println(e);
                        }
                       String url = "jdbc:mysql://localhost:3306/";
                        String dbName = "students";
                       String username = "root";
                       String password = "teste";
            Connection con = DriverManager.getConnection(url+dbName,
            username, password);
            java.sql.Statement stat = con.createStatement();
            String query = "Select distinct btg from "+table+" where
            subject='"+holder+"'";
                  ResultSet result = stat.executeQuery(query);
                        while(result.next())
                        {
                                btgvar=result.getBoolean("btg");
                        }
                 con.close();
                } catch (SQLException e) {
                        e.printStackTrace();
        }
                return btgvar;
}
```

```
public boolean updateCoordinationAttributes(String holder, String table) {
       boolean btgvar=false;
       try
        {
            // Load the JDBC driver
            String driverName = "com.mysql.jdbc.Driver";
             // MySQL MM JDBC driver

                  try {
                    Class.forName(driverName);
                    } catch(Exception e) {
                        e.printStackTrace();
                        System.out.println(e);
                    }
            String url = "jdbc:mysql://localhost:3306/";
            String dbName = "students";
             String username = "root";
             String password = "teste";
            Connection con =
            DriverManager.getConnection(url+dbName, username, password);
            java.sql.Statement stat = con.createStatement();
            String query = "update "+table+" set btg=true
                  where subject='"+holder+"'";
            int result = stat.executeUpdate(query);
            btgvar = true;
            con.close();
           } catch (SQLException e) {
            e.printStackTrace();
            System.out.println(e);
        }
        return btgvar;
}

try {
     String policy = "/usr/local/apache/conf/policybtg-url.xml";
     logger.info("read policy file - "+policy);
     File file = new File(policy);
     FileInputStream fis = new FileInputStream(file);
     String ldapbase = "dc=kent,dc=ac,dc=uk";
     String user = "cn=" + request.getParameter("user") + "," + ldapbase;
     logger.info("user to be authenticated - "+user);
     String ldapissuer = "cn=admin,dc=kent,dc=ac,dc=uk";
     Principal issuer = new SimplePERMISPrincipal(ldapissuer);
     Principal holder = new SimplePERMISPrincipal(user);
     SimplePERMISToken token = new
     SimplePERMISToken(holder,issuer,"permisRole","lecturer");
     SimplePERMISPolicyFinder finder = new SimplePERMISPolicyFinder(file);

     this.pba = new issrg.pba.rbac.PermisRBAC(finder);
     Subject subject = pba.getCreds(holder, new
     Object[]{TokenType.SIMPLE_PERMIS_TOKEN.asAttribute(token)};
     Target target = new PermisTarget("http://issrg-testbed-
     2.cs.kent.ac.uk/confidential");

     Action act = new PermisAction("BTG");
     java.util.Map<String, Object> env = new java.util.Hashtable<String,
     Object>();

     // BTG ENV for now is fixed but will be fed by new saam when it performs
     env variables
     boolean btgvar = true;
     env.put("urn:uk:ac:kent:cs:issrg:attribute:btg",btgvar);

     // Call permis authentication with btg action to get obligations back if
     there are any

     Response res  = this.pba.authzDecision(subject, act, target, env);
     if (res.isAuthorised()) {
           logger.debug("Authentication Authorized");
```

```
            Obligations obls = res.getObligations();
            if (obls!=null){
               String obligations = obls.toString();
                logger.info("got obligations back - "+obligations);
                // Get obligationID to know what coordination service to call
               String oblID = "btg";
               String table = "coordatts"+oblID;
               // Update coordination attribute BTG
               boolean btgenv = false;
                btgenv = updateCoordinationAttributes(user,table);
                 logger.info("Coordination table updated - "+table);
                // Check if there is an email obligation and call   obligation
                object to parse and perform it

                 List<Element> emailObs =
                 EmailObligation.getEmailObligations(obls.asElement());

                 // Calling email obligation service to perform obligation
                 EmailObligation service = new EmailObligation();

                    for (Element emailObl : emailObs){
                           int id = service.start(emailObl);
                           EmailObject email = service.commit(id);
                           logger.info("Performed email obligation - "+email);
                    }
                  // Open requested URL
                    String link = "http://issrg-testbed- 2.cs.kent.ac.uk/btg-
                    url/btggrant.php";
%>
<SCRIPT language="JavaScript">
window.open("<%=link%>",'_self');
</SCRIPT>
<%
             }
            } else {
             logger.debug("Authentication Unauthorized");
                 String link = "http://issrg-testbed-
                 2.cs.kent.ac.uk/students/HTTP_UNAUTHORIZED.html";
%>
<SCRIPT language="JavaScript">
window.open("<%=link%>",'_self');
</SCRIPT>
<%
            }
           } catch (Throwable ex) {
               ex.printStackTrace();
               out.println(ex);
           }
%>
</BODY>
  </HTML>
```

Part II

Code for the *EmailObligation.java*.

