4ª ed

MIM

One way to patient empowerment

A proposal for an authorization model

Cátia Andreia Santos Pereira

MESTRADO EM
INFORMÁTICA MÉDICA
2º CICLO DE ESTUDOS

OCTOBER|2011

4ª ed

MIM

One way to patient empowerment

A proposal for an authorization model

Cátia Andreia Santos Pereira

MESTRADO EM
INFORMÁTICA MÉDICA
2º CICLO DE ESTUDOS

ORIENTADORES:

Ana Margarida Leite de Almeida Ferreira
Informatics Specialist in Computer Center
Faculty of Medicine, University of Porto

Ricardo João Cruz Correia
Assistant Professor
Department of Health Information and Decision Sciences – CIDES
Faculty of Medicine, University of Porto

To my parents and sister for all their unconditional support and constant encouragements

Contents

Abbreviations and Acronyms ..... **i**
List of figures ..... **iii**
List of tables ..... **v**
Acknowledgements ..... **vii**
Context ..... **ix**
Abstract ..... **xi**
Resumo ..... **xiii**
Structure of the thesis ..... **xv**
Contributions ..... **xvii**
1. Introduction and Motivation **1**

1.1 Background 4
1.1.1 Healthcare Legislation 4
1.1.2 Impact of facilitating patients accessing their medical records 5
1.1.3 The fundamentals of access control 6
1.1.4 NIST RBAC 9
1.2 Research question 16
1.3 Objectives 16

2. Customizable access control models for patients: a systematic review. **19**

2.1 Introduction 21
2.2 Methods 21
2.3 Results 23
2.4 Discussion 29

3. Model definition **31**

3.1 Introduction 33
3.2 ISO 13606-4 33
3.3 RBAC model 35
3.4 Break the Glass access 39
3.5 Temporal Constraints 40
3.6 Discussion 40

4. The proposed patient authorization model 41

4.1 Introduction 43
4.2 Prerequisites 43
4.2.1 Patient's Healthcare Network 43
4.2.2 Authentication 45
4.2.3 Access to record components 45
4.2.4 Insertion of new record components 46
4.3 The formal proposed patient authorization model and architecture 46
4.4 Discussion 49

5. Patient authorization model - proof of concept 51

5.1 Introduction 53
5.2 Example of patient administration 53
5.3 Storyboards and use-cases 53
5.3.1 Storyboard 1 – The patient corrects data in his EHR 53
5.3.2 Storyboard 2 – The patient has the need of medical care while travelling 55
5.3.3 Storyboard 3 – The patient's son accesses his father's EHR 56
5.4 Discussion 58

6. Conclusions and recommendations 61

6.1 Research summary 63
6.2 Main findings 63
6.3 Limitations of the patient's authorization model 64
6.4 Recommendations and future work 64
6.5 Conclusions 65

References 67
Appendix 75

Articles submitted to the Conference HealthInf 2012 waiting for approval 77

Abbreviations and Acronyms

ABAC	Attribute-Based Access Control
AdJ	Administrator Junior
AdS	Administrator Senior
AJ	Administrative Junior
AMD	Age Related Macula Degeneration
ANSI	American National Standards Institute
ARBAC	Administrative Role Based Access Control
AS	Administrative Senior
ATM	Automatic Teller Machine
BTG	Break-The-Glass
BTG-RBAC	Break-The-Glass Role Based Access Control
CB	Color Blindness
CEN	Comité Européen de Normalisation
CIDES	Department of Health Information and Decision Sciences
CINTESIS	Center for Research in Health Technologies and Information Systems
CPR	Computerized Patient Record
CRUD	Create, Read, Update and Delete
C-TMAC	Contextual Team Based Access Control
DAC	Discretionary Access Control
DD	Demographic Data
DM II	Diabetes Mellitus II
DSD	Dynamic Separation of Duties
EHR	Electronic Health Record
EMR	Electronic Medical Record
FMUP	Faculty of Medicine University of Porto
GP	General Practitioner
GTRBAC	Generalized Temporal Role Based Access Control
HCP	Healthcare Professional
HIPAA	Health Insurance Portability and Accountability Act
HIS	Healthcare Information Systems
HP	Healthcare Professional (functional role)
HRP	Health-related Professional

IEEE	Institute of Electric and Electronics Engineers
INCITS	International Committee for Information Technology Standards
IS	Information System
ISO	International Standards Organization
IT	Information Technology
MAC	Mandatory Access Control
MeSH	Medical Subject Heading terms
NIST	National Institute of Standards and Technology
OASIS	Open Architecture for Security Interworking Services
OBS	Objects
ORBAC	Organizational Role Based Access Control
OPS	Operations
P	Patient
PA	Permission-assignment
Pen A	Penicillin Allergy
PMAC	Privilege Management and Access Control
PHN	Patient's Healthcare Network
PHP	Personal Healthcare Professional
PIN	Personal Identification Number
PrHP	Privileged Healthcare Professional
PRMS	Permissions
RBAC	Role Based Access Control
SC	Subject of Care
SCa	Subject of Care Area
SCA1	Subject of Care Agent Direct
SCA2	Subject of Care Agent Indirect
SitBAC	Situation Based Access Control
SoD	Separation of Duties
SSD	Static Separation of Duties
TBAC	Task-Based Access Control
UA	User-assignment

List of figures

FIGURE 1.1: ELEMENTS AND THEIR RELATIONS IN THE CORE RBAC MODEL..... 10
FIGURE 1.2: CORE RBAC INTERACTIONS DIAGRAM [FERREIRA 2010]. 12
FIGURE 1.3: USER, ROLE AND PERMISSION RELATIONSHIP 12
FIGURE 1.4: ROLE HIERARCHY, AN EXAMPLE [FERRAIOLO, ET AL. 2007]..... 13
FIGURE 1.5: SUMMARY OF RBAC MODEL [FERRAIOLO, ET AL. 2007] [SEJONG AND RAVI 2002] [RAVI, ET AL. 1999]. 15
FIGURE 2.1: FLOWCHART REPRESENTING THE REVIEW PROCESS AND SUBSEQUENT RESULTS. 23
FIGURE 2.2: ILLUSTRATIVE ACCESS CONTROL EXAMPLE [ISO/TS 13606-4 2009]. 28
FIGURE 3.1: HIERARCHICAL FUNCTIONAL ROLES DIVIDED INTO THREE GROUPS. 36
FIGURE 3.2: ADMINISTRATOR HIERARCHY ROLES..... 38
FIGURE 4.1: PATIENT'S HEALTHCARE NETWORK..... 43
FIGURE 4.2: EXAMPLE OF A USER DELEGATION OUTSIDE OF THE PHN PERFORMED BY DR. CHEN TO DR. WHITE..... 44
FIGURE 4.3: ARCHITECTURE OF THE PROPOSED PATIENT AUTHORIZATION MODEL BASED ON [RAVI, ET AL. 1999], [SANDHU, ET AL. 2000], [JOSHI, ET AL. 2002], [FERREIRA, ET AL. 2009] AND [ISO/TS 13606-4 2009]. 48
FIGURE 5.1: USE CASE 1 FOR STORYBOARD 1. 55
FIGURE 5.2: USE CASE 2 FOR STORYBOARD 2. 56
FIGURE 5.3: USE CASE 3 FOR STORYBOARD 3. 57

List of tables

TABLE 1.1: BRIEF COMPARISON BETWEEN THE ACCESS CONTROL MODELS: DAC, MAC AND RBAC [JOSHI, ET AL. 2001]. 9
TABLE 2.1: SUMMARY OF RESULTS OF THE LITERATURE REVIEW. 25
TABLE 3.1: SENSITIVITY VALUES AND LEVELS DEFINED FOR EACH RECORD_COMPONENT [ISO/TS 13606-4 2009]. 34
TABLE 3.2: LIST OF FUNCTIONAL ROLES [ISO/TS 13606-4 2009]. 34
TABLE 3.3: MAPPING OF FUNCTIONAL ROLES IN RECORD_COMPONENT SENSIVITY. ADAPTED FROM [ISO/TS 13606-4 2009]. 37
TABLE 5.1: EXAMPLE OF THREE STORYBOARDS WITH THE PERMISSIONS TO ACCESS AN EHR DEFINED BY THE PATIENT. 54

Acknowledgements

To my mentor and supervisor, Doutora Ana Margarida Ferreira, whose availability and help whenever I requested, expertise, understanding, and friendship were essential in accomplishing this work.

To my supervisor, Doutor Ricardo Correia, I would like to acknowledge his constant support, friendship and knowledge in the area of health informatics.

To Doutor Luis Filipe Antunes I would like to acknowledge his expertise help in formal models' definition.

To my colleagues in Center for Research in Health Technologies and Information Systems (CINTESIS) for their support and help.

And last but not least to all my friends for being an inexhaustible source of patience, support and encouragement helped me to pursue my goals with passion and dedication.

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

Cátia Santos Pereira
October 17, 2011

Context

After finishing a graduation in Biomedical Engineering at the Polytechnic Institute of Bragança, in 2009, the author started in the same year a Masters' degree in Medical Informatics at the Faculty of Medicine, University of Porto. This master degree increases the author's interest in computer security and she writes the first article in this area: "Protection of clinical data - Comparison of European with American Legislation and respective technological applicability."

In March 2010, the author started working as research investigator in Center for Research in Health Technologies and Information Systems (CINTESIS) at the Faculty of Medicine, University of Porto. The author researches and works in the area of software engineering in health information systems.

In July 2011, the author starts working as a research investigator in the project OFELIA – Open Federated Environments Leveraging Identity and Authorization [PTDC/EIA- EIA/104328/2008] funded by FEDER funds (Programa Operacional Factores de Competitividade – COMPETE) and by National funds (FCT – Fundação para a Ciência e a Tecnologia) in CINTESIS. This project challenged the author's knowledge in the information security domain together the knowledge obtained in the first year of master's degree as well as the previously developed work in software engineering. All this developed expertise resulted in this master thesis.

Abstract

European and American Legislation for protection of medical data agree that the patient has the right to play a pivotal role in the decisions regarding the content and distribution of her/his medical records. The Role Based Access Control (RBAC) model is the most commonly used access control model in healthcare but there are also standards that define guidelines for access control in healthcare.

The aim of this master thesis is to firstly verify if existing standards and RBAC based models comply with legislation requirements regarding patient access as well as customized access to his/her Electronic Health Record (EHR) and secondly to define and propose a patient authorization model based on RBAC to be used and customized by the patient.

A literature review of published material was performed and comprised 22 articles and standards from which 12 were included for analysis. Results of the systematic review show that only two models and two standards include patients as a user of the EHR and only one model and one standard provide the possibility for them to customize access control to their EHR. Existing standards define some guidelines for these issues but they are too generic to be directly applied to real healthcare settings.

The proposed patient authorization model is described within a "Patient's Healthcare Network" (PHN), and combines several characteristics from ISO 13606-4 standard, RBAC and Administration Role Based Access Control (ARBAC) models, temporal constraints, user delegation and break the glass permissions. The patient will actively manage the roles and permissions as well as give permissions of user delegation to other roles, if necessary.

With this model is expected to start bridging the gap that exists between legislation and what really happens in practice in terms of patients controlling and be actively involved in their healthcare. Future work includes the implementation and evaluation of the proposed model with a specific case study in real healthcare practice.

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

Resumo

Tanto a Legislação Europeia como a Legislação Americana para proteção de dados clínicos concordam que o utente tem o papel principal relativamente a decisões sobre o conteúdo e distribuição dos seus registos clínicos. O modelo de Controlo de Acesso Baseado em Papéis (RBAC - *Role Based Access Control*) é o modelo de controlo de acesso mais usado na área da Saúde mas também existem normas para controlo de acesso nesta área.

Esta tese de mestrado tem como intuito numa primeira fase verificar a existência de normas e modelos baseados no modelo RBAC que estejam de acordo com os requisitos da legislação, no que diz respeito ao utente aceder assim como personalizar o acesso ao seu registo clinico electrónico (EHR - *Electronic Health Record*) e numa fase posterior definir e propor um modelo de autorização baseado no modelo RBAC para ser usado e personalizado pelo utente.

Realizou-se uma revisão da literatura que teve como resultado 22 artigos e normas de onde 12 foram incluídos para análise. Os resultados da revisão sistemática mostraram que somente dois modelos e duas normas incluem o utente como um utilizador do EHR e somente um modelo e uma norma mencionam a possibilidade do utente personalizar o controlo de acesso do seu EHR. As normas definem apenas protocolos sobre estas questões por isso são muito genéricas para ser aplicadas diretamente nos cenários de cuidados de saúde.

O modelo de autorização do utente é descrito dentro de uma "rede de cuidados de saúde" (PHN - *Patient Healthcare Network*) e combina características da norma ISO 13606-4, modelo RBAC e modelo de administração RBAC (ARBAC - *Administrative Role Based Access Control*), restrições temporais, delegação de utilizador e permissões para "partir o vidro". O utente administrará os papéis e funções do modelo assim como dará permissões de delegação de utilizadores para outros papéis, se necessário.

Com este modelo é esperado que preencha a lacuna existente entre a legislação e o se verifica na realidade em termos do utente controlar e estar ativamente envolvido nos seus cuidados de saúde. Como trabalho futuro pretende-se implementar e avaliar o modelo de autorização proposto num cenário de cuidados de saúde real.

Palavras-chave: Empoderamento do Paciente, Segurança Informática, Confidencialidade, Registo Clinico Electrónico, Modelo de Controlo de Acesso Baseado em Papéis e Normas de Controlo de Acesso.

Structure of the thesis

This section presents the organization of the thesis. This MSc thesis is organized into six chapters.

The first one "*Introduction and Motivation*" introduces the theme of this thesis in the subchapter "Background", describes the research questions and details the objectives of the execution of this work.

The second chapter "*Customizable access control models for patients: a systematic review*" includes a state of the art review about Role Based Access Control (RBAC) models in healthcare setting. As an outcome of this review a paper, "Providing for patient empowerment - A systematic review on customizable access control models", was submitted for the Healthinf conference and is awaiting approval.

The third chapter "*Model definition*" follows the results of the second chapter, organizing the features of the authorization models found in the systematic review and defining the functions of these features in the proposed patient authorization model.

"*The proposed authorization model*" is the fourth chapter and describes the authorization model prerequisites as well as its formal architecture.

Chapter five "*Patient authorization model proof of concept*" presents a set of storyboards that help to understand the model behavior as well as the utility and flexibility of the proposed model.

From chapters three, four and five resulted the elaboration of the paper "One way to patient empowerment - A proposal for an authorization model" submitted for Healthinf conference and awaiting approval.

And, finally, chapter six "*Conclusions and recommendations*" presents the research summary, the main findings, the limitations of the proposed authorization model as well as the recommendations and future work.

Contributions

This section describes the contributions that were obtained during this research. These include: articles that were published and submitted as well as oral communications where this work was very often discussed and improved.

Articles published

C. Pereira*, et al.*, "Protection of clinical data - Comparison of European with American Legislation and respective technological applicability In Proceedings of the International Conference on Health Informatics - HealthInf 2011, Rome, Italy, 2011.

Santos-Pereira, *et al.*, "The International Standard ISO/IEC 9126-1 as a support to define requirements for Health Information Systems - preliminary study" In Proceedings of the 6ª Conferência Ibérica de Sistemas e Tecnologias de Informação - CISTI 2011. Chaves, Portugal, 2011.

Articles submitted and waiting for approval

Santos-Pereira*, et al.*, "Providing for patient empowerment - A systematic review on customizable access control models" submitted to International Conference on Health Informatics - HealthInf 2012, Vilamoura, Portugal, 2012.

Santos-Pereira*, et al.*, "One way to patient empowerment - A proposal for an authorization model" submitted to International Conference on Health Informatics - HealthInf 2012, Vilamoura, Portugal, 2012.

Oral communications

"Protection of clinical data - Comparison of European with American Legislation and respective technological applicability" in Health Informatics Symposium 2010, in Faculty of Science, University of Porto.

"Protection of clinical data - Comparison of European with American Legislation and respective technological applicability" in Health Informatics Seminary 2011, in Faculty of Medicine, University of Porto.

"One way to patient empowerment - A proposal for an authorization model", Health Informatics Symposium 2011, in Faculty of Science, University of Porto.

"One way to patient empowerment - A proposal for an authorization model", in Conference Medinfor II "A medicina na era da informação", 2011, in Faculty of Medicine, University of Porto.

Others contributions during the last two years not directly associated with this research

"*HealthCare Anywhere - Interoperabilidade entre Sistemas Clínicos*", proposal for a Patient Health Record that allows the patient to access their clinical history during the moment of care. This report includes state of the art, patient mobility study, evaluation of healthcare professional's information needs in the moment of care in the context of patient's geographic mobility, architecture system, requirements specification and evaluation protocol (March/2010 — May/2011).

- The chapter "*Evaluation of healthcare professional's information needs in the moment of care in the context of patient's geographic mobility*" was written using as its basis a questionnaire performed to health professionals in different health institutions (health centers and hospitals). This work is still in progress in collaboration with the project "*SAHIB - Enhancing multi-institutional health data availability through multi-agent systems"* [PTDC/EIA-EIA/105352/2008] funded by FEDER funds (Programa Operacional Factores de Competitividade – COMPETE) and by National funds (FCT – Fundação para a Ciência e a Tecnologia) (October/2010 →).

Collaborator in the project "*Optimização de Sistemas de Informação: melhorando interfaces gráficos do utilizador e a gestão de armazenamento através de aprendizagem automática em dados de logs de utilizadores*" [PTDC/EIA-EIA/099920/2008] done the collection and preparation of the various Hospital Information System's logs (July/2010 — October/2010).

Collaborator in the audit report "*Auditoria à aplicação WebGDH",* writing the chapter "Requirements Specification" (January/2011 — February/2011).

1. Introduction and Motivation

"It's a job that's never started that takes the longest to finish."
J. R. R. Tolkien

For the past two decades, many paper-based health systems have been replaced by electronic-based records such as Electronic Health Records (EHR) [Peleg, et al. 2008] [Watts, et al. 2010].

EHRs can introduce more potential benefits than paper-based records such as enhancing readability, availability and accessibility of information [Watts, et al. 2010]. EHRs can also help to empower patients to take a more active role in their health and in the health of their families. Patients can receive electronic copies of their medical records and share their health information securely over the Internet with their families [Department of Health & Human Services 2011]. However, healthcare information systems (HIS) security threats have increased significantly in recent years [Samy, et al. 2009].

Protection of medical data regulations such as *Health Insurance Portability Accountability Act* (HIPAA) in American legislation and the *Recommendation No R (97) 5* in European legislation cannot fully protect the security of patient's data [U.S. Department of Health & Human Services 1996] [Council of Europe 1997] [Watts, et al. 2010] [Samy, et al. 2009], for instance, during the period from 2006 to 2007, in USA, over 1.5 million names were exposed during data breaches that occurred in hospitals alone [Solutions 2008].

Vaast, E. classified threats to hospital HIS in two main categories: internal and external threats [Vaast 2007]. An internal threat includes various types of employee behavior such as employee´s ignorance, curiosity, recklessness, taking someone else´s password and giving their password to another employee. The external threats can include viruses and spyware attacks, hackers and intruders in the premises.

Advanced security is required in communication and use of health information due to the high sensitivity of person-related information and its corresponding personal and social impact [Joshi, et al. 2001].

The main goals of information security are to achieve confidentiality, integrity, and availability of information. [Joshi, et al. 2001]. The aim of confidentiality is to ensure that information is not accessed by an unauthorized person. The goal of information integrity is to protect information from unauthorized modification. Information availability ensures that information is available when needed and is not made inaccessible by malicious data-denial activities or others [Joshi, et al. 2001]. Keeping patient data private is one of the most important requirements in a HIS [Watts, et al. 2010].

According to the ISO/TS 22600 international standard authorization is the process of granting rights, which includes the granting of access rights [ISO/TS 22600-2 2006]. Access control is essential to provide for the confidentiality of

EHR because it is part of the authorization process where the system checks if the user can access the resources he/she requested. The most commonly used access control model in healthcare is the Role Based Access Control (RBAC) [Sandhu, et al. 2000, Ferreira, et al. 2007].

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

In addition, some studies regarding the access of medical records by the patient suggest modest improvements in doctor-patient communication adherence, patient empowerment and patient education [Ross and Lin 2003] [Ferreira, et al. 2007]. Patient empowerment in the health care context means to promote autonomous self-regulation so that the individual's potential for health and wellness is maximized, this begins with information and education and includes seeking out information about one's own illness or condition, and actively participating in the treatment decisions [Lau 2002].

1.1 Background

1.1.1 Healthcare Legislation

In the USA, in 1996, the Law 104-191, also known as the "Health Insurance Portability and Accountability Act of 1996" – HIPPA, was published. For this legislation, two regulation documents were created. They provide a set of best practices that healthcare institutions must follow in order to guarantee a minimum level of information security. These documents are called Security Rule and Privacy Rule [Pereira, et al. 2011]. Similar legal efforts in this area are under way in Canada, Ireland, South Africa, and Australia [Ross and Lin 2003].

In Europe, in 1997, the European Recommendation on the Protection of Medical Data focuses on ensuring proper safeguard and management of the confidentiality, integrity and availability of personal medical data [Council of Europe 1997]. Furthermore, it states that medical data is subject to the rights and fundamental freedoms of the individual, stating this way the right to privacy. In 2004, the same 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 collection, processing and access [Council of Europe 2004].

In 2005, Portugal approved the Law 12/2005, called the "Law of Genetic Information", whose Article 3 deals with the patient as the ownership of health information. So, as the ownership he/she has the right to access his/her medical information [República Portuguesa 2005]. The "*Conselho National de Ética para as Ciências da Vida*" (National Council of Ethics for Life Sciences), in 2011 published the document "*Parecer nº 60 - Informação de Saúde e Registo Informáticos de Saúde*", which relates that health record informatics applications may provide mechanisms: (1) that allow only the medical record's access by authorized healthcare professionals (HCP) that have direct responsibility in the care of the patient; (2) in case of patient privacy breaches, the system should provides an alert mechanism; (3) where HCP can fundament their reasons and identify them in case of trying to access unauthorized medical information of a patient [Conselho Nacional de Ética para as Ciências da Vida 2011].

These laws are similar because state that the subject of care (normally the patient) has the right to play a pivotal role in the decisions regarding the content and distribution of her/his medical records, as well as the right to be informed of its contents [U.S. Department of Health & Human Services 1996] [Council of Europe 1997].

In the information age, people and governments are becoming more aware of the need to protect their private electronic data from falling into the wrong hands. This is especially true for medical data which most people regard as sensitive [Beimel and Peleg 2009]. In a near future, information technology may make it even easier to provide patients a chance to review their records in a safe way [Hassol, et al. 2004]. This research tries to get a step closer to this future.

1.1.2 Impact of facilitating patients accessing their medical records

In the healthcare domain, digital data that is collected about the patient into a medical record is often called Electronic Health Record (EHR), Electronic Medical Record (EMR), or Computerized Patient Record (CPR). EHR has many functions and includes various kinds of data items such as diagnoses, hospital admissions, medications, operations, laboratory tests, imaging, and pathology data [Hayrinen, et al. 2008] [Peleg, et al. 2008]. In order to protect patient´s privacy it is essential to provide information confidentiality. The

design and implementation of proper models for authorization and access control for EHR are fundamental [Motta 2003].

Some studies regarding the access, by the patients to their EHR suggest modest improvements in doctor-patient communication adherence, patient empowerment and patient education [Ross and Lin 2003] [Ferreira, et al. 2007]. This process can also make patients more careful when following medical recommendations [Ferreira, et al. 2007].

Although patients may find some parts of their EHR difficult to understand, patients who are offered a chance to review their EHR are mostly satisfied with the experience [Ross and Lin 2003] [Hassol, et al. 2004] [Ferreira, et al. 2007] [Honeyman, et al. 2005]. On the other hand healthcare providers also recognized the benefit of patient's ability to review and comment on their medical information prior to a visit [Siteman, et al. 2006]. This fact can allow patients more autonomy and self-efficacy by increasing a sense of ownership to their medical records.

Patients as wells as HCP seem to be unanimous in their belief that the impact of patient's accessing their medical records can be positive for both parties [Ferreira, et al. 2007].

1.1.3 The fundamentals of access control

Privacy can be interpreted as a human desire to keep certain personal details confidential [Peleg, et al. 2008]. The privacy preservation problem has a major effect on human communities, as it touches upon social, cultural, economical, and political aspects. Privacy solutions can be roughly divided into three categories [Peleg, et al. 2008]:

- Privacy preservation via identity protection, e.g., fingerprint recognition system;
- Privacy preservation via anonymity, e.g. anonymizing private data that include explicit identifiers;
- Privacy preservation via restricting access to data, e.g., access control and authorization models.

Access control is only one aspect of a comprehensive computer security solution, but is one of the most noted. Every time a user logs on to a multiuser computer system, access control is enforced. Access Control is critical to preserving the confidentiality and integrity of information [Ferraiolo, et al. 2007].

Authentication vs. Authorization

Authorization and authentication are fundamental to access control. They are distinct concepts but often confused. Authorization, in fact, is dependent on authentication [Ferraiolo, et al. 2007].

Authentication is the process of reliably identifying security subjects by securely associating an identifier and its authenticator [ISO/TS 22600-2 2006]. Every computer user is familiar with passwords, the most common form of authentication. Less commons forms of authentication include biometrics (e.g. fingerprint readers) and smart cards. Authentication is based on the following factors:

- Something you know (e.g. password, personal identification number (PIN), or lock combination);
- Something you have (e.g. smart-card, automatic teller machine (ATM) card or key);
- Something you are (e.g. fingerprint or retinal pattern or a facial characteristic).

While authentication is a process of determining who you are, authorization determines what you are allowed to do. Authorization is the process of granting access rights [ISO/TS 22600-2 2006], it refers to a yes or no decision as to whether a user is granted access to a system resource [Ferraiolo, et al. 2007]. An information system must maintain some relationship between user IDs and system resources, possibly by attaching a list of authorized users to resources, or by storing a list of accessible resources with each user ID.

Comparing MAC, DAC and RBAC

Traditional access control models are broadly categorized as discretionary access control (DAC) and mandatory access control (MAC) models. New models such as role-based access control (RBAC) model received increased attention as a generalized approach to access control because they provide several well-recognized advantages [Joshi, et al. 2001].

In the **Discretionary Access Control** model, all subjects and objects in a system are enumerated and the owner of those objects specifies the access authorization rules for each subject and object. Subjects can be users, groups, or processes that act on behalf of other subjects. If a subject is the owner of an object, the subject is authorized to grant or revoke access rights on the object to other subjects at his discretion [Joshi, et al. 2001, Giuri 1996].

DAC can be represented by an access control matrix that indicates which subjects (one row for each) can access which objects (each column) via which modes (the cell contents) [Eyers, et al. 2005].

This model is often perceived as meeting the security processing needs of industry and civilian government [Ferraiolo, et al. 2007].

In the **Mandatory Access Control** (MAC) model, all subjects and objects are classified based on predefined sensitivity levels that are used in the access decision process [Giuri 1996]. An important goal of a MAC model is to control information flow in order to ensure confidentiality and integrity of the information, which is not addressed by DAC models. MAC is normally useful for military systems [Giuri 1996] where there is a strict ordering to both principals (e.g. users) and privileges or resources [Eyers, et al. 2005].

The most widely used access control model in healthcare is the **Role Based Access Control** (RBAC) [Sandhu, et al. 2000] [Ferreira, et al. 2007] [Beimel and Peleg 2009]. This model has emerged as a promising alternative to traditional discretionary and mandatory access control (DAC and MAC) models [Joshi, et al. 2001] [Giuri 1996] [Osborn, et al. 2000].

The Role-based access control (RBAC) model, was proposed in 1996 by Sandhu *et al.*, who adopted the "need to know" concept and integrated it into the model [Sandhu, et al. 2000] [Peleg, et al. 2008]. The concept assumes that privacy is preserved as long as data access processes occur only when they are necessary for a right purpose, and minimum details are revealed along the process. This model has an access control policy that bases access control decisions on the functions the user is allowed to perform within an organization [Giuri 1996].

RBAC is by many considered particularly well-suited for HIS, because it provides several well-recognized advantages like simplicity and ease of administration, flexibility and scalability [Røstad 2009].

RBAC is receiving increased attention as a generalized approach to access control because it provides several well-recognized advantages [Joshi, et al. 2001]. Table 1.1 describes a brief comparison between the previously mentioned models.

Table 1.1: Brief comparison between the access control models: DAC, MAC and RBAC [Joshi, et al. 2001].

DAC	• Ownership-based, flexible, does not provide a high degree of security, and hence low assurance • It cannot be used where classification levels are needed • Types of versions have tried to include classification levels
MAC	• Administration-based • Information flow control rules • High level of security, and hence high assurance, but less flexible
RBAC	• Policy-neutral/ flexible • Principle of least privilege • Separation of duties • Easy administration features • Able to express DAC, MAC, and user specific policies using role hierarchy and constraints • Can be easily incorporated into current technologies

Each model uses different types of methods to control how subjects access resources. These methods depend on the business and security goals of an organization. The models can be used exclusively or combined so that they achieve the necessary security level required by the environment.

To enforce its objectives and rules, a model uses authentication and/or access control technologies and mechanisms. Examples of authentication mechanisms are: username/password or PIN; biometrics; token devices; smartcards. Examples of access control mechanisms are: access control lists, capability tables, policy-based systems or constrained user interfaces [Gollmann 1999].

1.1.4 NIST RBAC

NIST proposed a reference model, the Role Based Access Control model which was approved as a standard and published in the document ANSI INCITS 359-2004 [Sandhu, et al. 2000]. The RBAC model is defined in terms of different model components, including the Core RBAC, the Hierarchical

RBAC, and the Constrained RBAC. The Core RBAC defines a minimum collection of RBAC elements, element sets, and their relations. The Hierarchical RBAC component adds relations for supporting role hierarchies. Constrained RBAC adds Separation of Duties (SOD) relations to the RBAC model, which are used to avoid conflict of interest [Sandhu, et al. 2000] [Ferraiolo, et al. 2001]. The described components are explained below.

Core RBAC

RBAC is designed to simplify security administration by introducing the "role" abstraction between principals (subjects) and privileges (objects) [Sandhu, et al. 2000] [Eyers, et al. 2005].

Core RBAC recognizes five administrative elements: Users (USERS), Roles (ROLES) and Permissions (PRMS), where permissions are composed of Operations (OPS) applied to Objects (OBS) and five relations, which are the User-Assignment (UA), the Permission-Assignment PA, the User-Session (U-S), the Session-Role (S-R), and the set of Permissions (PRMS). The most basic of these relations are UA and PA. Permissions are associated with roles, and users are made members of roles, thereby acquiring the roles' permissions (see Figure 1.1).

Figure 1.1: Elements and their relations in the Core RBAC model.

This arrangement provides flexibility and granularity of assignment of permissions to roles and users to roles.

The collection of permissions assigned to a role confers the potential to perform duties, tasks, functions, or any other abstraction of a work-related activity. Assigning a user to a role gives the user the ability to perform these activities.

- $UA \subseteq USERS \times ROLES$, a many-to-many mapping between users and roles (user-to-role assignment relation).
- Assigned_users: $(r{:}ROLES) \rightarrow 2^{USERS}$, the mapping of role r onto a set of users
- $PRMS = 2^{(OPS \times OBS)}$, the set of permissions

- *PA* ⊆ *PRMS X ROLES*, a many-to-many mapping between permissions and roles (role-permissions assignment relation)
- assigned_permissions *(r:ROLES)* → 2^{PRMS}, the mapping of role r onto a set of permissions.
- SESSIONS= set of sessions
- session_users *(s: SESSIONS)* → *USERS* is a mapping of a session s onto the corresponding users.
- session_roles *(s: SESSIONS)* → 2^{ROLES} is a mapping of a session onto a set of roles.

Within the authorization process the function ***CheckAccess*** takes the current session, the requested operation, and the object that is the target of operation as inputs. It then checks if there is a role *r* mapped to the current session, such that *r* has been allocated the permission to perform the operation *op* on the object *obj*. If such a role exists, a TRUE (GRANT) value is returned as the access decision if not, a FALSE (DENY) value will be returned. According to the RBAC standard this can be formalized in [Gansen, et al. 2007]:

$$CheckAccess(s,op,obj) = \exists r \in ROLES,\ r \in S\text{-}R(U\text{-}S(s)) \wedge ((op,obj) \in PRMS \wedge (r, (op,obj)) \in PA)$$

The steps to access a resource by a user with the Core RBAC standard are [Ferreira, et al. 2009] (see Figure 1.2):

1. The user sends an *access application resource* request to the application;
2. The application contacts the Authn Service (Authentication Service) to authenticate the user;
3. The Authn 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.

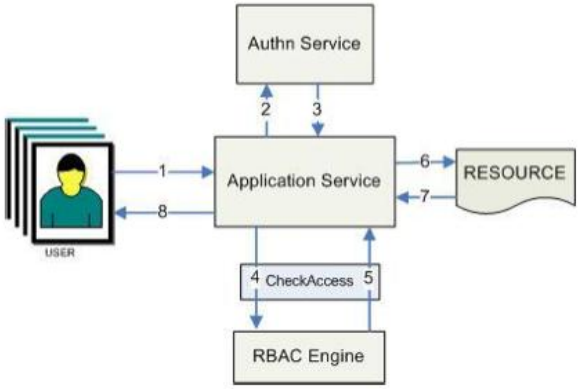

Figure 1.2: Core RBAC interactions diagram [Ferreira 2010].

Figure 1.3 describes users-roles and role-privilege associations. Tom and John are loan officers so they can write loan data, read accounts and execute transactions A, B and C.

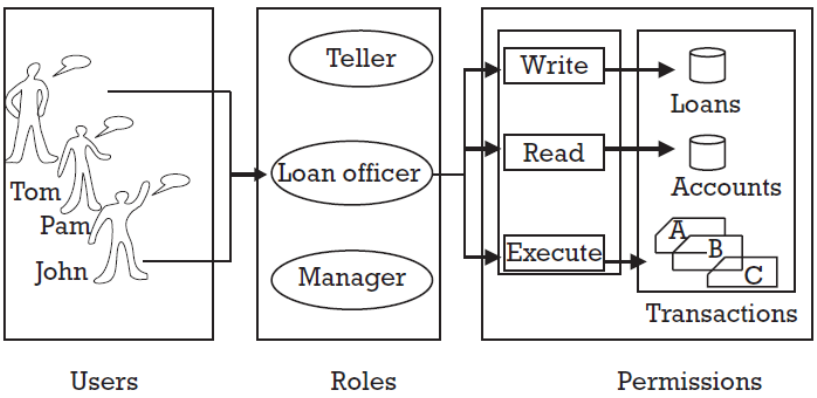

Figure 1.3: User, role and permission relationship

Hierarchical RBAC

Role hierarchies are a natural means for structuring roles to reflect an organization´s line of authority and responsibility. A hierarchy is mathematically

a partial order defining a seniority relation between roles, whereby senior roles acquire the permissions of their juniors, and junior roles acquire the user membership of their seniors.

Role inheritance relation are a third kind of authorization in addition to user-role and role-permission authorizations described in Core RBAC [Ferraiolo, et al. 2007]. If a role A inherits role B, it means that all of B's permissions are available via role A. In the example shown in Figure 1.4 the roles cardiologist and oncologist inherit the roles physician and resident. Any user that is assigned to the role cardiologist is authorized for the permissions that are assigned to the role cardiologist and authorized for the permissions that are assigned to the roles physician and resident.

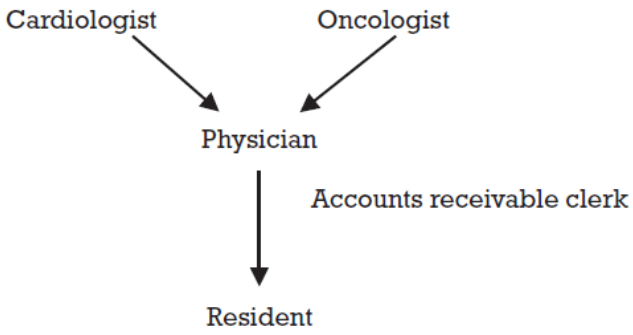

Figure 1.4: Role hierarchy, an example [Ferraiolo, et al. 2007]

RBAC recognizes two types of role hierarchies:

General Hierarchical RBAC - In this case, there is support for an arbitrary partial order to serve as the role hierarchy, to include the concept of multiple inheritances of permissions and user membership among roles.

Limited (Restricted) Hierarchical RBAC – Some systems may impose restrictions on the role hierarchy. Most commonly, hierarchies are limited to simple structures such as trees or inverted trees.

Constrained RBAC – Separation of Duties

Constrained RBAC adds a requirement for enforcing Separation of Duties (SoD). SoD is a fundamental principle in security systems, both automated and manual. Although there are many variations, SoD is fundamentally a requirement that critical operations are divided among two or more people, so

that no single individual can compromise security [Ferraiolo, et al. 2007]. The purpose of this principle is to discourage fraud by spreading the responsibility and authority for an action or task over multiple people. Although SoD is easy to understand, it is hard to express this principle in computer security systems [Simon and Zurko 1997].

A comprehensive survey by Simon and Zurko [Simon and Zurko 1997] found two large categories of SoD methods: static and dynamic. A simple way to distinguish between these two forms is to consider the time at which the role constraints are applied. Static SoD places constraints on roles at the time users are authorized for roles, on the other hand in dynamic SoD, constraints are invoked when users are actively using the system.

Static Separation of duties (SSD) – Is the simplest variation of Separation of Duty, that is, to enforce constraints on the assignment of users to roles. The **SSD** defined in this model are limited to those relations that place restrictions on sets of roles and in particular on their ability to form UA relations. This means that if a user is assigned to one role, the user is prohibited from being a member of a second role. An SSD policy can be centrally specified and then uniformly imposed on specific roles.

Though it has the advantage of simplicity, SSD does not reflect the actual functioning of human organizations. Users often have legitimate reasons for wanting or needing to act in two different roles, and careful construction of a security policy can ensure that these "violations" are secure.

Dynamic Separation of duties (DSD) – Static Separation of Duties relations reduce the number of potential permissions that can be made available to a user by placing constraints on the users that can be assigned to a set of roles. DSD relations, like SSD relations are intended to limit the permissions that are available to a user. However, DSD relations differ from SSD relations by the context in which these limitations are imposed, in other words, only if there are some users who are able to activate two different roles (in two different sessions).

Depending on an organization's security needs and resources, either static or dynamic rules may be appropriate.

Administration RBAC

In a large enterprise the number of roles can be in the hundreds or thousands; the number of users can be in the tens, hundreds of thousands, or in extreme circumstances over a million; and the number of objects can easily exceed a

million [Sejong and Ravi 2002]. Managing these roles, users, and their interrelationships is a difficult task that is often highly centralized in a small team of security administrators. One way to administer RBAC is the deployment of RBAC, this replaces the very difficult and intractable problem of managing authorization data, scattered over numerous platforms and administrative domains, with a less difficult but significant problem of managing roles. Role administration can be considered to be just another application of RBAC [Ferraiolo, et al. 2007].

Figure 1.5 illustrates the model RBAC with administration RBAC. The top half shows users, roles, and permissions that control or protect access to data and resources; the bottom half shows administrative roles and permissions. A role administrator performs the role management functions through the execution of administrative permissions (administrative operations on RBAC elements and relations).

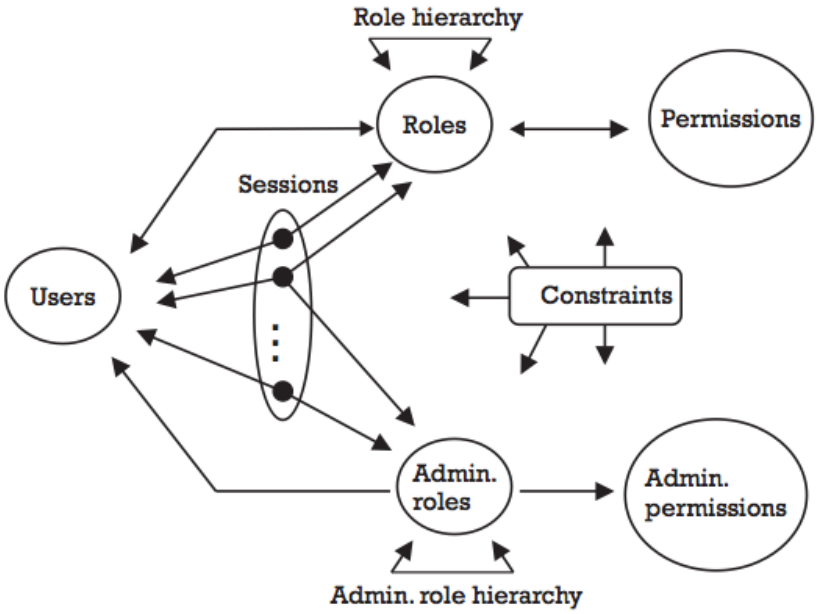

Figure 1.5: Summary of RBAC model [Ferraiolo, et al. 2007] [Sejong and Ravi 2002] [Ravi, et al. 1999].

1.2 Research question

Current research on access control aims to bridge the lack of research in this area. Because if, on one hand, legislation empowers the patient to be responsible and be active in protecting, controlling and managing his/her medical records, on the other hand, there are also studies that prove the benefits of the patient involvement on their own EHR [Ross and Lin 2003] [Hassol, et al. 2004] [Ferreira, et al. 2007] [Honeyman, et al. 2005].