```
package issrg.obligations;
import issrg.utils.handler.HandlerServiceException;
import issrg.utils.handler.XMLParser;
import issrg.utils.xml.IterableChildList;
import java.util.ArrayList;
import java.util.HashMap;
import java.util.List;
import java.util.Map;
import java.util.Properties;
import javax.mail.Authenticator;
import javax.mail.Message;
import javax.mail.PasswordAuthentication;
```

```
import javax.mail.Session;
import javax.mail.Transport;
import javax.mail.internet.InternetAddress;
import javax.mail.internet.MimeMessage;
import org.w3c.dom.Element;
import org.w3c.dom.Node;
import org.apache.log4j.Level;
import org.apache.log4j.Logger;
import org.apache.log4j.SimpleLayout;
import org.apache.log4j.FileAppender;
import org.apache.log4j.RollingFileAppender;

public class EmailObligation {
    private Map<Integer, EmailObject> unprocessed;
    private int serial;
    private static Logger logger = Logger.getLogger(EmailObligation.class);

    public EmailObligation() {
           unprocessed = new HashMap<Integer, EmailObject>();
    }

    public int start(Element obligation) {
           unprocessed.put(++serial, new EmailObject(obligation));

           // if all is ok return (ready,tid) and perform commit else return
           an error and perform rollback

           logger.info("Email obligation STARTED");
           return serial;
    }

    public EmailObject commit(int id) {
           EmailObject email = unprocessed.remove(id);
    postMail(new
    String[]{email.getTo()},email.getSubject(),email.getBody(),"af84@kent.ac
    .uk");
    logger.info("Email obligation COMMITTED");
    return email;
    }

    public EmailObject rollback(int id) {
           EmailObject email = unprocessed.remove(id);
           logger.info("Email obligation ROLLBACK");
           return null;
    }

    public static List<Element> getEmailObligations(Node obligations) {
           List<Element> res = new ArrayList<Element>();
           for (Node child : new IterableChildList(obligations)) {
                  if (!(child instanceof Element)) {
                         continue;
                  }
           Element elem = (Element) child;
                  if (
                  "urn:oasis:names:tc:xacml:email".equals(elem.getAttribute("
                  ObligationID"))) {
                         res.add(elem);
                  }
    }
    return res;
    }

    // This method sends an email message

    public void postMail( String recipients[ ], String subject, String
    message , String from) {
        boolean debug = false;
       try {
         //Set the host smtp address
```

```
          Properties props = new Properties();

          // Using authentication with the SMTP server
            props.put("mail.smtp.auth", "true");
            props.put("mail.smtp.port", "465");
            props.put("mail.smtp.socketFactory.port", "465");
            props.put("mail.smtp.socketFactory.class","javax.net.ssl.SSLSocke
            tFactory");
            props.put("mail.smtp.socketFactory.fallback", "false");
            props.setProperty("mail.smtp.quitwait", "false"); */
            props.put("mail.smtp.host", "mx.cs.kent.ac.uk");
            props.put("mail.transport.protocol", "smtp");

            Session s = Session.getDefaultInstance(props);
            s.setDebug(debug);

          // create a message
          Message msg = new MimeMessage(s);

          // set the from and to address
          InternetAddress addressFrom = new InternetAddress(from);
          msg.setFrom(addressFrom);

          InternetAddress[] addressTo = new
          InternetAddress[recipients.length];
          for (int i = 0; i < recipients.length; i++)
          {
              addressTo[i] = new InternetAddress(recipients[i]);
          }
          msg.setRecipients(Message.RecipientType.TO, addressTo);

          // Optional : You can also set your custom headers in the Email if
          you Want
          msg.addHeader("MyHeaderName", "myHeaderValue");

          // Setting the Subject and Content Type
          msg.setSubject(subject);
          msg.setContent(message, "text/plain");
          Transport.send(msg);

        } catch (Throwable ex) {
              ex.printStackTrace();
        }
    }
    private class SMTPAuthenticator extends       javax.mail.Authenticator {
    public PasswordAuthentication getPasswordAuthentication() {
                String username = "af84";
                String password = "teste";
                return new PasswordAuthentication(username,password);
          }
    }
}
```

Part III

Code for the *Emailobject.java*.

```
package issrg.obligations;
import issrg.utils.xml.IterableChildList;
import org.apache.log4j.Level;
import org.apache.log4j.Logger;
import org.apache.log4j.RollingFileAppender;
import org.apache.log4j.SimpleLayout;
import org.apache.log4j.FileAppender;
import org.w3c.dom.Element;
import org.w3c.dom.Node;
import org.w3c.dom.NodeList;
```

```
public class EmailObject {
    private static Logger logger = Logger.getLogger(EmailObject.class);

    private static final String
    MAILTO="urn:oasis:names:tc:xacml:2.0:example:attribute:mailto";
    private static final String
    SUBJECT="urn:oasis:names:tc:xacml:2.0:example:attribute:subject";
    private static final String
    TEXT="urn:oasis:names:tc:xacml:2.0:example:attribute:text";

           private String from;
           private String to;
           private String subject;
           private String body;

           public String getFrom() {
                  return from;
           }

           public String getTo() {
                  return to;
           }

           public String getSubject() {
                  return subject;
           }

           public String getBody() {
                  return body;
           }

           public EmailObject(Element obligation) {

                  from = "";
                  Node child = obligation.getFirstChild();
                  to = getAttributeValue(child);
                  child = child.getNextSibling();
                  subject = getAttributeValue(child);
                  child = child.getNextSibling();
                  body = getAttributeValue(child);

           }

           // Node is an AttributeAssignement element
           private String getAttributeValue(Node node) {
                  if (!(node instanceof Element)) {
                 logger.debug("Empty node - Element expected");
                  return "element  expected";
                  }
                  Element elem = (Element) node;
           NodeList list =
    elem.getElementsByTagName("AttributeValue");
           if (list.getLength() > 0) {
                  logger.info("Element found:
                  "+list.item(0).getFirstChild().getNodeValue());
                  return list.item(0).getFirstChild().getNodeValue();
           } else {
                  return "finished";
           }
    }

           public String toString() {
                  return "From:" + from + "\n "
                  + "To:" + to + "\n "
                  + "Subject:" + subject + "\n "
                  + "Message:" + body + "\n";
           }
    }
```