Motived by this fact, this MSc project focuses research on extended RBAC models and standards that comply with legislation requirements and procedures regarding patients accessing their EHR. It is essential to have an access control model that gives the patients the needed empowerment and control owner their health. Patients must be able to easily define who can access what regarding their medical records and customize the access control model whenever needed.

The main research questions that this study proposes to answer are:

1) Do existing access control standards and RBAC based models comply with legislation requirements regarding patients' access to their EHR?
2) What are the necessary characteristics that a patient authorization model based on RBAC should integrate in order to be used and customized by the patient himself/herself?
    a. Who and in what situations can healthcare professionals and other types of users access a patient medical record?
    b. How will the patient define and manage this model?

1.3 Objectives

For the research questions that were formulated in the previous section, two main objectives were defined:

1) To analyze if existing access control models and standards allow patients' to access their EHR, as well as, define what healthcare providers can access which resources within their EHR, allowing this way for patients to customize access control rules and take full responsibility and control over their healthcare.

2) To define and propose a patient authorization model to be used and customized by the patient. The model is based on RBAC and the patient can define whom and in what situations an authorized healthcare professional can access his/her medical record.

2. Customizable access control models for patients: a systematic review

"Research is to see what everybody else has seen, and to think what nobody else has thought."

Albert Szent-Gyorgyi

2.1 Introduction

Access control is essential to provide for the confidentiality of EHR and the RBAC model is the most commonly used access control model in healthcare. Many authors focused their research in extending the RBAC model according to some needed characteristics. For example, the Attribute-Based Access Control (ABAC) [Shen and Hong 2006], bases the authorization in attributes and the Task-Based Access Control model (TBAC) [Thomas and Sandhu 1997] integrate temporal or inter-task constraints in RBAC.

However there are also some international standards that define guidelines for access control in healthcare. The International Organization for Standardization (ISO) has an area dedicated to health informatics, the ISO/TC 215, that intends to promote interoperability between independent systems, to enable compatibility and consistency for health information and data [ISO/TC 215 2001].

So, the goal of this chapter is to research if the existing standards and RBAC based extension models comply with healthcare legislation for protection of medical data and procedures regarding patients' accessing their EHR. Furthermore, this study also aims to verify if existing models and standards provide for patients' definition of what healthcare professionals can access within their medical records, allowing this way for patients to customize access control rules or, in other words, if these models and standards allow patients to customize their EHR.

2.2 Methods

The literature review was performed in June 28, 2011 with searches in Pubmed, IEEE Xplore, ISI Web of Knowledge and International Organization for Standardization.

The queries applied were:

- *"RBAC [All Fields] AND ("Health"[MeSH Terms] OR "Health"[All Fields]) AND Model [All Fields]"* in Pubmed;
- *"RBAC Health Model<in>metadata"* in IEEE Xplore;
- *"Topic (RBAC Health Model)"* in ISI Web of Knowledge;
- *"Health Access Control Model"* in ISO web site.

The results from these queries were filtered according to the following inclusion criteria:

- Language of the article (English);
- Review of title and abstracts (adequate context).

The review was done in several stages. Initially, the repeated articles in the various databases were identified, they were then reviewed according to the inclusion criteria and finally read and analyzed.

For each article/standard, three relevant characteristics were analyzed:

(a) If they referred to EHR;

(b) If they included within their access control policies the possibility for patients to also access their EHR;

(c) If there was the capability for the patient himself/herself to customize that model and define his/her own access control rules, regarding their EHR.

After the analysis of the found articles/standards, their citations were also reviewed and those that suited the inclusion criteria were also integrated in the review.

The search for full text articles was performed in the following databases:

- Google Scholar,
- Open Repository of University of Porto,
- Open Access Repository Scientific Portugal.

Figure 2.1 presents the review process including the results that were obtained in each stage. A total of 22 articles and standards were obtained from the search queries. From these, 4 articles were excluded because they were repeated. All remaining 18 articles and standards were written in English and were all available as full text. However, after the analysis of titles and abstracts, 10 articles/standards were not fit to be included within the review. After analysis of the articles/standards that are cited by those found within the search, 4 articles/standards were included, so a total of 12 articles/standards were included in the final review.

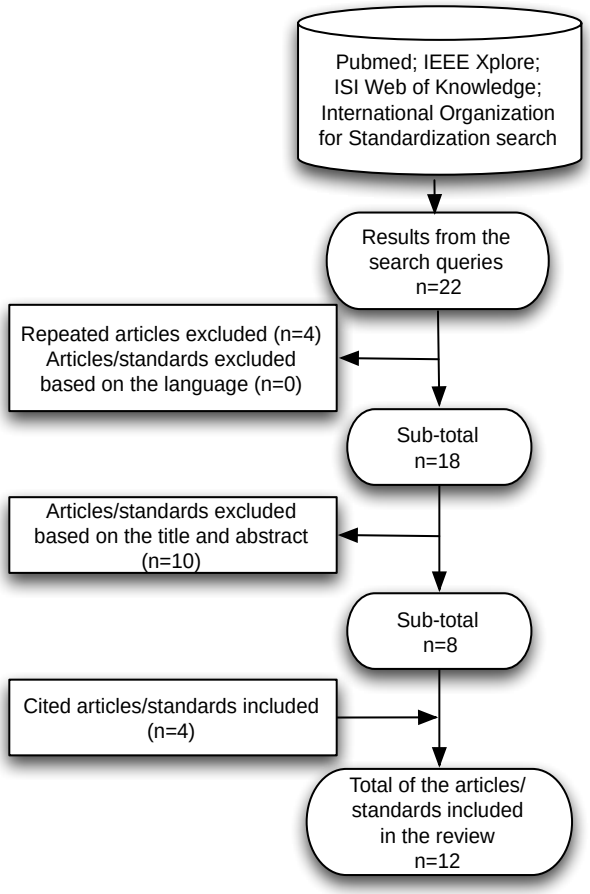

Figure 2.1: Flowchart representing the review process and subsequent results.

2.3 Results

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

Table 2.1 presents in more detail the results of the analysis of the 12 articles/standards that were included in the review. The results are divided between articles and standards found in the queries and articles and standards found within the citations of included articles and standards. "X" means the

existence while "—" means the inexistence of each characteristic. The results of a more detailed analysis of each article and standard are describe in the following paragraphs.

The model of **Abou El Kalam** et al. focuses mainly on the relation between clinician and patient and the involvement of the clinician, at the moment of the process of care [Abou El Kalam and Deswarte 2003]. However, the article does not describe the types of roles, which the model integrates. It just alerts for the need of patients' consent to access their most sensitive healthcare information.

J. Reid et al. present a model based on RBAC which defines a new characteristic where a set of privileges held by a role can be allowed or denied to other roles without using traditional RBAC constraints, such as separation of duties [Reid, et al. 2003]. This model introduces a very generic role hierarchy where the role *care team* is included without referring to a role for the patient.

Motta and Furuie define a model that regulates user access to medical records based on organizational roles [Motta and Furuie 2003]. They suggest defining a role hierarchy with inheritance of authorizations and modeling the types of data found in an EHR according to its clinical contents (e.g. demographics, prescriptions). They also propose a technique for handling conflicts between authorizations. The authors also refer the possibility of including the role *patient* so that users can see their own data and have also the possibility of determining the level of security access for each data element of their record. The authors cite the schema of access control defined by Schoenberg and Safran as an example to follow [Schoenberg and Safran 2000].

In the Organization Based Access Control (**ORBAC**) model the specification of the security policy is parameterized by the organization, for instance, a private clinic or a department of an Hospital [El Kalam, et al. 2003]. The authors refer four types of views for the Electronic Health Record: (1) administrative_record, (2) medical_record, (3) surgical_record and (4) patient_record. The last view concerns the whole EHR and integrates the previous three. There is not, however, a specification of who can access the patient record view and if the patient himself/herself would be able to access and define access permissions to his/her record.

Table 2.1: Summary of results of the literature review.

	Models and Standards	*References*	*EHR application*	*Patient Access*	*Patient Customization*
Articles/ standards found within the queries	"Security model for health care computing and communication systems"	[Abou El Kalam and Deswarte 2003]	X	—	—
	"A novel use of RBAC to protect privacy in distributed health care information systems"	[Reid, et al. 2003]	X	—	—
	Contextual Role-Based Access Control	[Motta and Furuie 2003, Motta and Furuie 2004]	X	X	X
	Organization Based Access Control (ORBAC)	[El Kalam, et al. 2003]	X	—	—
	Privilege Management and Access Control (ISO/TS 22600)	[ISO/TS 22600-2 2006, Blobel, et al. 2006]	X	X	—
	RBAC with privacy based extensions	[Patrick 2007]	X	X	—
	Situation Based Access Control (SitBAC)	[Beimel and Peleg 2009]	X	—	—
	Break-the-Glass Role Based Access Control (BTG-RBAC)	[Ferreira, et al. 2010]	X	—	—
Cited articles/standards	Open Architecture for Security Interworking Services (OASIS)	[Yao, et al. 2001]	X	—	—
	Contextual Team Based Access Control (C-TMAC)	[Georgiadis, et al. 2001]	X	—	—
	Generalized Temporal Role Based Access Control (GTRBAC)	[Joshi, et al. 2002, Joshi, et al. 2003]	X	—	—
	Electronic health record communication-Security (ISO/TS 13606)	[ISO/TS-13606 2009]	X	X	X

The Privilege Management and Access Control (PMAC) is included in the standard **ISO/TS 22600 part 2** [ISO/TS 22600-2 2006]. PMAC refers RBAC as the reference access control model to follow. This standard also refers that administration constraints may need to be enforced, for example, by using *separation of duties,* but does not define how and what other procedures must be included and applied besides these constraints to still guarantee EHR confidentiality. The annex A of this same standard presents a set of *functional roles*, which include the *subject of care* (normally the patient) and *subject of care agent* (parent or guardian), to manage the creation, access, processing and communication of healthcare information. It is not clearly defined within the standard who delegates access control permissions to the functional roles, which record components a role can access nor if the patient can take part in the delegation process.

Patrick et al. propose a RBAC model with privacy-based extension, amidst others challenges, the most pressing privacy concerns that have observed for e-Health care informatics include: (1) acquisition, storage, and processing of e-Health data; (2) consent to process and disclose e-Health data; (3) rights of the data subject (typically the patient) to access and rectify his/her own health dataset [Patrick 2007]. So the authors propose to include in their model the role *e-patient* in order to comply with the medical data protection legislation. This role has the right to access and correct his EHR. However, the authors do not specify which privileges are associated with this role and by whom and how the access control rules can be customized.

Beimel et al. introduce the Situation Based Access Control (**SitBAC**) model which was designed for expressing scenarios of patient data access request as a basis to preserve the patient's privacy [Beimel and Peleg 2009]. The strengths of SitBAC are in its ability to structurally specify scenarios of patient's data access via situation models, they represent a situation where the data-requestor definition is partial (e.g. the role is missing), and represent scenarios where the data-requestor and the required data do not belong to the same organization. However this model does not mention any types of roles nor the patient as another user that can access the medical record.

The Break-the-Glass Role Based Access Control (**BTG-RBAC**) model includes *Break The Glass* permission/action within the RBAC engine [Ferreira, et al. 2010]. This can be used to *break* or override the access control rules in a controlled manner, in other words*, Break the Glass* is needed when normal access controls to processes are insufficient and access control policies for

emergency situations are required. This model extends the Core RBAC model with obligations [Gansen, et al. 2007] and defines generically when a role can have permissions to BTG on specific resources. Patient roles are never mentioned.

The Open Architecture for Security Interworking Services (**OASIS**) model adds concepts such as *Appointment, Prerequisite roles* and *Constraints* to the RBAC model [Yao, et al. 2001]. Only when the role activation rule is satisfied then a role is activated. *Appointment* certificates may be issued in many different circumstances and those are specific to each application. An example is that a hospital administrator does not need to be medically qualified yet may issue a credential which indicates that a user is employed as a doctor. This is a case of an *administrative role*. This model does not allow hierarchic roles or role inheritance because the authors argue that hierarchies are not possible to execute in distributed environments. Although this model is very detailed in describing roles, it does not specify the types of roles that can be used.

The Contextual Team Based Access Control (**C-TMAC**) model integrates the concepts of *team* and *contexts* into RBAC [Georgiadis, et al. 2001]. Teams are associated with contexts and users are members of those teams. Examples show the association of permissions to a set of roles (*doctor*, *head nurse* and *nurse*) in a specific context. None of these examples describe the role patient. As OASIS, the C-TMAC model does not define hierarchic roles.

Joshi et al. added *Temporal Constraints* to the RBAC model with the extension Generalized Temporal Role Based Access Control (**GTRBAC**) [Joshi, et al. 2002]. GTRBAC makes a clear distinction between *role enabling* and *role activation*. This model includes hierarchic roles, inheritance, separation of duties and time constraints. The model does not specify the types of roles and permissions that can be applied.

The standard **ISO/TS 13606** came to improve some of the ISO/TS 22600 limitations [ISO/TS-13606 2009]. It describes the privilege methodology to be used in order to specify the access control to an EHR. In part 4, *data sensitivity levels* for each *record component* are defined and the *functional roles* are mapped to each one of those components regarding the defined privileges and permissions. This standard explores the idea of patient empowerment, where the patient has access to his/her EHR and can customize access to its components by delegating permissions to each functional role. Moreover, this standard presents a set of access control archetypes for the EHR structure.

Annex A of this standard describes some use-case healthcare scenarios that exemplify the use of functional roles and which parts of the EHR record

can be accessed by those roles. Figure 2.2 shows an example of one healthcare scenario presented in the standard. The purpose of this example is to show how a generic EHR policy can be defined. It should be noted that this policy is itself an evidence that *Joanna Jones* (patient) has something to hide, and can restrict access so that her *guardian* (Joanna's mother) does not know of its existence.

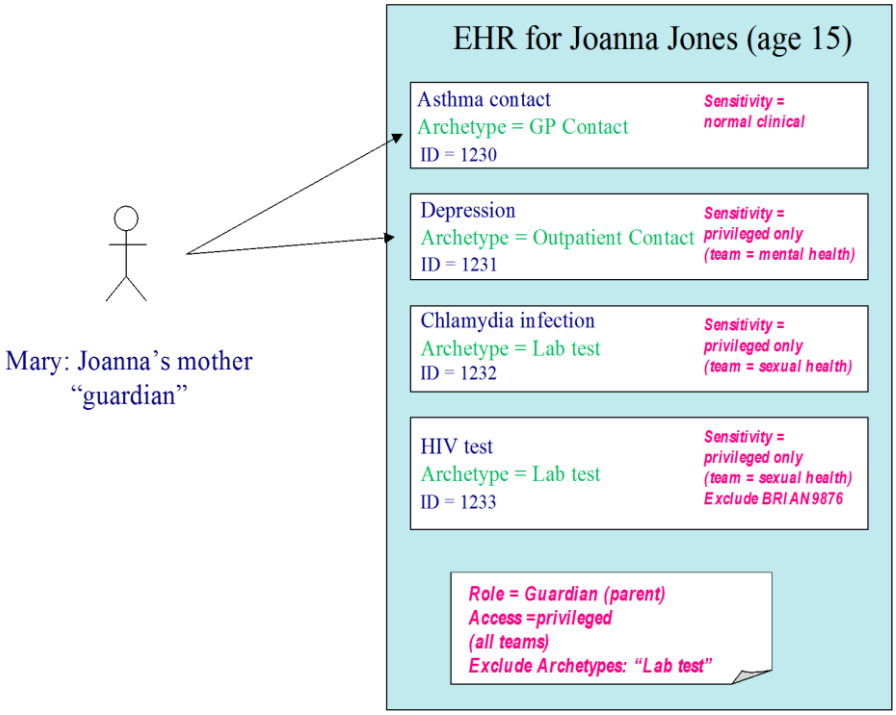

Figure 2.2: Illustrative access control example [ISO/TS 13606-4 2009].

2.4 Discussion

Results of the systematic review show that several authors dedicate their research to the definition and improvement of access control models, which are based on RBAC and within the healthcare domain, specifically to access EHR.

In summary, only the model of Motta and Furuie [Motta and Furuie 2003] and the model of Patrick et al. [Patrick 2007] together with the two ISO standards presented include the patient as one more role to access the EHR. In addition, the ISO/TS 13606-4 standard and the model of Motta and Furuie [Motta and Furuie 2003] introduce also, in a generic way, the capability of the patients to customize access control rules to their EHR.

For a better understanding of the differences between the models selected for review it was performed a behavior test of the models and the ISO-22600-2 standard in the context of the use-case presented in Figure 2.2. Limitations are also discussed for the ISO/TS 13606-4 standard for the same use case example:

• The models proposed by Motta and Furuie [Motta and Furuie 2003]and Patrick et al. [Patrick 2007] are not possible to apply to this use-case, because the authors do not define: the possibility of the *subject of care agent* to access the *subject of care* EHR; data sensitivity levels for each record component; and who (or what role) has access to each record component.

• The ISO/TS 22600-2 standard [ISO/TS 22600-2 2006] provides a set of functional roles that include *subject of care* and *subject of care agent* however, as in the previous models, it does not include the definition of the data sensitivity levels, types of record components and association between functional roles and record components. For these reasons it is not possible to apply this standard to the use-case.

• In the use-case presented in the ISO/TS 13606-4 standard [ISO/TS 13606-4 2009] (Figure 2.2) Joanna's mother does not have access to two types of record components (Chlamydia infection and HIV test). This standard does not foresee emergencies situations where the access to this data would be indispensable. It also does not foresee where and at what time a functional role can access a patient's EHR. Usually this access would not be made outside the workplace and past the shift hours.

Despite the limitations previously described, as was mentioned before, this standard defines clearly, with multiple examples (tables and use-cases), the associations between functional roles and record components as well as record component sensitivity. However, due to it being a standard, the definition of

functional role is appropriately generic but, in the case of health providers, it is difficult to define which HCP (users) are assigned to which functional roles. The health institution where the providers work manages this assignment. This standard does not define constraints in the attribution of different functional roles to the same user in the same session (e.g. dynamic separation of duties). It also does not define either functional role hierarchy or functional role inheritance and how the patient will be able to customize the model with the restrictions that he/she wants to apply.

Nevertheless, with all these characteristics, the standard ISO/TS 13606-4 is the most complete standard in terms of our research goals.

In conclusion, in spite of generically allowing the patients to customize the access control rules to their medical records, the models and standard discussed are too generic to be applied directly to specific healthcare scenarios where customization is required. None of the analyzed research studies describe how the patient can customize his/her EHR in more specific scenarios.

There is, therefore, a lack of research within this area. Because if on one hand legislation empowers the patient to be responsible and active in protecting, controlling and managing his/her medical records, on the other hand, there are no specific guidelines that can provide for this.

Although the models/standards presented in this chapter do not comply with the goals of this research, they provide security mechanisms that could integrate a new extension of the RBAC model (e.g. Break the Glass features and Temporal Constraints). This new model extension could explore these security mechanisms as well as the definitions proposed by the ISO/TS 13606-4 standard.

3. Model definition

"Logic will get you from A to B. Imagination will take you everywhere."
Albert Einstein

3.1 Introduction

According to the results of the previous chapter, this chapter describes the characteristics from the various presented access control models and standards that can be included within the definition of a new patient authorization RBAC based model. The results of the systematic review showed that the standard ISO 13606 part 4 clearly presents with multiples examples a set of functional roles and record components as well as record component sensitivities which could integrate the new patient authorization RBAC model.

Besides this standard other security mechanisms could integrate the new model, such as BTG and temporal constraints presented in the models BTG-RBAC and GTRBAC respectively, as well as security mechanisms of the RBAC model itself (e.g. separation of duties constraints).

3.2 ISO 13606-4

The ISO 13606 describes the privilege methodology to be used in order to specify the access control to an EHR. The part 4 of this standard [ISO/TS 13606-4 2009] expresses also the **record components** that an EHR may integrate such as: Personal Care; Privileged Care; Clinical Care; Clinical Management and Care Management (see description in Table 3.1).

This standard also describes a set of **functional roles** (Subject of Care; Subject of Care Agent; Personal Healthcare Professional; Privilege Healthcare Professional; Healthcare Professional; Health-related Professional and Administrator) and which role can access what record components. The functional role administrator refers to the team of administrative personnel that can access the EHR. However, so that this role is not confused with the role, which manages the access control model, the administrative team will be associated with the *administrative* functional role and the access control model managers will be associated with the *administrator* functional role.

Table 3.2 shows the list of functional roles.

Table 3.1: Sensitivity values and levels defined for each Record_Component [ISO/TS 13606-4 2009].

SENSITIVITY value	Sensitivity level	Description of intended access to RECORD_COMPONENTs of this sensitivity
Personal care	5	to be shared by the subject of care perhaps with only one or two other people whom they trust most, or only accessible to the subject of care (and to others by one-off authorizations)
Privileged care	4	access restricted to a small group of people caring intimately for the patient, perhaps an immediate care team or senior clinical party (the privileged clinical setting needs to be specified e.g. mental health)
Clinical care	3	default for normal clinical care access (i.e. most clinical staff directly caring for the patient should be able to access nearly all of the EHR)
Clinical management	2	less sensitive RECORD_COMPONENTs, that might need to be accessed by a wider range of personnel not all of whom are actively caring for the patient (e.g. radiology staff)
Care management	1	RECORD_COMPONENTs that might need to be accessed by a wide range of administrative staff to manage the subject of care's access to health services

Table 3.2: List of Functional Roles [ISO/TS 13606-4 2009].

Functional Role	Brief description
Subject of care	principal data subject of the electronic health record
Subject of care agent	e.g. parent, guardian, carer, or other legal representative
Personal healthcare professional	healthcare professional or professionals with the closest relationship to the patient, often the patient's GP
Privileged healthcare professional	nominated by the subject of care OR nominated by the healthcare facility of care (if there is a nomination by regulation, practice, etc. such as an emergency over-ride)
Healthcare professional	party involved in providing direct care to the patient
Health-related professional	party indirectly involved in patient care, teaching, research, etc.)
Administrator	any other parties supporting service provision to the patient

3.3 RBAC model

The Role Based Access Control model (Sandhu et al., 2000) integrates the Core RBAC, Hierarchical RBAC, and Constrained RBAC, which includes Separation of Duties (SoD) as verified in section 1.1.4 (NIST RBAC).

Chapter 2 presented five administrative elements of the **Core RBAC**: Users (U), Roles (ROLES) and Permissions (PRMS), where permissions are composed of Operations (OPS) applied to Objects (OBS). In the new model, ROLES with similar authorization are organized in Functional Roles. The possible OPS will be create, read, update and delete (CRUD) [Baxter, et al. 2007], that can be divided into more specific operations depending on the needs. The OBS will be the record components presented by ISO/IEC 13606-4.

According to the definitions of **Hierarchical RBAC**, were defined three hierarchical trees. In the new proposed model, the functional roles described in were organized into three main groups: subject of care (Group I), healthcare professionals (Group II) and administrative access (Group III) (see Figure 3.1). Each group incorporates both role inheritance and permission inheritance.

In Group I there are two important roles, the subject of care agent direct and the subject of care agent indirect. The former relates to users that have a close familiar relation (e.g. Patient' father, Patient' son, Patient' husband) with the patient and the latter related to more distant relations, which can also have interest in some parts of the patient's healthcare but have less permissions of access (e.g. patient' cousin, patient' grandfather).

Group III includes the senior (with more permissions) and junior administrative roles.

Another important concept to include in the new model is the **SoD** concept. In SSD if a user is assigned to one role, the user is prohibited from being a member of a second role [Ferraiolo, et al. 2007]. SSD will integrate the new patient authorization model because the user will only be able to use one exclusive role per session in order to avoid conflicts between functional roles.

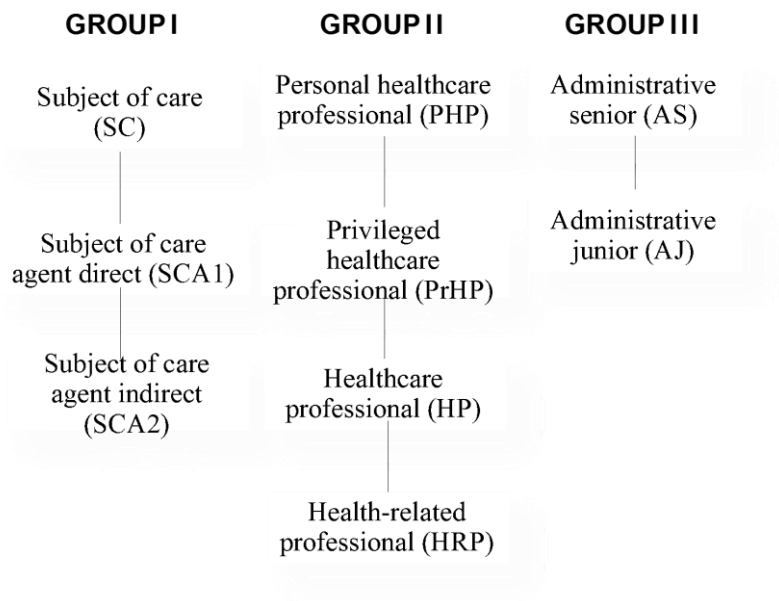

Figure 3.1: Hierarchical functional roles divided into three groups.

When the system needs to reach an access decision it should use a table similar to Table 3.3. This table defines the basis for how sensitivity levels and functional roles can be mapped. For a specific functional role the information requester may have, access permissions that are associated accordingly. The set of functional roles presented in Table 3.3 are divided into three hierarchical groups according to Figure 3.1

Table 3.3: Mapping of functional roles in record_component sensivity. Adapted from [ISO/TS 13606-4 2009].

		RECORD_COMPONENT sensitivity				
	Functional Role	**Care management**	**Clinical management**	**Clinical care**	**Privileged care**	**Personal care**
Group I	Subject of care	Y	Y	Y	Y	Y
	Subject of care agent	Y	Y	Y	Y	Y
Group II	Personal healthcare professional	Y	Y	Y	Y	Y
	Privileged healthcare professional	Y	Y	Y	Y+	++
	Healthcare professional	Y	Y	Y		
	Health-related professional	Y	Y			
Group III	Administrative	Y				

NOTE 1 Y indicates that access will be granted to RECORD_COMPONENTs of this sensitivity unless otherwise dictated by other policy constraints, as specified according to clause 7 of this part standard.
NOTE 2 + Indicates that access will be granted if the EHR Recipient is a member of the same speciality or clinical service as that in which the RECORD_COMPONENT was created e.g. sexual health clinic, prison health service (as specified in the service_setting attribute for the composer of the COMPOSITION in the Reference Model of Part 1). This access may also be granted in health care 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, such as in the armed forces of some countries.

Several existing approaches to **RBAC Administration** use role hierarchies to specify administration domain, e.g. of administrators roles are senior-most role (Director) and junior-most role (Employee). These role hierarchies are similar to the previous described hierarchies [Sejong and Ravi 2002].

In the proposed model, the role of administrator (administrator senior) of the roles and permissions of an EHR is associated with the patient of that EHR. The patient will actively manage the roles and permissions as well as give permissions of administration to other roles, if necessary. Other users may be part of the administrator's role hierarchy (see Figure 3.2). So the patient can define that some users may also accumulate functions of model administrators (administrator junior). The administration permissions of the role administrator junior will be more restrictive than the senior.

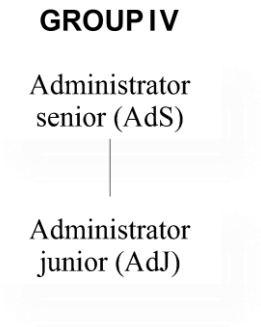

Figure 3.2: Administrator hierarchy roles.

In RBAC, senior role inherits junior's role permissions by virtue of the role hierarchy. But, junior role is not allowed to carry out the permission, which is only granted to the senior or other role groups. When a senior role fails to operate, junior roles may not continue to perform their jobs when they need the senior role permissions [SangYeob and SuhHyun 2000]. In this case RBAC provides **Role Delegation,** which is a mechanism of assigning access rights to a user. Delegation may occur in two forms: administrative delegation and user delegation [Crampton and Khambhammettu 2008]. An administrative delegation allows an administrator to assign access rights to a user and does not, necessarily, require that the administrator possesses the ability to use these access rights. On the other hand, a user delegation allows a user to assign a subset of his available rights to another user [Ferraiolo, et al. 2007]. User delegation is usually a short-lived operation [Crampton and Khambhammettu 2008]. User delegation in the proposed authorization model will be an important mechanism to activate specially in situations when an HCP would need, for instance, a second opinion from a colleague that has no permissions to access the required her. In this situation, delegation of permissions can be a good temporary solution.

Moreover, in emergency or unanticipated situations, the role administrator can choose which record components a user may not know of its existence or may know but needs to perform BTG in order to access it. More on this is explained next.

EHR access control rules administration can be a difficult task and patients must also be vigilant about users' activity in their EHR. Although they can assume that users can be trusted to exercise discretion in how they use

resources, patients cannot simply neglect the possibilities of security breaches [Longhua, et al. 2002]. Extensive **auditing** is important to ensure traceability of user actions. The proposed patient authorization model should allow patients to access users' audit logs. So the patient, as an administrator of the roles can track who does what within his/her health information. For example, access to record components should be registered together with the user's name, role, as well as date and time; all delegation and revocation actions should be saved on the audit trail.

This is very important in delegation attributions but also for the role administrator and in what time periods. Roles and users with more permissions should be closed monitored. The key challenge is to make the audit logs accessible and understandable to the patient. Ideally, these audit logs should be ordered with the most accessed records by what roles and users and what days and times this was performed. This process can be similar to what is used in social networks nowadays, when users can visualize who accessed their profile more often [Gutierrez, et al. 2009].

3.4 Break the Glass access

The Break the Glass (BTG) option can be used in order to break or override the access controls in a controlled manner. This should allow a user to override the access control rules stated by the access control manager and access what the user requests, even though he was not previously authorized to do it. When this is done, other BTG rules come into play which may monitor, record or report the user's actions, thus making him responsible and oblige him to justify what he/she did afterwards [Ferreira, et al. 2009].

Characteristics from the BTG-RBAC model are included within the proposed authorization model. This way, the BTG access will be activated whenever a user tries to access resources with a role that does not include the permissions to do it. When the BTG access is activated the HCP can access what was requested but is alerted for the fact that he/she does not have immediate access and that responsible parties (mostly the patients or someone defined by the patient) will be informed and can later ask for justification if the BTG is performed.

3.5 Temporal Constraints

The Generalized Temporal Role Based Access Control (GTRBAC) [Joshi, et al. 2002] model introduces a set of language constructs for the specification of temporal constraints on roles, including constraints permissions.

These constraints are also included within the new patient authorization model in order to restrict access to Groups II and III in terms of temporal duration, for instance, during the healthcare professionals' shift.

3.6 Discussion

The characteristics described in this chapter are important and should be integrated in the proposed patient authorization model. RBAC security features, temporal constraints and ISO 13606-4 information sensivity definitions will provide confidentiality and privacy to patient information and, on the other hand, break the glass mechanisms provide for availability of information in emergency situations.

All these characteristics will provide for a more secure and flexible to the proposed patient authorization model.

4. The proposed patient authorization model

"If information ends up in the wrong hands, the lives of people very often are immediately at risk."

Gijs de Vries

4.1 Introduction

After selecting the features that should be included within the patient authorization model proposed in this dissertation, this chapter describes the prerequisites, architecture and formal definition that are needed in order to use the model in real healthcare scenarios.

4.2 Prerequisites

4.2.1 Patient's Healthcare Network

The proposed patient authorization model is described within a Patient's Healthcare Network (PHN). The concept of PHN refers to all the healthcare institutions that the patient usually attends as well as health centers, referral hospitals, private hospitals, commercial laboratories and health insurers (see Figure 4.1). It is important to define the institutions where the patient attends consultations and treatments because only the professionals that work in these institutions should usually have access to that patient's EHR. All professionals outside that PHN are normally excluded from access to the EHR of the patient. However, the patient can define, within his/her model, a temporary role for HCP outside that PHN to access their EHR in a predefined period of time, preferably in their presence.

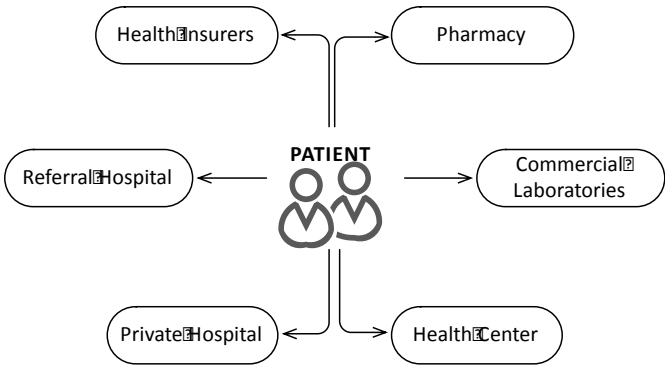

Figure 4.1: Patient's Healthcare Network.

In some situations, when the patient integrates an institution inside the PHN the providers of that institution may wish to share information with other providers (e.g. to get a second opinion) who do not belong to their PHN.

In this situation, if the role provider has delegation permissions he could attribute temporary access to a user outside the PHN to obtain a second opinion.

Figure 4.2 illustrates this case with an example. Jennifer is a patient that is being followed in Institution A (belongs to PHN), Jennifer has the role subject of care and manager senior in their own EHR. Dr. Jain is Jennifer's Gynecologist and has permissions to access Jennifer's EHR with the role

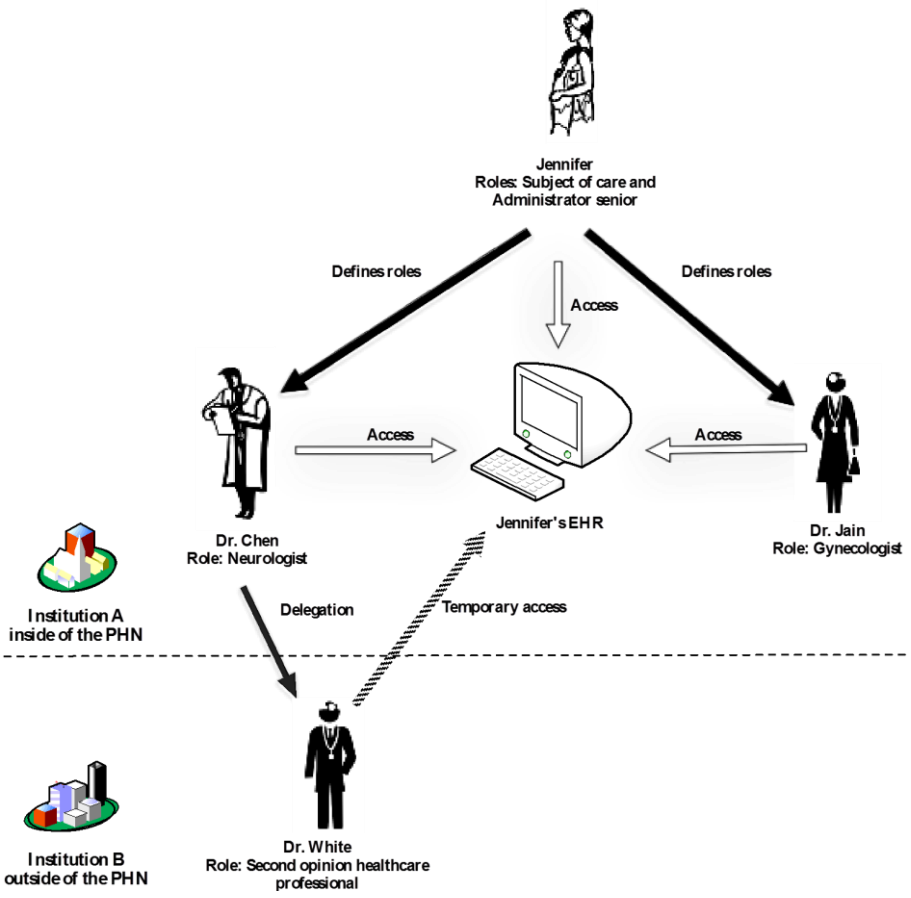

Figure 4.2: Example of a user delegation outside of the PHN performed by Dr. Chen to Dr. White.

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

4.2.2 Authentication

In the proposed model, for users to access the EHR and its components they need to provide three pieces of information: a login (for identification); a password (for authentication); and a role (for authorization). The first two are presented initially and only if authentication is successful will, a list of roles that was previously associated to that user, be available. The user can only select one role for each session. Each role has different permissions associated to different parts of EHR components, according to what the patient has previously defined within the model. Moreover, the model predicts beyond passwords (something the user know), the utilization of a two-factor authentication, with the use of smart cards or tokens (something the user has) whenever needed. The single-factor authentication can also be called password-based authentication, is widely used to verify the identity of users and faces many times fraudulent and theft problems [Shah, et al. 2009].

4.2.3 Access to record components

The access permissions of a role to a specific record component is going to depend on the mapping that was previously made by the administrator senior (usually the patient). A specific role will have access to a record component if the administrator would have defined any of the CRUD operations or BTG to be part of his/her access permissions. If a role has not defined any of those operations or BTG to a record component that role will not be able to access any record component and not even know of its existence (the record components will be invisible for that role).

4.2.4 Insertion of new record components

The patient, as administrator senior, needs to be informed about the consequences of access permissions/restrictions of certain medical information. The key is to keep the patient informed of exactly what is the sensitivity of the record components, so then he can make informed decisions. When the healthcare providers introduce new record components associated to a patient's EHR, they should define the sensitivity levels of those components according to ISO 13606-4 (see Table 3.2) in order for the patient to understand the sensitivity of that information, helping this way the patient to manage the permissions/restrictions of his model's roles.

4.3 The formal proposed patient authorization model and architecture

This section describes in more detail the formal definition of the proposed patient authorization model and presents a visual description of the model architecture. The features included within the proposed patient authorization model are detailed within Figure 4.3.

Figure 4.3 presents the architecture of the proposed patient authorization model as the integration of several other models as well as previously mentioned characteristics [Ravi, et al. 1999], [Sandhu, et al. 2000], [Joshi, et al. 2002], [Ferreira, et al. 2009], [ISO/TS 13606-4 2009]. The proposed model integrates both the specification of access and the definition by the patient of permissions to access his/her EHR. It puts the patient in the centre of these operations. Patient as an administrator senior can customize/manage the permissions of all the other users.

Defining now formally the new relations of the proposed model from the Core RBAC model that include [Ravi, et al. 1999], [Sandhu, et al. 2000], [Joshi, et al. 2002], [Ferreira, et al. 2009], [ISO/TS 13606-4 2009] features.

U, is a set of users; F_ROLES and A_ROLES, are disjoint set of functional roles and administrator roles; PA_BTG and APA, are disjoint sets of permissions and administrative permissions; S, is a set of sessions, OPS and OBS, are a set of operations and objects respectively.

- $UA \subseteq U \ X \ F\_ROLES$, a many-to-many mapping between users and functional roles (user-to-functional role assignment relation).

$AUA \subseteq U \ X \ A\_ROLES$, a many-to-many mapping between users and administrator roles (user-to-administrator role assignment relation).

- Assigned_users: $(r: F\_ROLES) \rightarrow 2^{USERS}$, the mapping of functional role r onto a set of users
Assigned_users: $(r: A\_ROLES) \rightarrow 2^{USERS}$, the mapping of administrator role r onto a set of users

- $OPRMS \subseteq OPRMS\_BTG$ and $OPRMS\_BTG \subseteq PRMS \ X \ BTGs \ X \ OBLGS$
$OPRMS\_BTG = OPRMS \ X \ 2^{(BTG)}$
$PA\_BTG \subseteq OPRMS\_BTG \ X \ F\_ROLES$
$APA \subseteq A\_PERMS \ X \ A\_ROLES$, permission to administrator roles assignment relation

- $RH \subseteq F\_ROLES \ X \ F\_ROLES$, partially ordered functional role hierarchy
$ARH \subseteq A\_ROLES \ X \ A\_ROLES$, partially ordered administrator role hierarchy (both hierarchies are written as ≥ in infixe notation)

- assigned_permissions $(r: ROLES) \rightarrow 2^{PRMS}$, the mapping of role r onto a set of permissions.

- SESSIONS= set of sessions
session_users $(s: SESSIONS) \rightarrow USERS$ is a mapping of a session s onto a single user.
session_functionalroles $(s: SESSIONS) \rightarrow 2^{F\_ROLES \ \cup \ A\_ROLES}$ is a mapping of a session s_i to a set roles $(s_i) \subseteq \{r \mid (\exists r' \geq r) \ [(user(s_i), r') \in UA \cup AUA]\}$ (which can change with time).
Session s_i has permissions $U_{r \in roles(si)} \{p \mid (\exists r'' \leq r) \ [(p,r'') \in PA\_BTG \cup APA \ ]\}$

- There is a collection of Temporal Constraints which values of the various components enumerated above are allowed or forbidden for a period of time.

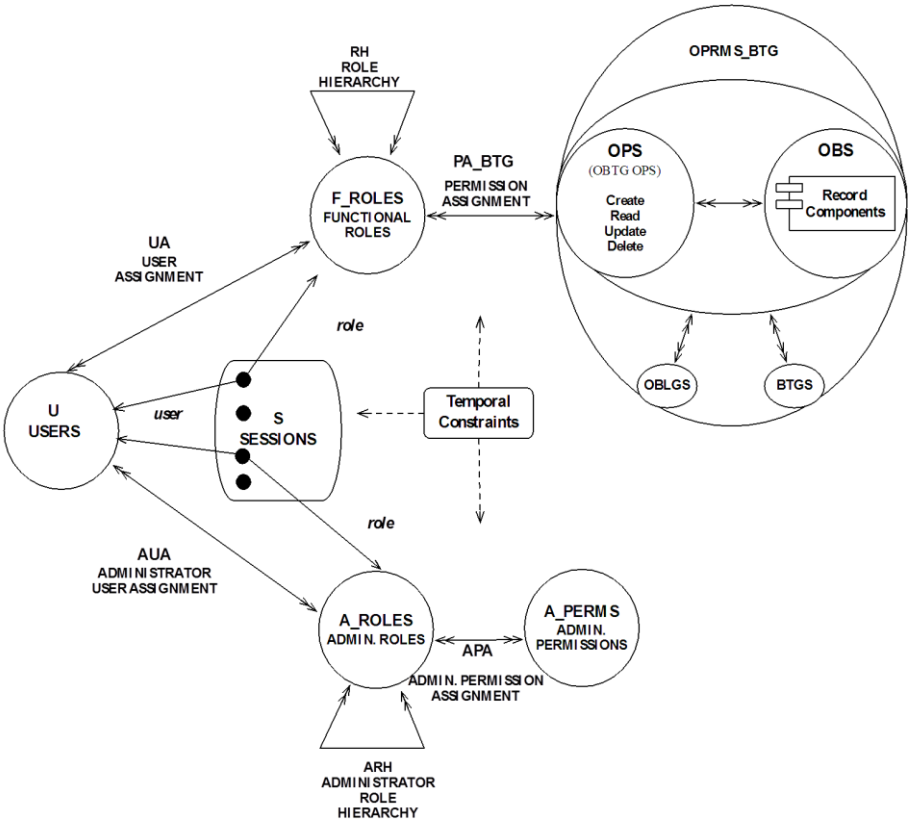

Figure 4.3: Architecture of the proposed patient authorization model based on [Ravi, et al. 1999], [Sandhu, et al. 2000], [Joshi, et al. 2002], [Ferreira, et al. 2009] and [ISO/TS 13606-4 2009].

The top half of the Figure 4.3 shows users, functional roles, and permissions (include BTG) that control operations (create, read, update and delete) in record components; the bottom half shows administrator roles and permissions. A role administrator performs their functions through the execution of administrator permissions (administrator operations on RBAC elements and relations). Both administrator roles and functional are organized into a role hierarchy. The schema also includes temporal constraints that allowed or forbidden actions for a period of time.

4.4 Discussion

This chapter presents the proposed patient authorization model that integrates BTG features, temporal constraints and ISO 13606-4 definitions within the NIST RBAC model in a secure, controlled and responsible way.

To access a patient's EHR the user should belong to the patient's PHN, however a user can also access the patient's EHR if there are any delegated permissions defined for him or in emergency situations activating the mechanism BTG.

There is however one fact that must be stressed. This model requires that a responsible party (include the patient) audits the reasons why BTG actions and user delegation actions were performed within the system.

For authentication it is proposed a two-factor authentication in order to improve EHR access security.

One way to help the patient to be informed of EHR component sensitivities the healthcare providers can initially introduce those levels each time they introduce a new record component, and the patient can decide to use them or not.

5. Patient authorization model - proof of concept

"Nothing in life is to be feared, it is only to be understood. Now is the time to understand more, so that we may fear less."

Marie Curie

5.1 Introduction

To better understand how the new model can work in real practice this chapter presents storyboard examples of how a patient defined and mapped access control permissions to three functional roles. The usage scenarios are: the patient corrects data in his EHR, the patient has the need of medical care while travelling, and the patient's son accesses his father's EHR.

5.2 Example of patient administration

Table 5.1 presents an example of how a patient, as an administrator senior, manages his/her EHR and defines access control rules for the three stated previously scenarios (storyboard 1, 2 and 3 described below). The roles patient (P), temporary privileged healthcare professional (TPrHP) and patient's son (PS) are presented in this table and those roles are associated with the functional roles: subject of care (SC), privileged healthcare professional (PrHP) and subject of care agent direct (SCA1). Respectively, several access operations and record components were also defined: BTG operation, knows the existence of the record component and temporal constraints for various objects (record components), namely, diabetes mellitus II (DM II), color blindness (CB), penicillin allergy (PenA), age related macula degeneration (AMD), demographic data (DD) and subject of care area (SCa). The main possible operations on these record components are Create (C), Read (R), Update (U) and Delete (D). In Table 5.1 "NA" means "not applicable".

5.3 Storyboards and use-cases

5.3.1 Storyboard 1 – The patient corrects data in his EHR

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

Table 5.1: Example of three storyboards with the permissions to access an EHR defined by the patient.

	Objects	Operations	BTG option	Knows the existence	Temporal constraints
Storyboard 1: **Functional role**: SC **Role:** P **User**: John Adams	**DM II**	CRUD	NA	NA	NA
	CB	CRUD	NA	NA	NA
	SCa	CRUD	NA	NA	NA
	DD	CRUD	NA	NA	NA
Storyboard 2: **Functional role**: PrHP **Role:** TPrHP **User**: John Adams	**DM II**	R	No	Yes	Available during 1h
	CB	None	No	No	None
	PenA	R	No	Yes	Available during 1h
	AMD	None	No	No	None
Storyboard 3: **Functional role**: SCA1 **Role**: PS **User**: Robert Adams	**DM II**	None	Yes	Yes	No
	CB	R	No	Yes	No
	PenA	R	No	Yes	No
	AMD	None	No	No	No
	DD	RU	No	Yes	No
	SCa	None	No	No	No

Figure 5.1 illustrates a use case that represents storyboard 1. When user John accesses his EHR, as the functional role subject of care, he has permissions to perform all the operations (CRUD) in all the EHR record components.

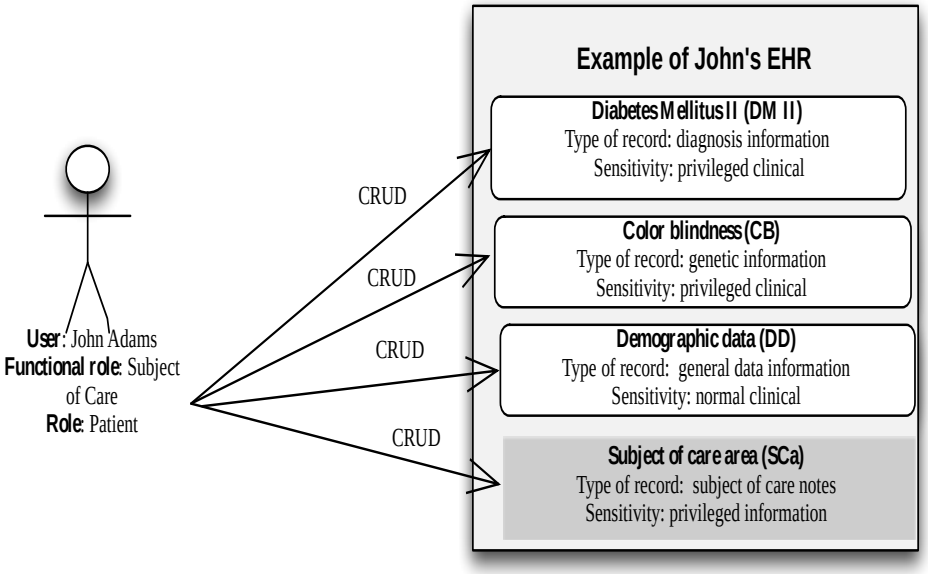

Figure 5.1: Use case 1 for storyboard 1.

5.3.2 Storyboard 2 – The patient has the need of medical care while travelling

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

Figure 5.2 illustrates the use-case relating to storyboard 2. Since the HCP did not have access to the patient's EHR, the patient can access the system by previously defining the role he wants to use for that session. In this use-case, the patient chose the role *temporary privileged healthcare professional* and gave temporary access to the provider that was treating him at that time. The HCP can only access (read- only) components DM II and PenA of that EHR. The role TPrHP has not defined the permissions to perform BTG in any other component of the record so the healthcare professional does not even know of any other components' existence. As the new authorization model allows to define temporal constraints, since this is a temporary role, John associated a limited timeframe to be used (only 1hour).

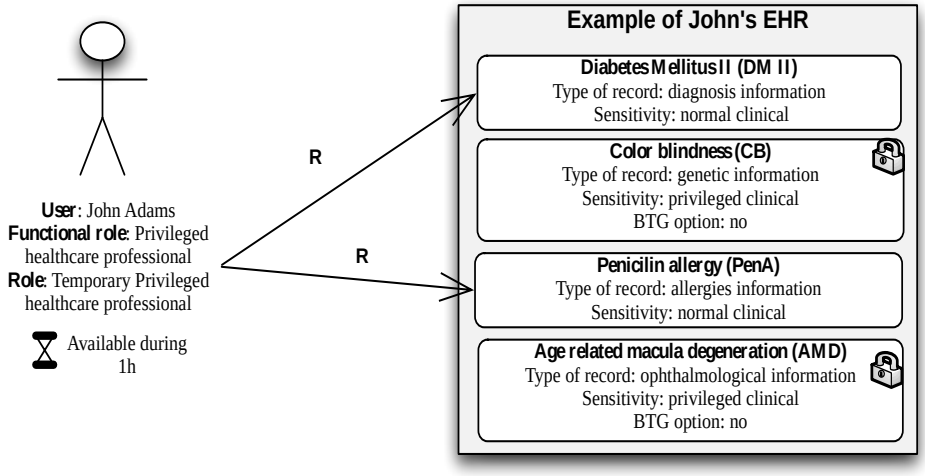

Figure 5.2: Use case 2 for storyboard 2.

5.3.3 Storyboard 3 – The patient's son accesses his father's EHR

John is 59 years old and his son (Robert) suspects he has Diabetes Mellitus and is not treating this condition and taking all the proper care and medication that was prescribed by John's GP. The son accesses John's EHR using the role (PS), whose permissions were previously defined by his father.

The role Patient's Son (*PS*) is hierarchically bellow the functional role subject of care direct (*SC1*), where the patient can associate his/her most direct relatives such as a son/daughter or a parent.

The permissions of the role PS are described in use-case 3 (Figure 5.3) and include the following components: read-only CB and PenA, as well as read and alter the DD component. The contents of the component AMD and the subject of care area are restricted and not visible to the role PS. However, the component DM II is visible to the role PS and John's son can see that this component exists but has no immediate access to its contents. He can perform BTG on this component if he really needs to access it as defined within the model by his father. If he performs the BTG operation on this component, the patient and other responsible parties that were defined by the patient, will be notified of this BTG action and in what components of his EHR they were performed. The patient can, after the fact, require further justifications.

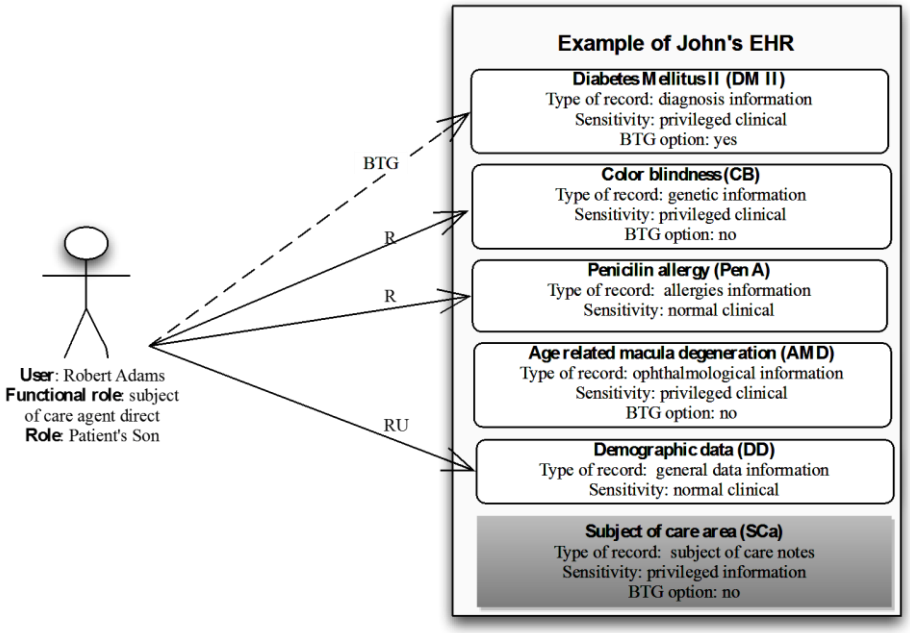

Figure 5.3: Use case 3 for storyboard 3.

5.4 Discussion

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

In the second use-case scenario with the use of the role temporary privileged healthcare professional, the HCP does not belong to the PHN so he would have to blindly treat the patient as a newcomer, without any previous information. The proposed patient authorization model allows the HCP to have a minimum information content that can help in a faster and more successful patient treatment. The patient would have defined this role previously so that it could be used in such a case. As this is a temporary role, a temporary session is created so that once the patient is consulted and treated, his privacy remains and that same HCP that treated him cannot re-access the same EHR.

In the last use-case scenario the patient's son is allowed to access some components of the father's EHR. Other parts can be invisible to the role *PS* or they can be visible but not accessible. These can be associated with the permission to BTG. This allows more flexibility, as it can, sometimes, be the difference between better or worse patient treatment or even between life and death.

In conclusion, the proposed patient authorization model allows for a greater participation, responsibility and control over information security and contents of patients' EHR within the healthcare practice. This model is innovative as it allows the patient to define access control permissions within his PHN but also outside this network when necessary, providing a better healthcare treatment at the point of care. The functional roles subject of care agent direct (SCA1) and

indirect (SCA2) can also be beneficial because they can allow patients' relatives to also take part and help in their treatment.

Furthermore, these can help treating patients' relatives when, for example, they can have access to relevant genetic information about their parents or other relatives. Even if this information is not directly accessible, those functional roles could have the BTG permission to access it and the owner of the EHR would always be notified of the actions performed within his/her EHR.

The flexibility of access and definition of access by the patient is not meant to invade or compromise HCP' workflows or privacy as there will be a restricted area (EHR component) only to be used and accessed by that HCP. It is a reserved area that can be associated to the role or only the user where the HCP can write their personal notes and information about that patient. The temporal constraint with the separation of duties integrated within the authorization model allows to define the level of patients' privacy as fine-grained as the patient desires.

6. Conclusions and recommendations

"Rather than love, than money, than faith, than fame, than fairness... give me truth."
Henry Thoreau

6.1 Research summary

At the beginning of this research it was identified, by means of a literature review, the access control models and standards that allows the patients access their EHR as well as customize the access control rules. The work most complete in terms of research goals was the standard ISO 13606 part 4. However others access control models were selected because they explain interesting security mechanisms that could integrate the proposed patient access control model such as BTG-RBAC and GTRBAC.

After selected the security characteristics was defined the proposed model within a "Patient Healthcare Network". In order to define the administration features of the proposed model was used as reference the ARBAC model. The characteristics of RBAC model were the basis of the proposed model and were also integrated namely Core RBAC, Hierarchical RBAC, Separation of Duties and User Delegation.

The objectives of this MSc thesis work were achieved. However this work should be continued because it is only an initial protocol. The main actors that will use this authorization model (patients) do not set their opinion so *mixed methods* and *focus groups* could be a way to they expresses their needs.

6.2 Main findings

The results of the systematic review (Chapter 2) show that several authors dedicate their research of access control models to the definition and improvement of access control models but none of the models and standards found, fully satisfy the research question of the systematic review, that is allowing the patients to customize the access control rules to their medical records and access their EHR. Although the models and standards do not comply with the goal of the research, they provide security mechanisms and guidelines that could integrate a new extension of the RBAC model (with ISO 13606-4 characteristics, break the glass features and temporal constraints).

The proposed patient authorization model allows for a greater participation, responsibility and control over information security and medical records by the patient. With this new model, the patient can access the EHR as a subject of care, as well as allow family members to do the same (functional roles subject of care agent direct and indirect). With this proposed model the patient, in

addition to the functional role subject of care, accumulates administration functions (functional role Administrator senior). The patient can choose and define which permissions each role can access and with which temporal constraints.

Access to the patient's EHR can be restricted only to HCP that belong to the PHN, or in emergency situations, if the healthcare providers do not have access to that patient EHR (because they do not belong to the PHN) they can break the glass and temporarily access the necessary medical records. On the other hand if the HCP needs a second opinion of other HCP that again does not belong to the PHN the former HCP can delegate permissions so that other HCP can also temporarily access anonymized information in order to get another opinion on the treatment at hand.

6.3 Limitations of the patient's authorization model

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

Again, the option of using this proposed model centered on the patient, could be given to patients themselves, and they could decide what parts of their EHR they want to know and control.

6.4 Recommendations and future work

According to the previous mentioned findings, 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:

- the use of more specific queries in their research and search not only access control models but also standards;
- to integrate both legislation and user needs in their research;
- to use *focus groups* and *mixed methods* with patients and health providers to study of the needs of the actors and their receptivity in the use of the proposed access control model;
- to study which conditions and in what situations the patient wants access and manage their own authorization model;
- the use and test of this proposed model in order to improve and correct defects.

Future work includes the implementation and evaluation of the proposed authorization model with a specific case study in real healthcare practice. Before this implementation there is the need to define what are the needed quality requirements to better define the model as well as a protocol to define how and what has to be evaluated when the model is applied in real practice. Another important addition to this model will be the definition and association of access control permissions directly to users and not only to generic roles. This allows for exceptions to be made inside the group of functional roles and allow a more fine-grained and personalized access control definition.

6.5 Conclusions

The results of this research work thesis constitute the starting point to define a RBAC based patient authorization model that can be used in real healthcare practice. With this new model we hope to bridge the gap that exists between legislation (with medical data protection definition) and what really happens in practice regarding patients' accessing their medical records and customizing the access control rules of the authorization model. With the growth of new technologies and the interest that patients have to be in control and take an active part in their treatment, they need to have a simple but focused model that allows them to easily define access permissions but also closely collaborate and interact with their providers.

References

[1] Ferraiolo, D. F., D. R. Kuhn, and R. Chandramouli, *Role-Based Access Control*, 2 ed.: Artech House, 2007.

[2] Ferreira, A. M., "Modelling Access Control for Healthcare Information Systems - How to control access through policies, human processes and legislation," PhD, Computer Science, University of Porto, Porto, 2010.

[3] *Health informatics - Electronic health record communication* ISO/TS 13606-4:2009, 2009.

[4] Ravi, S., B. Venkata, and M. Qamar. (1999). "The ARBAC97 model for role-based administration of roles." ACM Trans. Inf. Syst. Secur. 1094-9224, vol. 2, pp. 105-135.

[5] Sandhu, R., D. Ferraiolo, and R. Kuhn. (2000). The NIST model for role-based access control: towards a unified standard. Proceedings of the fifth ACM workshop on Role-based access control, Berlin, Germany, pp. 47-63.

[6] Joshi, J., E. Bertino, and A. Ghafoor. (2002). Temporal hierarchies and inheritance semantics for GTRBAC. Proceedings of the seventh ACM symposium on Access control models and technologies, Monterey, California, USA, pp. 74-83.

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

[8] Peleg, M., D. Beimel, D. Dori, and Y. Denekamp. (2008). "Situation-Based Access Control: Privacy management via modeling of patient data access scenarios." Journal of Biomedical Informatics, vol. 41, pp. 1028-1040.

[9] Watts, J., H. M. Yu, and X. H. Yuan. (2010). "Case Study: Using Smart Cards with PKI to Implement Data Access Control for Health Information Systems." IEEE Southeastcon 2010: Energizing Our Future, pp. 163-167.

[10] Department of Health & Human Services. (2011, 23/9/2011). *The office of the national coordinator for health information technology*. Available: http://healthit.hhs.gov/portal/server.pt?open=512&objID=2996&mode=2

[11] *Health Insurance Portability and Accountability Act* U. S. D. o. H. H. Services, 1996.

[12] *Protection of Medical Data - Recommendation nºR (97) 5,* Committee of Ministers to Member States, 1997.

[13] Samy, G. N., R. Ahmad, and Z. Ismail. (2009). "Threats to Health Information Security." Fifth International Conference on Information Assurance and Security, Vol 2, Proceedings, pp. 540-543.

[14] Solutions, K. F., "Healthcare Information and Management Systems Society (HIMSS) Analytics Report: Security of Patient Data," Kroll Fraud Solutions, USA2008.

[15] Vaast, E. (2007). "Danger is in the eye of the beholders: Social representations of Information Systems security in healthcare." Journal of Strategic Information Systems, vol. 16, pp. 130-152.

[16] Joshi, J., W. G. Aref, A. Ghafoor, and E. H. Spafford. (2001). "Security models for web-based applications." Commun. ACM, vol. 44, pp. 38-44.

[17] *Health Informatics - Privilege management and access control* ISO/TS 22600-2:2006, 2006.

[18] Ferreira, A., R. Cruz-Correia, L. Antunes, and D. Chadwick. (2007). "Access Control: how can it improve patients' healthcare? ." Stud Health Technol Inform, vol. 127, pp. 65-76.

[19] Pereira, C., C. Oliveira, C. Vilaça, and A. Ferreira. (2011). Protection of clinical data - Comparison of European with American Legislation and respective technological applicability. HealthInf 2011 - International Conference on Health Informatics, Rome, pp. 567-570.

[20] Ross, S. E. and C. T. Lin. (2003). "The effects of promoting patient access to medical records: A review." Journal of the American Medical Informatics Association, vol. 10, pp. 129-138.

[21] Ferreira, A., A. Correia, A. Silva, A. Corte, A. Pinto, A. Saavedra, A. L. Pereira, A. F. Pereira, R. Cruz-Correia, and L. F. Antunes. (2007). "Why Facilitate Patient Access to Medical Records." Medical and Care Compunetics 4, vol. 127, pp. 77-90.

[22] Lau, D. H. (2002). "Patient empowerment--a patient-centred approach to improve care." Hong Kong medical journal = Xianggang yi xue za zhi / Hong Kong Academy of Medicine, vol. 8, pp. 372-4.

[23] *On the impact of information technologies on health care - The patient and Internet Recommendation* C. o. Ministers, 2004.

[24] *Lei de Informação Genética Pessoal de Saúde.,* Diário da República 12/2005, 2005.

[25] *Parecer sobre Informação de Saúde e Registos Informáticos de Saúde,* Conselho Nacional de Ética para as Ciências da Vida Parecer 60/CNECV/2011, 2011.

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

[27] Hassol, A., J. M. Walker, D. Kidder, K. Rokita, D. Young, S. Pierdon, D. Deitz, S. Kuck, and E. Ortiz. (2004). "Patient experiences and attitudes about access to a patient electronic health care record and linked web messaging." Journal of the American Medical Informatics Association : JAMIA, vol. 11, pp. 505-13.

[28] Hayrinen, K., K. Saranto, and P. Nykanen. (2008). "Definition, structure, content, use and impacts of electronic health records: A review of the research literature." International Journal of Medical Informatics, vol. 77, pp. 291-304.

[29] Motta, G., Furuie S.„ "A Contextual Role-Based Access Control Authorization Model for Electronic Patient Record," in *IEEE Transactions on Information Techonology in Biomedicine* vol. 7, ed, 2003, p. 202:207.

[30] Honeyman, A., B. Cox, and B. Fisher. (2005). "Potential impacts of patient access to their electronic care records." Informatics in primary care, vol. 13, pp. 55-60.

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

[32] Giuri, L. (1996). Role-based access control: a natural approach. Proceedings of the first ACM Workshop on Role-based access control, Gaithersburg, Maryland, United States, p. 13.

[33] Eyers, D. M., J. Bacon, and K. Moody. (2005). "OASIS role based acess control for electronic health records." IEEE,

[34] Osborn, S., R. Sandhu, and Q. Munawer. (2000). "Configuring role-based access control to enforce mandatory and discretionary access control policies." ACM Trans. Inf. Syst. Secur., vol. 3, pp. 85-106.

[35] Røstad, L., "Access Control in Healthcare Information Systems," PhD, Department of Computer and Information Science, Norwegian University of Science and Technology, Trondheim, 2009.

[36] Gollmann, D., *Computer security*. New York: John Wiley & Sons, Inc., 1999.

[37] Ferraiolo, D., R. Sabdhu, S. Gavrila, D. R. Kuhn, and R. Chandramoulin. (2001). "Proposed NIST Standard for Role-Based Access Control." ACM Transations on Information and System Security, vol. 4, pp. 224-274.

[38] Gansen, Z., D. Chadwick, and S. Otenko. (Year). Obligations for Role Based Access Control. Advanced Information Networking and Applications Workshops, 2007, AINAW '07. 21st International Conference on, pp. 424-431.

[39] Simon, R. and M. E. Zurko. (1997). Separation of Duty in Role-based Environments. Proceedings of the 10th IEEE workshop on Computer Security Foundations, p. 183.

[40] Sejong, O. and S. Ravi, "A model for role administration using organization structure," in *Proceedings of the seventh ACM symposium on Access control models and technologies 1-58113-496-7*, ed. Monterey, California, USA: ACM, 2002, pp. 155-162.

[41] Shen, H.-b. and F. Hong. (2006). An Attribute-Based Access Control Model for Web Services. Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies, pp. 74-79.

[42] Thomas, R. and R. Sandhu, *Task-based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management*: Chapman & Hall, 1997.

[43] ISO/TC 215, "Health Informatics ", ed. Switzerland: International Organization for Standardization's (ISO) Technical Committee (TC), 2001.

[44] Abou El Kalam, A. and Y. Deswarte. (2003). "Security model for health care computing and communication systems." Security and Privacy in the Age of Uncertainty, vol. 122, pp. 277-288.

[45] Reid, J., I. Cheong, M. Henricksen, and J. Smith. (2003). "A novel use of RBAC to protect privacy in distributed health care information systems." Information Security and Privacy, Proceedings, vol. 2727, pp. 403-415.

[46] Motta, G. H. M. B. and S. S. Furuie. (2003). "A contextual role-based access control authorization model for electronic patient record." Ieee Transactions on Information Technology in Biomedicine, vol. 7, pp. 202-207.

[47] Schoenberg, R. and C. Safran. (2000). "Internet based repository of medical records that retains patient confidentiality." British Medical Journal, vol. 321, p. 1199.

[48] El Kalam, A. A., R. El Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miege, C. Saurel, and G. Trouessin. (2003). "Organization based access control." IEEE 4th International Workshop on Policies for Distributed Systems and Networks, Proceedings, pp. 120-131.

[49] Motta, G. H. M. B. and S. S. Furuie. (2004). "MAAC: a software tool for user authentication and access control to the electronic patient record in

open distributed environment." Medical Imaging 2004: Pacs and Imaging Informatics, vol. 5, pp. 360-371.

[50] Blobel, B., R. Nordberg, J. M. Davis, and P. Pharow. (2006). "Modelling privilege management and access control." International Journal of Medical Informatics, vol. 75, pp. 597-623.

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

[52] Ferreira, A., R. Correia, D. Chadwick, and L. Antunes. (2010). "Access control in healthcare: the methodology from legislation to practice." Studies in health technology and informatics, vol. 160, pp. 666-70.

[53] Yao, W., K. Moody, and J. Bacon. (2001). A model of OASIS role-based access control and its support for active security. Proceedings of the sixth ACM symposium on Access control models and technologies, Chantilly, Virginia, United States, pp. 171-181.

[54] Georgiadis, C. K., I. Mavridis, G. Pangalos, and R. K. Thomas. (2001). Flexible team-based access control using contexts. Proceedings of the sixth ACM symposium on Access control models and technologies, Chantilly, Virginia, United States, pp. 21-27.

[55] Joshi, J., B. Shafiq, A. Ghafoor, and E. Bertino. (2003). Dependencies and separation of duty constraints in GTRBAC. Proceedings of the eighth ACM symposium on Access control models and technologies, Como, Italy, pp. 51-64.

[56] ISO/TS-13606, "Health informatics - Electronic health record communication " in *Part 4: Security* vol. 13606-4:2009, ed: ISO/TC, 2009.

[57] Baxter, C., R. Dell, S. Publ, and R. Race. (2007). "Assessing and improving EHR data quality." Journal of AHIMA / American Health Information Management Association, vol. 78, pp. 69-72.

[58] SangYeob, N. and C. SuhHyun, "Role delegation in role-based access control," in *Proceedings of the fifth ACM workshop on Role-based access control 1-58113-259-X*, ed. Berlin, Germany: ACM, 2000, pp. 39-44.

[59] Crampton, J. and H. Khambhammettu. (2008). "Delegation in role-based access control." International Journal of Information Security, vol. 7, pp. 123-136.

[60] Longhua, Z., A. Gail-Joon, and C. Bei-Tseng, "A role-based delegation framework for healthcare information systems," in *Proceedings of the seventh ACM symposium on Access control models and technologies 1-58113-496-7*, ed. Monterey, California, USA: ACM, 2002, pp. 125-134.

[61] Gutierrez, A., A. Godiyal, M. Stockton, M. LeMay, C. Gunter, and R. Campbell, "Sh@re: negotiated audit in social networks," in *Proceedings of the 2009 IEEE international conference on Systems, Man and Cybernetics 978-1- 4244-2793-2*, ed. San Antonio, TX, USA: IEEE Press, 2009, pp. 74-79.

[62] Shah, S. U., Fazl-e-Hadi, and A. A. Minhas. (2009). "New Factor of Authentication: Something You Process." International Conference on Future Computer and Communications, Proceedings, pp. 102-106.

[63] Microsoft. (2011, October). *Microsoft Health Vault*. Available: http://www.microsoft.com/en-us/healthvault/

[64] American Health Information Management Association Foundation. (2011, October). *myPHR*. Available: http://www.myphr.com/

Appendix

Articles submitted to the Conference HealthInf 2012 waiting for approval

PROVIDING FOR PATIENT EMPOWERMENT

A systematic review on customizable access control models

Cátia Santos-Pereira[1], Ricardo Cruz-Correia[1,2] and Ana Ferreira[1,3]

1. Center for Research in Health Techonologies and Information Systems,University of Porto - Portugal - CINTESIS
2. Department of Health Information and Decision Sciences - CIDES
3. Informatics Centre, University of Porto – Portugal
4. Faculty of Medicine of the University of Porto,Portugal
{catiap, rcorreia, amlaf}@med.up.pt

Keywords: Patient Empowerment, Electronic Health Records, Role Based Access Control Models, Access Control Standards and Guidelines.

Abstract: American and European legislation state that patients must be able to see, copy, correct and control who can access their medical records. The most commonly used access control model in healthcare is the Role Based Access Control (RBAC) but there are also standards that define guidelines for access control in healthcare. The main objective of this paper is to verify if existing standards and RBAC based models comply with legislation requirements regarding patient access as well as customized access to his/her Electronic Health Record (EHR). A literature review of published material was performed and comprised 22 articles and standards from which 12 were included for analysis. Results show that only two models and two standards include patients as a user of the EHR and only one model and one standard provide the possibility for them to customize access control to their EHR. Existing standards define some guidelines for these issues but they are too generic to be directly applied to real healthcare settings. Future work includes the definition of an access control model that will allow both access and easy definition, by the patients, of access control rules regarding their EHR within several healthcare scenarios.

1 INTRODUCTION

According to the American Legislation (Health Insurance Portability Accountability Act - HIPAA) and the European legislation (Recommendation No R (97) 5) for protection of medical data, the subject of care has the right to play a pivotal role in the decisions regarding the content and distribution of her/his medical records, as well as the right to be informed of its contents (HIPAA, 1996) (Rec97, 1997) (Pereira et al., 2011).

The ISO/TR 20514 defines Electronic Health Record (EHR) as a repository of patient data in digital form, stored and exchanged securely, and accessible by multiple authorized users (ISO/TR-20514, 2005).

Some studies regarding the access of medical records by the patient suggest modest improvements in doctor-patient communication adherence, patient empowerment and patient education (Ross and Lin, 2003) (Ferreira et al., 2007a). This process makes patients more careful in following medical recommendations (Ferreira et al., 2007a). Although patients may find some parts of their medical records difficult to understand, patients who are offered a chance to review their medical records are mostly satisfied with the experience (Ferreira et al., 2007a) (Ross and Lin, 2003) (Hassol et al., 2004) (Honeyman et al., 2005). On the other hand healthcare providers also recognized the benefit of patient's ability to review and comment on their medical information prior to a visit (Siteman et al., 2006).

Access control is essential to provide for the confidentiality of EHR because it is part of the authorization process where the system checks if the user can access the resources he/she requested. The most commonly used access control model in healthcare is the Role Based Access Control (RBAC) (Ferreira et al., 2007b) (Sandhu et al., 2000). Many authors focused their research in extending the RBAC model according to some needed characteristics. For example, the Attribute-Based Access Control (ABAC) (Shen and Hong, 2006), bases the authorization in attributes and the Task-Based Access Control model (TBAC) (Thomas and Sandhu, 1997) integrate temporal or inter-task constraints in RBAC.

In addition, there are also some international standards that define guidelines for access control in healthcare. The International Organization for Standardization (ISO) has an area dedicated to health informatics, the ISO/TC 215, that pretend to promote interoperability between independent systems, to enable compatibility and consistency for health information and data (ISO/TC-215, 2001).

The main objective of this paper is to verify if the existing standards and RBAC based extension models comply with legislation requirements and procedures regarding patients' access to their EHR. Moreover, this study aims to analyse if existing models and standards provide for patients' definition of what healthcare professionals can access within their medical records, allowing this way for patients to customize access control rules and take full responsibility and control of their health.

2 METHODS

The literature review was performed in June 28, 2011 with searches in Pubmed, IEEE Xplore, ISI Web of Knowledge and International Organization for Standardization.

The queries applied were:

- *"RBAC [All Fields] AND ("Health"[MeSH Terms] OR "Health"[All Fields]) AND Model [All Fields]"* in Pubmed;
- *"RBAC Health Model<in>metadata"* in IEEE Xplore;
- *"Topic (RBAC Health Model)"* in ISI Web of Knowledge;
- *"Health Access Control Model"* in ISO.

The results from the these queries were filtered according to the following inclusion criteria:

- Language of the article (English);
- Review of title and abstracts (adequate context).

The review was done in several stages. Initially, the repeated articles in the various databases were identified, they were then reviewed according to the inclusion criteria and finally read and analysed.

For each article/standard, three relevant characteristics were analysed: (a) if they referred to EHR; (b) if they included within their access control policies the possibility for patients to also access their EHR; (c) and, most importantly, if there was the capability for the patient himself/herself to customize that model and define his/her own access control rules, regarding their EHR.

After the analysis of these articles/standards, their citations were also reviewed and those that suited to the inclusion criteria were also integrated in the review.

The search for full text articles was performed in the following databases: Google Scholar, Open Repository of University of Porto and the Open Access Repository Scientific Portugal. As a last resort, a request via e-mail for the full article was sent to the authors.

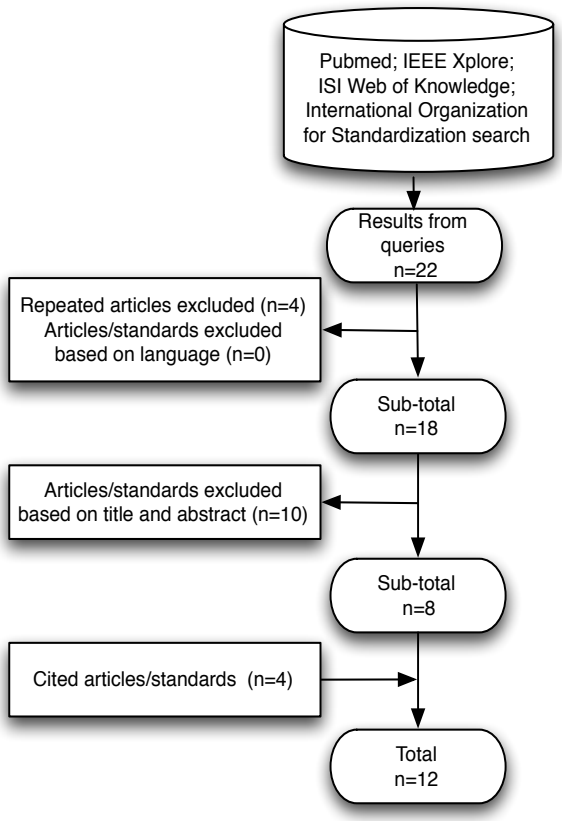

Figure 1: Flowchart representing the review process and the results.

A total of 22 articles/standards were obtained from the search queries. The Figure 1 presents the review process including the results that were obtained in each stage. From these, 4 articles were excluded because they were repeated. All remaining 18 articles/standards were written in English and were all available as full text. However, after the analysis of title and abstract, 10 articles/standards were not fit to be included within the review. After analysis of the articles/standards that are cited by the articles/standards found within the search, 4 articles/standards were included, so a total of 12 articles/standards were included in the final review.

3 RESULTS

From these 12 articles/standards, 10 of them present RBAC extension models while 2 describe access control standards and guidelines in healthcare.
Table 1 presents in more detail the results of the analysis of the 12 articles/standards that were included in the review. The results are divided between articles and standards found in the queries and articles and standards found within the citations of included articles/standards. "X" means the existence while "—" means the inexistence of each characteristic. The results of a more detailed analysis of each article and standard are describe in the following paragraphs.

The model of Abou EL Kalam et al. focuses mainly on the relation between clinician and patient and the involvement of the clinician, at the moment of the request, and the process of care (Abou El Kalam and Deswarte, 2003).

However, the article does not describe the type of roles, which the model integrates. It just alerts for the need of patients' consent to access their most sensitive healthcare information.

J. Reid et al. presents a model based in RBAC which defines a new characteristic where a set of privileges held by a role can be allowed or denied to other roles without using traditional RBAC constraints, such as separation of duties (Reid et al., 2003). This model introduces a very generic role hierarchy where the role *care team* is included and without referring to the role of the patient.

The Contextual Role-Based Access Control is a model that regulates user access to medical records based on organizational roles (Motta and Furuie, 2003). The authors also refer the possibility of including the role *patient* so that users can see their own data and have also the possibility of determining the level of security access for each data element of their record. The authors cite the schema of access control defined by (Schoenberg and Safran, 2000) as an example to follow.

In the Organization Based Access Control (ORBAC) model the specification of the security policy is parameterized by the organization, for instance, a private clinic or a department of an Hospital (El Kalam et al., 2003). The authors refer four types of views for the Electronic Health Record: (1) *administrative_record*, (2) *medical_record*, (3) *surgical_record* and (4) *patient_record*. The last view concerns the whole EHR and integrates the previous three. There is not, however, a specification of who can access the patient record view and if the patient himself/herself would be able to access and define access permissions to his/her record.

The Privilege Management and Access Control (PMAC) is included in the standard ISO/TS 22600 part 2 (ISO/TS-22600, 2006). PMAC refers RBAC as a reference to follow regarding access control models. This standard also refers that administration constraints may need to be enforced, for example, by using *separation of duties,* but does not define how and what other procedures must be included and applied besides these constraints to still guarantee EHR confidentiality. The annex A of this standard presents a set of *functional roles*, which include the *subject of care* (normally the patient) and *subject of care agent* (parent or guardian), to manage the creation, access, processing and communication of healthcare information. It is not clearly defined within the standard who delegates access control permissions to the functional roles, which record components a role can access nor if the patient can take part in the delegation process.

Patrick et al. proposed a RBAC model with privacy-based extension, amidst other challenges (Patrick C. K., 2007). The most pressing privacy concerns that have been observed for e-Health care informatics include: (1) acquisition, storage, and processing of e-Health data; (2) consent to process and disclose e-Health data; (3) and rights of the data subject (typically the patient) to access and rectify his/her own health dataset. The authors propose to include in their model the role *e-patient* in order to comply with the medical data protection legislation. This role has the right to access and correct his EHR. However, the authors do not specify which privileges are associated with this role and who and how can the access control rules be customized.

Beimel et al. introduce the Situation Based Access Control (SitBAC) model which was designed for expressing scenarios of patient data access request as a basis to preserve the patient's privacy (Beimel and Peleg, 2009). The model does not mention any type

of roles nor the patient as another user to access the medical record.

The Break-the-Glass Role Based Access Control (BTG-RBAC) includes *Break The Glass* permission/action within the RBAC engine (Ferreira et al., 2010). This can be used to *break* or override the access control rules in a controlled manner. This model extends the Core RBAC model with obligations (Gansen et al., 2007) and defines generically when a role can have permissions to BTG on specific resources. Patient roles are never mentioned.

The Open Architecture for Security Interworking Services (OASIS) model adds concepts such as *Appointment, Pre-requisite roles* and *Constraints* to the RBAC model (Yao et al., 2001). Only when the role activation rule is satisfied is the role activated. This model does not allow hierarchic roles or role inheritance because the authors argue that hierarchies are not possible to execute in distributed environments. Although this model is very detailed in describing roles, it does not specify the type of roles that can be used.

The Contextual Team Based Access Control (C-TMAC) model integrates the concepts *team* and *contexts* into RBAC (Georgiadis et al., 2001). Teams are associated with contexts and users are members of those teams. Examples show the association of permissions to a set of roles (*doctor*, *head nurse* and *nurse*) in a specific context. None of these examples describe the role patient. As OASIS, the C-TMAC model does not define hierarchic roles.

Joshi et al. added *Temporal Constraints* to the RBAC model (Joshi et al., 2002). In particular, Generalized Temporal Role Based Access Control (GTRBAC) makes a clear distinction between *role*

Table 1: Summary of results of the research

	Models and Standards	Reference	EHR application	Patient permissions	Patient customization
Articles/ standards found within the queries	"Security model for health care computing and communication systems"	(Abou El Kalam and Deswarte, 2003)	X	—	—
	"A novel use of RBAC to protect privacy in distributed health care information systems"	(Reid et al., 2003)	X	—	—
	Contextual Role-Based Access Control	(Motta and Furuie, 2004, Motta and Furuie, 2003)	X	X	X
	Organization Based Access Control (ORBAC)	(El Kalam et al., 2003)	X	—	—
	Privilege Management and Access Control (ISO/TS 22600)	(ISO/TS-22600, 2006, Blobel et al., 2006)	X	X	—
	RBAC with privacy based extensions	(Patrick C. K., 2007)	X	X	—
	Situation Based Access Control (SitBAC)	(Beimel and Peleg, 2009)	X	—	—
	Break-the-Glass Role Based Access Control (BTG-RBAC)	(Ferreira et al., 2010)	X	—	—
Cited articles/standards	Open Architecture for Security Interworking Services (OASIS)	(Yao et al., 2001)	X	—	—
	Contextual Team Based Access Control (C-TMAC)	(Georgiadis et al., 2001)	X	—	—
	Generalized Temporal Role Based Access Control (GTRBAC)	(Joshi et al., 2002, Joshi et al., 2003)	X	—	—
	Electronic health record communication- Security (ISO/TS 13606)	(ISO/TS-13606, 2009)	X	X	X

enabling and *role activation*. This model includes hierarchic roles and inheritance and separation of duties and time constraints. The model does not specify the type of roles and permissions that can be applied.

The standard ISO/TS 13606 (ISO/TS-13606, 2009) came to improve some of the ISO/TS 22600 limitations. It describes the privilege methodology to be used in order to specify the access control to an EHR. In part 4, *data sensitivity levels* for each *record component* are defined and the *functional roles* are mapped to each one of those components regarding the defined privileges and permissions. This standard explores the idea of patient empowerment, where the patients have access to their EHR and can customize its access by delegating permissions to each functional role. Moreover, this standard presents a set of access control archetypes for the EHR structure.

Annex A describes some use-case healthcare scenarios that exemplify the use of functional roles and which parts of the EHR record can be accessed by those roles, Figure 2 shows an example. The purpose of this example is to show how a generic EHR policy can be defined. It should be noted that this policy is itself an evidence that *Joanna Jones* (patient) has something to hide, and must be restricted in access so that her *guardian* (Joanna's mother) does not know of its existence.

4 DISCUSSION

Results show that several authors dedicate their research to the definition and improvement of access control models, which are based on RBAC, within the healthcare domain, specifically to access electronic health records.

In summary, only the model of Motta and Furuie (Motta and Furuie, 2003) and the model of Patrick et al. (Patrick C. K., 2007), together with the two ISO standards presented include the patient as one more role to access the EHR. In addition, the ISO/TS 13606-4 standard and the model of Motta and Furuie (Motta and Furuie, 2003) introduce also the capability of the patients to customize access control rules to their EHR.

For a better understanding of the differences between the models selected for review we now test the behaviour of the models and the ISO-22600-2 standard in the context of the use-case presented in Figure 2. We also discuss the limitations of the use-case:

- The models proposed by Motta and Furuie (Motta and Furuie, 2003) and Patrick et al. (Patrick C. K., 2007) are not possible to apply to this use-case, because the authors do not define: the possibility of the *Subject of Care Agent* to access the *Subject of Care* EHR; *data*

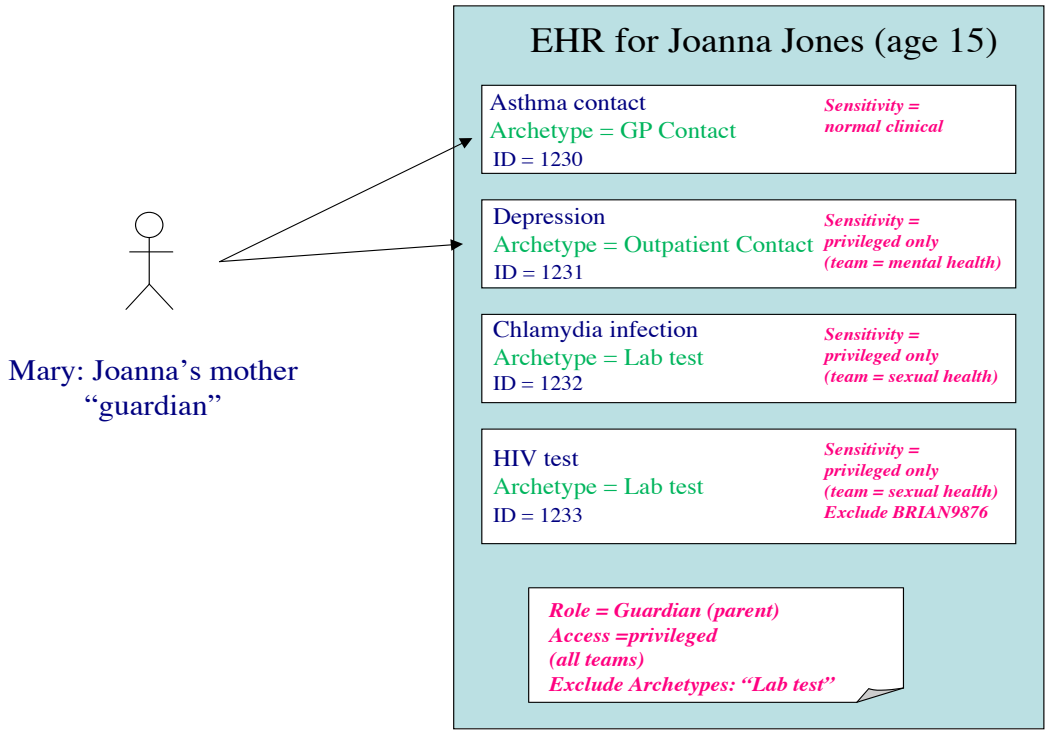

Figure 2: Illustrative access control example (ISO/TS-13606, 2009)

sensitivity levels for each *record component*; and who (*role*) has access of each *record component*.

- The ISO/TS 22600-2 standard (ISO/TS-22600, 2006) provides a set of functional roles that include *subject of care* and *subject of care agent* however, as in the previous models, it does not include the definition of the *data sensitivity levels*, *types of record components* and association between *functional roles* and *record components*. For these reasons it is not possible to apply it to the use-case.

- In the use-case presented in the ISO/TS 13606-4 standard (ISO/TS-13606, 2009) Joanna's mother does not have access to two types of *record components* (Chlamydia infection and HIV test). This standard does not foresee emergencies situations where the access to this data would be indispensable. It also does not foresee where and at what time a functional role can access a patient's EHR. Usually this access would not be made outside of the workplace and past the shift hours.

Despite the limitations previously described, as was mentioned before, this standard defines clearly, with multiple examples (tables and use-cases), the association between functional roles and record components as well as record component sensitivity. However, due to it being a standard, the definition of functional role is appropriately generic but, in the case of health professionals, it is difficult to define which health professionals (users) are assigned to which functional role. The health institution where the health professional works manages this assignment. This standard does not define constraints in the attribution of different functional roles to the same user in the same session (e.g. dynamic separation of duties). It also does not define either functional role hierarchy or functional role inheritance and how the patient will be able to customize the model with the restrictions that he/she wants to apply.

Nevertheless, with all these characteristics we think that the standard ISO/TS 13606-4 is the most complete standard in terms of our research goals.

However, in spite of generically allowing the patients to customize the access control rules to their medical records, the models are too generic to be applied directly to specific healthcare scenarios where customization is required. None of the analysed research studies describes how the patient can customize his/her EHR in more specific scenarios.

There is, therefore, a lack of research within this area. Because if on one hand legislation empowers the patient to be responsible and be active in protecting, controlling and managing his/her medical records, on the other hand, there are no specific guidelines that can provide for this.

Although some of the models presented in the results section do not reach the research goals, they provide security mechanisms that could integrate a new extension of the RBAC model (e.g. *Break the Glass policy* and *Time Constraints*). This new extension could integrate the definitions proposed by the ISO/TS 13606-4 standard as well as explore the security mechanisms of RBAC (e.g. *separation of duties constraints*, *role hierarchies)* and integrate mechanisms such as *break the glass* and *time constraints.*

5 CONCLUSION

Hassol et al. showed that patients were happy to have access to their own EHR and also concerned with the need to guarantee security and privacy of his/her medical data (Hassol et al., 2004).

The authors believe that it is essential to define an access control model that can give the patients the needed empowerment. Patients must be able to easily define who can access what regarding their medical records and customize the access control model whenever needed.

Future works include the definition of an access control model, based on the models and standards found, that will allow both access and easy definition and customization, by the patients, of access control rules regarding their medical records.

ACKNOWLEDGEMENTS

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

REFERENCES

Abou El Kalam, A. & Deswarte, Y. 2003. Security model for health care computing and communication systems. *Security and Privacy in the Age of Uncertainty,* 122**,** 277-288.

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

Blobel, B., Nordberg, R., Davis, J. M. & Pharow, P. 2006. Modelling privilege management and access control. *International Journal of Medical Informatics,* 75**,** 597-623.

El Kalam, A. A., El Baida, R., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., Miege, A., Saurel, C. & Trouessin, G. 2003. Organization based access control. *Ieee 4th International Workshop on Policies for Distributed Systems and Networks, Proceedings***,** 120-131.

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

Ferreira, A., Correia, R., Chadwick, D. & Antunes, L. 2010. Access control in healthcare: the methodology from legislation to practice. *Studies in health technology and informatics,* 160**,** 666-70.

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

Gansen, Z., Chadwick, D. & Otenko, S. Obligations for Role Based Access Control. Advanced Information Networking and Applications Workshops, 2007, AINAW '07. 21st International Conference on, 21-23 May 2007 2007. 424-431.

Georgiadis, C. K., Mavridis, I., Pangalos, G. & Thomas, R. K. 2001. Flexible team-based access control using contexts. *Proceedings of the sixth ACM symposium on Access control models and technologies.* Chantilly, Virginia, United States: ACM.

Hassol, A., Walker, J. M., Kidder, D., Rokita, K., Young, D., Pierdon, S., Deitz, D., Kuck, S. & Ortiz, E. 2004. Patient experiences and attitudes about access to a patient electronic health care record and linked web messaging. *Journal of the American Medical Informatics Association : JAMIA,* 11**,** 505-13.

HIPAA 1996. Health Insurance Portability and Accountability Act *In:* SERVICES, U. S. D. O. H. H. (ed.).

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

ISO/TC-215 2001. Health Informatics Switzerland: International Organization for Standardization's (ISO) Technical Committee (TC).

ISO/TR-20514 2005. Health informatics — Electronic health record — Definition, scope, and context. *In:* ISO/TR (ed.) *ISO/TR 20514.* Geneva.

ISO/TS-13606 2009. Health informatics - Electronic health record communication *Part 4: Security.* ISO/TC.

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

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

Joshi, J. B. D., Shafiq, B., Ghafoor, A. & Bertino, E. 2003. Dependencies and separation of duty constraints in GTRBAC. *Proceedings of the eighth ACM symposium on Access control models and technologies.* Como, Italy: ACM.

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

Motta, G. H. M. B. & Furuie, S. S. 2004. MAAC: a software tool for user authentication and access control to the electronic patient record in open distributed environment. *Medical Imaging 2004: Pacs and Imaging Informatics,* 5**,** 360-371.

Patrick C. K., H. a. Y. Z. 2007 Privacy Access Control Model for Aggregated e-Health Services. *Eleventh International IEEE EDOC Conference Workshop (EDOCW'07).*

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

Rec97 1997. Protection of Medical Data - Recommendation nºR (97) 5. *In:* STATES, C. O. M. T. M. (ed.). Europe.

Reid, J., Cheong, I., Henricksen, M. & Smith, J. 2003. A novel use of RBAC to protect privacy in distributed health care information systems. *Information Security and Privacy, Proceedings,* 2727**,** 403-415.

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

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

Schoenberg, R. & Safran, C. 2000. Internet based repository of medical records that retains patient confidentiality. *British Medical Journal,* 321**,** 1199.

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

Yao, W., Moody, K. & Bacon, J. 2001. A model of OASIS role-based access control and its support for active security. *Proceedings of the sixth ACM symposium on Access control models and technologies.* Chantilly, Virginia, United States: ACM.

ONE WAY TO PATIENT EMPOWERMENT
A proposal for an authorization model

Cátia Santos-Pereira[1,2,4], Luis Antunes[5,6], Ricardo Cruz-Correia[1,2,4] and Ana Ferreira[1,3,4]
1. *Center for Research in Health Techonologies and Information Systems – CINTESIS*
2. *Department of Health Information and Decision Sciences – CIDES*
3. *Informatics Centre - CI*
4. *Faculty of Medicine, University of Porto, Al. Prof. Hernâni Monteiro, 4200-319 Porto, Portugal*
{catiap, rcorreia, amlaf}@med.up.pt

5. *Institute of Telecommunications, University of Porto*
6. *Faculty of Science, University of Porto, Rua Campo Alegre, 4169 – 007 Porto, Portugal*
lfa@dcc.up.pt

Keywords: Role Based Access Control, Administration Role Based Access Control, ISO 13606-4 standard, Patient Empowerment, Authorization Model.

Abstract: American and European Legislation for protection of medical data agree that the patient has the right to play a pivotal role in the decisions regarding the content and distribution of her/his medical records. The Role Based Access Control (RBAC) model is the most commonly used access control model in healthcare. The aim of this work is to define and propose a patient authorization model based on RBAC to be used and customized by the patient. The proposed patient authorization model is described within a "Patient's Healthcare Network" (PHN), and combines several characteristics from ISO 13606-4 standard, RBAC and Administration Role Based Access Control (ARBAC) models, temporal constraints and break the glass permissions. The patient will actively manage the roles and permissions as well as give permissions of administration to other roles, if necessary. With this model we hope to start bridging the gap that exists between legislation and what really happens in practice in terms of patients controlling and be actively involved in their healthcare. Future work includes the implementation and evaluation of the proposed model with a specific case study in real healthcare practice.

1 INTRODUCTION

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

An authenticated user is authorized, within the system, to perform only certain actions that are associated to his or her role e.g. to search through certain medical records of only patients under his or her care (Shortliffe and Cimino, 2006). The Role Based Access Control (RBAC) model is the most commonly used access control model in healthcare (Ninghui and Ziqing, 2007), (Sandhu et al., 2000, Beimel and Peleg, 2009), (Ferreira et al., 2007) and has emerged as a promising alternative to traditional Discretionary Access Control (DAC) and Mandatory Access Control (MAC) models (Giuri, 1996), (Joshi et al., 2001), (Osborn et al., 2000), (Sandhu, 1998).

However in large enterprise systems, the number of roles can be in the hundreds or thousands, and users can be in the tens or hundreds of thousands. Managing these roles, users, and their interrelationships is a formidable task that is often

highly centralized in a small team of security administrators (Sejong and Ravi, 2002).

Both American Legislation (Health Insurance Portability Accountability Act - HIPAA) and the European legislation (Recommendation No R (97) 5) for protection of medical data, agree that the subject of care (normally the patient) has the right to play a pivotal role in the decisions regarding the content and distribution of her/his medical records, as well as the right to be informed of its contents (HIPAA, 1996), (Rec97, 1997), (Pereira et al., 2011).

A systematic review performed in June 2011 (Santos-Pereira, 2011), with the objective of verifying the existence of standards and RBAC based models that comply with legislation requirements regarding patient access as well as customized access of his/her Electronic Health Record (EHR), showed that existing standards define some guidelines for theses issues but they are too generic to be directly applied to real healthcare settings. The ISO/TS 13606-4 standard was the most complete standard in terms of the research goals.

There is, therefore, a lack of research within this area. Because if, on one hand, legislation empowers the patient to be responsible and be active in protecting, controlling and managing his/her medical records, on the other hand, there are no specific guidelines that can provide and define this in practice. So we believe that it is essential to define an access control model that gives the patients the needed empowerment. Patients must be able to easily define who can access what regarding their medical records and customize the access control model whenever needed.

The aim of this work is to define and propose a patient authorization model to be used and customized by the patient. The model is based on RBAC and with this model the patient can define who and in what situations an authorized healthcare professional can access his/her medical record.

2 METHODS

Several characteristics from various access control models and standards were studied in order to define the new authorization model (Santos-Pereira, 2011). These are mainly focused on the ISO 13606-4 standard and RBAC based models. This section presents the characteristics that were integrated within the new model and why.

2.1 The ISO 13606-4

The ISO 13606 describes the privilege methodology to be used in order to specify the access control to an EHR. The part 4 of this standard (ISO 13606-4) expresses also the **record components** that an EHR may integrate such as: Personal Care; Privileged Care; Clinical Care; Clinical Management and Care Management. It also describes which **functional roles** (Subject of Care; Subject of Care Agent; Personal Healthcare Professional; Privilege Healthcare Professional; Healthcare Professional; Health-related Professional; Administrator) can access those record components. When the system needs to reach an access decision it should use a table similar to Table 1. This table defines the basis for how sensitivity levels and functional roles can be mapped. For a specific functional role the information requester may have, access permissions that are associated accordingly.

2.2 NIST RBAC

The National Institute of Standards and Technology (NIST) proposed the Role Based Access Control model (Sandhu et al., 2000) integrating the Core RBAC, and later the Hierarchical RBAC, and Constrained RBAC, which includes Separation of Duties (SoD).

The **Core RBAC** recognizes five administrative elements: Users (U), Roles (ROLES) and Permissions (PRMS), where permissions are composed of Operations (OPS) applied to Objects (OBS). The most basic of the relations are **User-Assignment** (UA), and **Permission-Assignment** (PA).

The **Hierarchical RBAC** integrates the hierarchy concept, which is mathematically a partial order defining a seniority relation between roles, whereby senior roles acquire the permissions of their juniors, and junior roles acquire the user membership of their seniors. The role inheritance relation creates a third kind of authorization in addition to UA and PA authorizations (Ferraiolo et al., 2007). If a role A inherits role B, it means that all of B's permissions are available via role A. In the new proposed model, the functional roles described in Table 1 were organized into 3 main groups: subject of care (Group I), healthcare professionals (Group II) and administrative access (Group III) (see Figure 1). This later Group should not be confused with the description presented in Section 2.2.3 with the definition of RBAC management and roles to administer and define the access control rules. The administrators of Group III, Figure 1, are related to the administrative personnel of the healthcare institutions that manage mainly care management data as specified in Table 1.

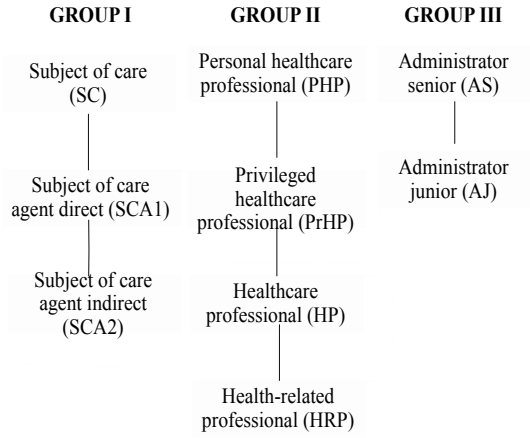

Figure 1: Hierarchical functional roles divided into 3 groups.

Another important concept to include in the new model is the **Separation of Duties** (SoD) concept. The U.S. Office of Management and Budget's Circular A-123 define SoD as key duties and responsibilities in authorizing, processing, recording, and reviewing official agency transactions that should be separated among individuals. SoD are divided in two large categories: static and dynamic.

In **Static Separation of Duty** (SSD) if a user is assigned to one role, the user is prohibited from being a member of a second role (Ferraiolo et al., 2007). SSD will integrate the new patient authorization because the user will only be able to use one exclusive role per session in order to avoid conflicts between functional roles.

With **Dynamic Separation of Duty** (DSD) users may be authorized for roles that may conflict, but limitations are imposed while the user is actively logged onto the system (Ferraiolo et al., 2007).

2.2.1 Break the Glass access

The Break the Glass (BTG) option can be used in order to break or override the access controls in a controlled manner. This should allow a user to override the access control rules stated by the access control manager and access what he requests, even though he was not previously authorized to do it. When this is done, other BTG rules come into play which may monitor, record or report the user´s actions, thus making him responsible and oblige him to justify what he did (Ferreira et al., 2009).

Characteristics from the BTG-RBAC model are included within this proposal. This way, the BTG access will be activated whenever a user tries to access resources with a role that does not include the permissions to do it. When the BTG access is activated the healthcare professional can access what he/she requested but being alerted for the fact that he/she does not have access and that responsible parties (mostly the patients or someone defined by the patient) will be informed and can later ask for

Table 1: Mapping of functional roles in record_component sensivity. Adapted from (ISO/TS-13606, 2009)

		RECORD_COMPONENT sensitivity				
	Functional Role	**Care management**	**Clinical management**	**Clinical care**	**Privileged care**	**Personal care**
Group I	Subject of care	Y	Y	Y	Y	Y
	Subject of care agent	Y	Y	Y	Y	Y
Group II	Personal healthcare professional	Y	Y	Y	Y	Y
	Privileged healthcare professional	Y	Y	Y	Y+	++
	Healthcare professional	Y	Y	Y		
	Health-related professional	Y	Y			
Group III	Administrator	Y				

NOTE 1 Y indicates that access will be granted to RECORD_COMPONENTs of this sensitivity unless otherwise dictated by other policy constraints, as specified according to clause 7 of this part standard.

NOTE 2 + Indicates that access will be granted if the EHR Recipient is a member of the same speciality or clinical service as that in which the RECORD_COMPONENT was created e.g. sexual health clinic, prison health service (as specified in the service_setting attribute for the composer of the COMPOSITION in the Reference Model of Part 1). This access may also be granted in health care 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, such as in the armed forces of some countries.

justification.

2.2.2 Temporal Constraints

The Generalized Temporal Role Based Access Control (GTRBAC) (Joshi et al., 2002) model introduces a set of language constructs for the specification of temporal constraints on roles, including constraints permissions. These constraints are also included within the new patient authorization model in order to restrict access to Groups II and III in terms of temporal duration, for instance, during the healthcare professionals' shift.

2.2.3 RBAC Management

The management of large RBAC systems remains a challenging open problem, because some of these systems may have hundreds of roles and tens of thousands of users (Ninghui and Ziqing, 2007).

There is a significant gap between the RBAC administration models developed by researchers, namely the ARBAC family (Ravi and Venkata, 1999), (Ravi et al., 1999), (Sejong and Ravi, 2002) and SARBAC (Jason, 2002), (Jason and George, 2003). Several existing approaches to RBAC administration use role hierarchies to specify administration domain, e.g. of administrators roles are senior-most role (Director) and junior-most role (Employee). These role hierarchies are similar to the previous described hierarchies (Sejong and Ravi, 2002). In the new model, the role of manager/administrator of the roles and permissions of an EHR is associated with the patient of that EHR. The patient will actively manage the roles and permissions as well as give permissions of administration to other roles, if necessary.

3 RESULTS

The new patient authorization model is described within a **Patient's Healthcare Network** (PHN). The concept of PHN refers to all the healthcare institutions that the patient usually attends as well as health centers, referral hospitals, private hospitals, commercial laboratories and health insurers (see Figure 2). It is important to define the institutions where the patient attends consultations and treatments because only the professionals that work in these institutions should usually have access to that patient's EHR. All professionals outside of the PHN are normally excluded from access to the EHR of the patient. However, the patient can define, within his/her model, a temporary role for healthcare professionals outside that PHN to access their EHR

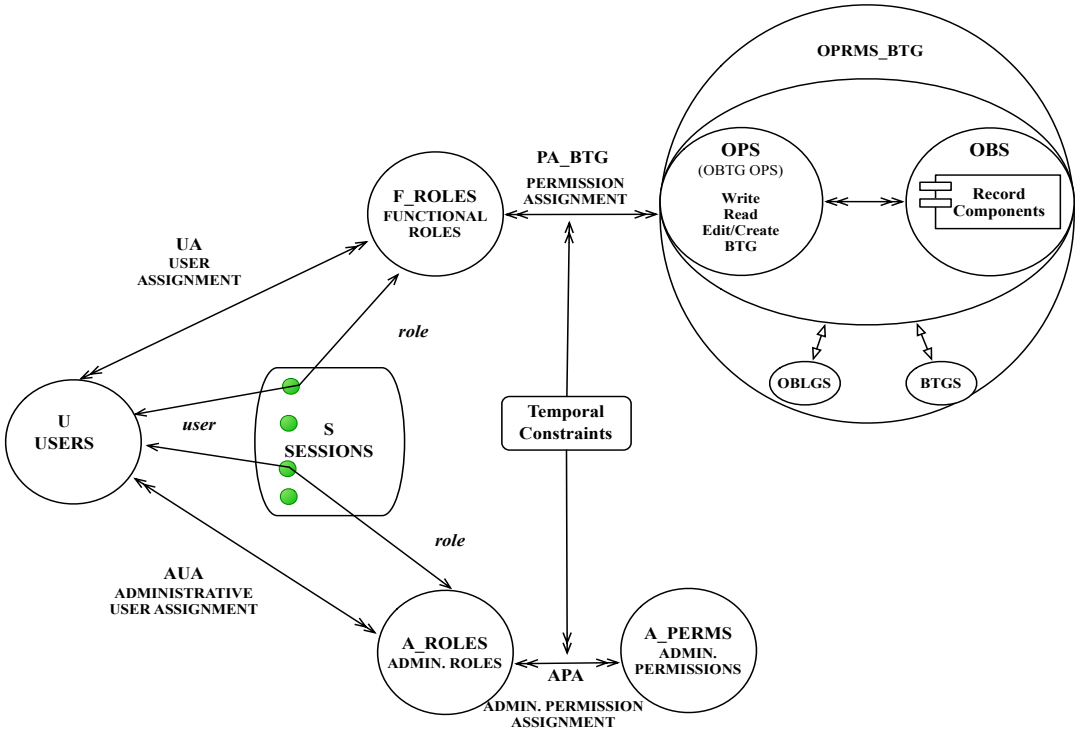

Figure 2: Architecture of the proposed patient authorization model based on (Sandhu et al., 2000), (Ravi et al., 1999), (Ferreira et al., 2009) and (Joshi et al., 2002).

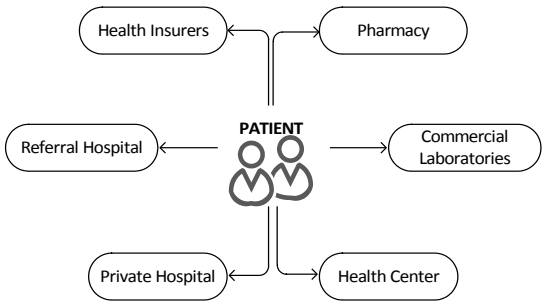

Figure 3: Patient's Healthcare Network.

in a predefined period of time, preferably in their presence.

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

Figure 3 presents the architecture of the proposed authorisation model as the integration of several other models (Sandhu et al., 2000), (Ravi et al., 1999), (Ferreira et al., 2009) and (Joshi et al., 2002). The new model integrates both the specification of access and the definition of permissions to access. It puts the user in the centre of these operations. But

Table 2: Example of two storyboards with the permissions to access an EHR defined by the patient.

	Record components	***Pre-requisite constraints***	***Operations***	***BTG option***	***Temporal constraints***
Functional role: Privileged Healthcare Professional (PrHP) **Role:** Temporary Privileged Healthcare Professional (TPrHP) **User**: Patient is the intermediary of GP to perform the authentication for this role	**DM II**	none	read	no	Available during 1h
	CB	Only ophthalmological team	none	no	none
	PenA	none	read	no	Available during 1h
	AMD	Only ophthalmological team	none	no	none
Functional role: Subject of care agent direct (SCA1) **Role**: Patient' son (PS) **User**: Robert Adams	**DM II**	Only Group II	none	yes	no
	CB	Only oftalmological team	read	no	no
	PenA	none	read	no	no
	AMD	Only oftalmological team	none	no	no
	DD	none	read AND write	no	no
	Subject of Care area	Only GP and subject of care	none	no	no

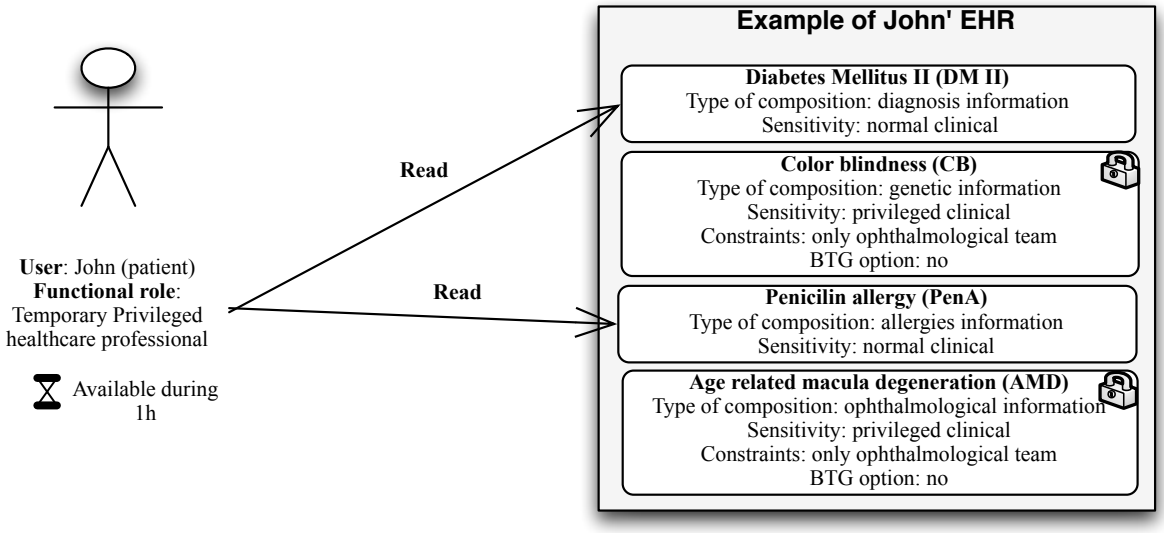

Figure 4: Use case 1 relating storyboard 1.

only the functional role *subject of care* can access both parts.

To better understand how the new model can work in real practice Table 2 presents two storyboards examples of how a patient mapped the permissions to two functional roles precisely to roles. One of the roles is the role **temporary privileged healthcare professional**.

Whenever the patient wants to allow a temporary access to a healthcare professional that is not within his PHN he/she activates this role (storyboard 1).

Storyboard 1: *John is 59 years old and he resides in Porto, Portugal. During his holidays in the Algarve John feels sick with fever and cough. He goes to the hospital in Faro and the doctor that treats him has no access to John's EHR because he is not within his PHN. The patient has previously defined the role* ***temporary privileged healthcare professional*** *and accesses his EHR with this role. Since John will be the one to introduce the authentication credentials, he decides to use a two-factor authentication with a smartcard, to guarantee that his credentials are not breached. After a successful authentication John proceeds normally to choose the role available from a list of roles, in this case the role TPrHP. Now the healthcare professional attending the patient has permissions to access the information that the patient defined for that role, and therefore assist in his treatment during a specified period of time.*

Figure 4 illustrates the use-case relating to storyboard 1. Since the healthcare professional did not have access to the patient's EHR, the patient can access the system by previously defining the role he wants to use for that session. In this use-case, the patient chose the role *temporary privileged healthcare professional* and gave temporary access to the healthcare professional that was treating him at that time. The professional can only access (read-only) components DM II and PenA of the EHR. The role *TPrHP* has not permission to perform BTG in any other component of the record so the healthcare professional does not even know of other components' existence. As the new authorization model allows temporal constraints, since this is a temporary role, John associated a limited timeframe to be used (only 1h).

The second role is the Patient' Son (*PS*) which belongs to functional role **subject of care direct** (*SC1*), and where the patient can associate his/her most direct relatives such as a son/daughter or a parent (storyboard 2).

Storyboard 2: *John is 59 years old and his son suspects he has Diabetes Mellitus and is not treating this condition and taking all the proper care and medications that were prescribed by John's GP. The son accesses John's EHR using the role (PS), whose permissions were previously defined by his father.*

These permissions are described in use-case 2 (Figure 5) and include the following components: read-only CB and PenA, as well as read and alter the DA component. The contents of the component AMD and the subject of care area are restricted and not visible to the role *PS*. However, the component DM II is visible to the role *PS* and John's son can see that this component exists but has no immediate

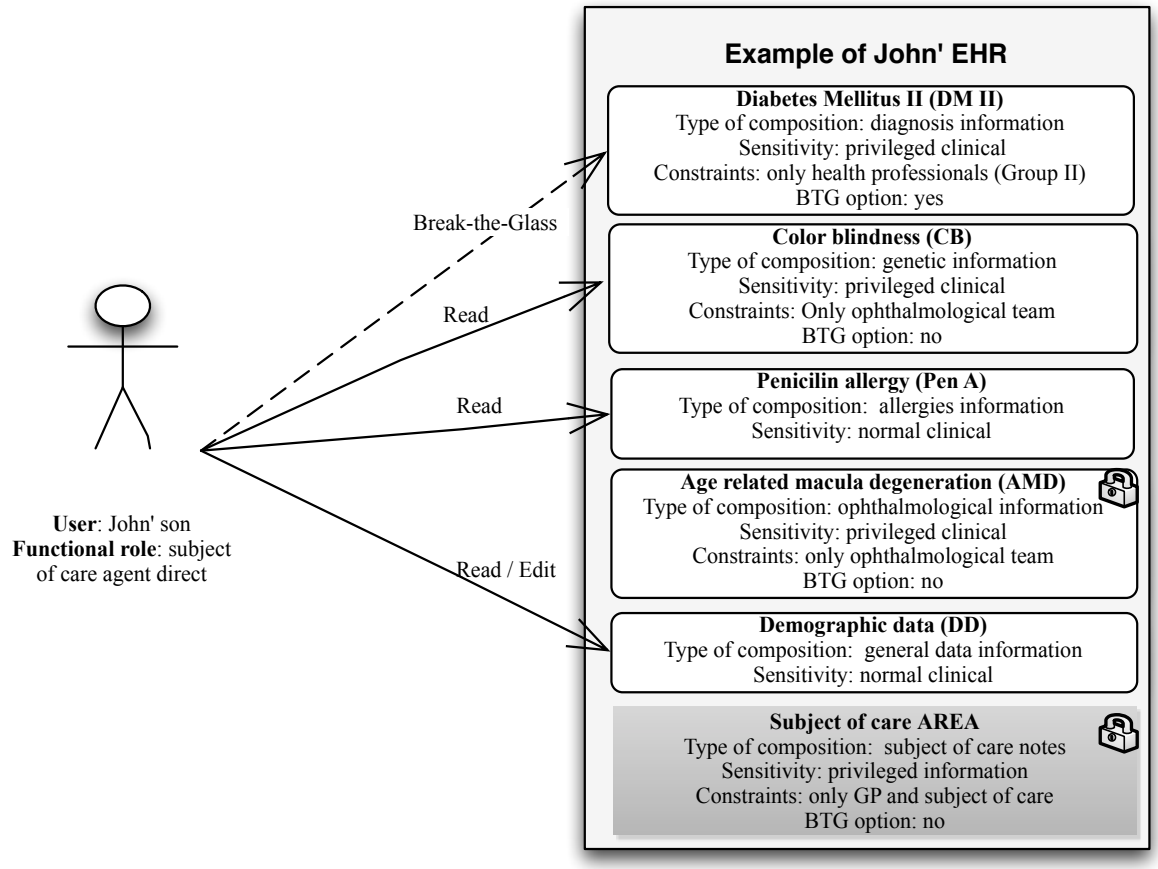

Figure 5: Use case 2 relating storyboard 2.

access to its content. He can perform BTG on this component if he really needs to access it as defined within the model by his father. If he performs the BTG on this component, the patient and other responsible parties that were defined by the patient, will be notified of this BTG action and in what components of his EHR they were performed. The patient can, after the fact, require further justifications.

4 DISCUSSION

In the first use-case scenario presented in this paper, with the use of the role *temporary privileged healthcare professional,* the healthcare professional does not belong to the patient's network of care so he would have to blindly treat the patient as a newcomer, without previous information. The new patient authorization model allows the healthcare professional to have a minimum information content that can help in a faster and more successful patient treatment. The patient would have defined this role previously so that it could be used in such a case. As this is a temporary role, a temporary session is created so that once the patient is consulted and treated, his/her privacy remains and that same healthcare professional that treated him/her cannot re-access the same EHR.

In the second use-case scenario the patient's son is allowed to access some components of the father's EHR. Other parts can be invisible to the role *PS* or they can be visible but not accessible. These can be associated with the permission to BTG. This allows more flexibility, as it can, sometimes, be the difference between better or worse patient treatment or even between life and death.

Additionally, the patient can also have his/her personal restricted area where he/she can write, for instance, his/her health diary, as is the case of a chronically disease patient. The patient can define that only his/her GP can have access to this component of the record.

The proposed patient authorization model allows for a greater participation, responsibility and control over information security and contents of his/her EHR. This model is innovative as it allows the

patient to define access control permissions within his PHN but also outside this network when necessary, providing a better healthcare treatment at the point of care. The functional roles subject of care agent direct (*SCA1*) and indirect (*SCA2*) can also be beneficial because they can allow patients' relatives to also take part and help in their treatment. Furthermore, these can help treating patients' relatives when, for example, they can have access to relevant genetic information about their parents or other relatives. Even if this information is not directly accessible, those functional roles could have the BTG permission to access it and the owner of the EHR would always be notified of the actions performed within his/her EHR.

The flexibility of access and definition of access by the patient is not meant to invade or compromise healthcare professionals' workflows or privacy as there will be a restricted area (EHR component) only to be used and accessed by that healthcare professional. It is a reserved area that can be associated to the role where the healthcare professionals can write their personal notes and information about that patient. The temporal constraint with the separation of duties integrated within the authorization model allows to define the level of patients' privacy as fine-grained as the patient desires.

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

Moreover, on the opposite note, access to most of his/her record may affect negatively the patient, as he/she cannot have the option to choose what to see and know. Again, the option of using this proposed model centered on the patient, could be given to pat ients themselves, and they could decide whether they want to know and control their EHR.

5 CONCLUSION

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

6 FUTURE WORK

Future work includes the implementation and evaluation of the proposed authorization model with a specific case study in real healthcare practice. Another important addition to this model will be the definition and association of access control permissions directly to users and not only to generic roles. This allows for exceptions to be made inside the group of functional roles and a more fine-grained and even personalized access control definition.

ACKNOWLEDGEMENTS

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

REFERENCES

Beimel, D. ,Peleg, M. 2009. The Context and the SitBAC Models for Privacy Preservation – An Experimental Comparison of Model Comprehension and Synthesis. IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING.

Ferraiolo, D. F., Kuhn, D. R. ,Chandramouli, R. 2007. *Role-Based Access Control*, Artech House.

Ferreira, A., Chadwick, D., Zao, G., Farinha, P., Correia, R., Chilro, R. ,Antunes, L. 2009. How securely break into RBAC: the BTG-RBAC model. *Proceedings from 25th Annual Computer Security Applications Conference - ACSAC2009*.

Ferreira, A., Cruz-Correia, R., Antunes, L. ,Chadwick, D. 2007. Access Control: how can it improve

patients' healthcare? . *Stud Health Technol Inform,* 127**,** 65-76.

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

HIPAA 1996. Health Insurance Portability and Accountability Act *In:* SERVICES, U. S. D. O. H. H. (ed.).

ISO/TS-13606 2009. Health informatics - Electronic health record communication *Part 4: Security.* ISO/TC.

Jason, C. 2002. Administrative scope and role hierarchy operations. *Proceedings of the seventh ACM symposium on Access control models and technologies, 1-58113-496-7.* Monterey, California, USA: ACM.

Jason, C. ,George, L. 2003. Administrative scope: A foundation for role-based administrative models. *ACM Trans. Inf. Syst. Secur.,1094-9224,* 6**,** 201-231.

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

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

Ninghui, L. ,Ziqing, M. 2007. Administration in role-based access control. *Proceedings of the 2nd ACM symposium on Information, computer and communications security, 1-59593-574-6.* Singapore: ACM.

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

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

Ravi, S. ,Venkata, B. 1999. Role-based administration of user-role assignment: The URA97 model and its Oracle implementation. *J. Comput. Secur. 0926-227,* 7**,** 317-342.

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

Rec97 1997. Protection of Medical Data - Recommendation nºR (97) 5. *In:* STATES, C. O. M. T. M. (ed.). Europe.

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

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

Sandhu, R. S. 1998. Role-based Access Control. *In:* MARVIN, V. Z. (ed.) *Advances in Computers.* Elsevier.

Santos-Pereira, C. 2011. *Design of "valet key" autorizathions mechanisms.* MSc in Biomedical Informatics, Faculdade de Medicina da Universidade do Porto. (in writting).

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

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

U.PORTO
FMUP FACULDADE DE MEDICINA
UNIVERSIDADE DO PORTO

U.PORTO
FC FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO