Grounding Information Security in Healthcare

Ana Ferreira[acd], Ricardo Correia[bd], David Chadwick[a], Luis Antunes[cd]

[a]Computing Laboratory, University of Kent, CT2 7NF Canterbury, Kent, UK.

[b]Biostatistics and Medical Informatics Department, Faculty of Medicine, Al. Prof. Hernâni Monteiro, 4200-319 Porto, Portugal

[c]Instituto de Telecomunicações, Faculdade de Ciências da Universidade do Porto, 4169-007 Porto, Portugal

[d]CINTESIS – Center for research in health information Systems and technologies, Faculty of Medicine, Al. Prof. Hernâni Monteiro, 4200-319 Porto, Portugal

Ana Ferreira. Computing Laboratory, University of Kent, CT2 7NF Canterbury, Kent, UK. af84@kent.ac.uk. Telf: +44 1227 824180, Fax: +44 1227 762811.

Abstract

Purpose

The objective of this paper is to show that grounded theory (GT), together with mixed methods, can be used to involve healthcare professionals in the design and definition of access control policies to EMR systems.

Methods

The mixed methods applied for this research included, in this sequence, focus groups (main qualitative method that used grounded theory for the data analysis) and structured questionnaires (secondary quantitative method).

Results

Results showed that the presented methodology can be used to involve healthcare professionals in the definition of access control policies to EMR systems and explore these issues in a diversified and integrated way. The methodology allowed for the generation of great amounts of data in the beginning of the study and in a short time span. Results from the applied methodology revealed a first glimpse of the theories to be generated and integrated, with future research, into the access control policies.

Conclusions

The methodological research described in this paper is very rarely, if ever, applied in developing security tools such as access control. Nevertheless, it can be an effective way of involving healthcare professionals in the definition of access control policies and in making information security more grounded into their workflows and daily practices.

Keywords: information security; access control; access control policy; electronic medical record; grounded theory; mixed methods.

1. Introduction

Information security is usually defined by three main characteristics: confidentiality - the prevention of unauthorized disclosure of information; integrity - the prevention of unauthorized modification of information; and availability - the prevention of unauthorised withholding of information or resources [1, 2].

In order to access information within a system there are usually 3 steps: identification – where users say who they are (e.g. with a unique username); authentication – where users prove they are who they say they are (e.g. using a password or PIN number); and authorisation – where access rights are given to the users. Authorisation can usually only occur after the first two steps have been successfully completed, and it checks if users have all the required privileges to access the resources they requested. Access control is part of the authorisation process that checks if users may access the resources they asked for. So it focuses on the interaction between users and technology, aiming to provide information confidentiality without compromising information availability.

The introduction of Electronic Medical Record (EMR) systems within healthcare organizations has allowed the integration of heterogeneous patient information that was usually scattered over different locations [3, 4]. EMR has become an essential source of information and an important support tool for healthcare professionals (HCP). However, there are some barriers that prevent the effective integration of EMR within the healthcare practice. These barriers can be grouped in terms of: time/cost, relational issues and educational needs [5, 6]. Time and cost barriers include the cost of EMR integration and the time healthcare professionals need to spend learning how to use the system. The relational barrier includes the perceptions that physicians and patients have about the use of EMR and how their relationship may be affected by its use (during a consultation, for example). The educational barrier comprises the lack of proficiency and difficulties that HCP have in interacting with EMR systems in order to perform their daily tasks [7].

HCP do not usually participate in the design and development of EMR systems (specifically in the access control function), so they usually have to change their workflow patterns and adapt their procedures and processes in order to access EMR systems within their practices [8]. This is very challenging as well as time and cost consuming [6]. Within healthcare, access to sensitive information is usually required by different professionals (e.g. GPs, doctors, nurses, administrative personnel) so access control to EMR can be very complex and hard to define and implement properly, and should start with the definition of structured and formal access control policies as well as access control models [9]. Ultimately, access control is closely related to the definition of a system's workflow how the system is to be used and how the tasks are to be

performed. Access control policies define who the actors of the system are and what they can access and do within the system. If access control in EMR can be closer to healthcare professionals' needs then some of the identified problems can be minimised, helping to ensure that EMR can be more effectively implemented and used and provide for better healthcare [8].

The objective of this paper is to show that grounded theory (GT) – a methodology that is very rarely, if ever applied in developing security tools such as access control – together with mixed methods, can be used to effectively involve HCP in the design and definition of access control policies for EMR systems.

The next Section presents the concept of grounded theory, mixed methods and their importance in this context; Section 3 introduces the methodology applied within this study while Section 4 presents the results of applying that same methodology. Section 5 discusses some of the results and presents the lessons learned from applying the research approach described here. It also discusses the limitations and areas of future research. Section 6 presents some concluding remarks.

2. Grounded Theory and Mixed Methods

Grounded theory is a research approach that focuses on developing theory from the qualitative analysis of data without any particular commitment at the outset to any specific kinds of data, lines of research or theoretical interests [10]. Instead of identifying a data sample at the outset, GT involves the process of theoretical sampling of successive sites and data sources, selected to test or refine new ideas as they emerge from the data. GT relies mainly on qualitative data acquired through a variety of methods such as observation and unstructured interviews in the initial stages and then more structured forms of data collection as the study becomes more focused. GT is commonly used in social science research where social scientists try to explore all aspects of human behaviour and environment. They re-examine the social world in order to better understand or explain why and how people behave [11]. Nevertheless, GT can also be applied in other areas of research where there is a need to generate theory and ideas from research data [12].

2.1 GT in this study

Healthcare is a complex environment so it is important to understand and learn as much as possible about it by collecting qualitative data and generating theories from that data. From these theories it will be possible to formulate access control policies and rules that can describe, closer to reality, users' interactions with the EMR and then include these in the subsequent design and implementation of an access control model. GT is an appropriate approach for this study as it focuses on understanding healthcare professionals' experiences, workflows and

behaviour as well as the social context during the implementation and use of EMR.

2.2 Qualitative vs quantitative methods

Qualitative methods are usually used to refer to ones used by researchers who work as ethnographers [11] [13], clinical and organizational psychologists or sociologists. Qualitative researchers tend to focus on situational and structural contexts but are weak on cross-comparisons as they often study only single situations, organizations and institutions. Quantitative researchers on the other hand focus on multivariate situations but are weak in context [10]. At the most basic level, quantitative research involves the use of methodological techniques that represent the human experience statistically while qualitative research provides detailed descriptions and analysis of the quality or substance of the human experience [11].

Table 1 - Differences between qualitative and quantitative methods [14].

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

2.3 Mixed methods' research

Despite the fact that there is a clear distinction between qualitative (theory generation) and quantitative (theory testing) methods, there is also much overlap both in practice and theory. So these methodologies should not be seen as orthogonal. They are similar in that they are both built on empirical or observable reality and regardless of their methodological and theoretical differences researchers agree that social research should be about the real world.

Some researchers opt for the use of mixed methods which combines both qualitative and quantitative techniques. Mixed methods research refers to those studies or lines of inquiry that integrate one or more qualitative and quantitative techniques for data collection and/or analysis [15]. Although mixed methods can lead to different and sometimes conflicting results, they can

be a rich source of discussion and can enhance the robustness of the study. Such results may also lead to different conclusions from those that would have been drawn from relying on one method alone and this demonstrates the value of collecting both types of data within a single study [16]. Combining methods may generate deeper insights than each method applied alone and can activate their complementary strengths and help to overcome their discrete weaknesses. The principle of complementarity relies on using the strengths of one method to enhance the other [17]. Each new set of data increases the confidence that the research results reflect reality rather than a methodological error. Divergent findings are equally important because they signal the need to analyze a research problem further and to be cautious in interpreting the significance of any set of data [18].

2.4 Mixed methods in this study

The complementarity of mixed methods will produce richer data and provide different views and experiences for the subject to be explored. GT is the most appropriate method to start the study, since it can generate various theories to be translated into access control rules and policies that are closer to end users' needs. The application of a smaller quantitative method afterwards will guarantee that those theories will be either confirmed or confronted. The latter can be further analysed to assure that the final data is the most accurate and closer to reality.

According to the priority-sequence model presented in Table 2 and the research objectives of this work we chose a smaller quantitative study to evaluate and interpret the results from a larger qualitative study (last row of Table 2 - QUAL→quant). The quantitative method provides a means to expand on what was learned through the main qualitative study. The classic use of this design is to explore the generalisability or transferability of conclusions from the qualitative research. Even a small quantitative follow-up can typically cover a much larger sample or range of setting than were present in the initial, in-depth qualitative research [17].

Table 2 – The priority-sequence model: complementary combinations of qualitative and quantitative methods. The priority decision is described by capital letters and the sequence decision by the arrow → (i.e. qual→QUANT means that the most important method is quantitative while in sequence the qualitative method is applied first) [17].

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

3. Methods

The selected methods chosen for this research comprised focus groups (the main qualitative study) followed by structured questionnaires (subsequent quantitative study). Focus groups were chosen because they better adapt to the objectives of this research – they are the most appropriate qualitative method when we need to assess different professionals' views and

experiences. They generate large amounts of qualitative information from only one discussion and in a relatively short period of time. It is difficult to perform observation studies in a HCP's working place because it is a very eclectic environment and it is not so easy to arrange in a short timescale. Structured questionnaires were chosen to complement the main qualitative study because they can be left with the HCPs for them to fill out in their own time without causing them too much stress or interfering with their busy schedules. The questionnaires can also further explore issues that came up during the focus groups' discussions in order to either complement or confront that data.

3.1 Focus Groups with HCPs

The main objective of focus groups (FG) is to gather opinions and experiences related to specific topics. This is obtained through sampling groups (6 to 8 people) of the required population, who meet to discuss a set of topics amongst themselves. The discussion can last on average from one to one and a half hours, and is guided by a skilled moderator who records the discussions. The data is first transcribed and then analysed in a qualitative manner.

3.1.1 Population

The selection of participants was made from postgraduate students at the Faculty of Medicine of the University of Porto. Students were chosen from the following Masters Courses: Medical Informatics and Evidence and Decision in Healthcare; and from the Doctoral Program Clinical and Healthcare Services Research. Both HCPs and informatics' professionals are enrolled on the Masters Courses, but only HCPs were selected and put into groups according to their professional background. One of these groups however had HCPs with mixed backgrounds. The doctoral program only enrols medical doctors and so these comprised one of the groups. The reason for grouping participants according to professional backgrounds (i.e. segmentation) facilitates discussions because all the participants in a group have similar experiences and backgrounds, usually at the same level [19].

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

3.1.2 Line of Discussion

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

1. The participants were given the main theme to discuss and other information regarding the process that would be followed during the course of the focus group. Each participant was asked to give their consent to participating.

2. Each participant was initially asked to give details about their profession and work location, as well as the use of EMR within their practice.
3. After that they were all asked to discuss amongst themselves:
    a. The use of paper records or EMR, what are the advantages or disadvantages of each
    b. access control issues in general
    c. access control mechanisms they use on a daily basis when accessing any system
    d. the problems and benefits of giving different access levels to different groups of users
    e. access control policies to EMR: who defines them, what should be improved

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

3.1.3 Data collection and analysis

Data was collected by audio recording the whole conversation while the conversations of the third and fourth group were also recorded with a video camera.

Table 3 – Description of each FG data collection

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

Regarding the analysis, only one person was involved during the whole process. The discussions from each focus group were transcribed into 4 separate word documents. Each document was then divided into smaller ones, containing only the dialogues belonging to each one of the participants, so that the data could be more easily related to a specific participant.

All documents were inserted into the qualitative analysis software, QSR NVivo 7 [20], and the coding was done using this tool to register and structure data in a more automatic way. The coding started after each focus group document was generated and was done separately for each group.

Discussion topic, categories and sub-categories that were generated from each group were not only used in the categorisation of subsequent group discussions but were also back categorised to the previous ones (where applicable).

The data analysis was performed in four phases. In the first phase, codes were generated from the data itself (in vivo coding), using a line-by-line coding strategy. These codes comprise the core ideas that were found within the text. Line-by-line coding helps to identify gaps, define actions and explicate both actions and meanings and leads to developing theoretical categories [21]. On a second phase, a more focused and structured coding was done and codes started to fit and be grouped into categories. The third phase was based on axial coding where relations between categories and sub-categories became more visible and so they were organized as such (see Figure 1). Phase 4 was customized and oriented to the objectives of this research and consisted in the generation of access control theories that could be integrated in an access control model in future research.

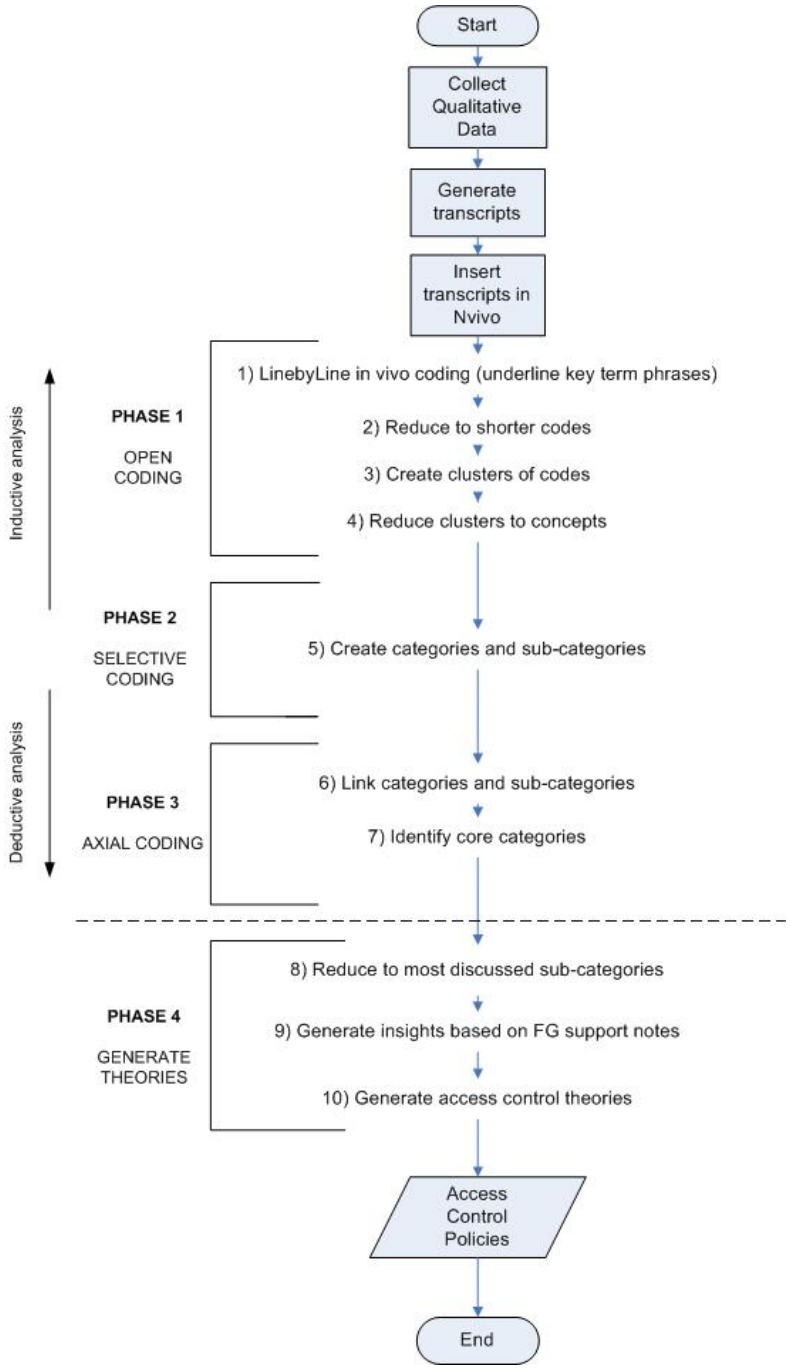

Figure 1 – Phases of data analysis for the focus groups.

Theoretical sampling was not incorporated in this study due to time and resources constraints so the GT approach used in this study was applied to data analysis and not to data collection. Also, theories achieved within this study are substantive theories because they evolved from the study of phenomenon from a particular situational context.

3.2 Structured Questionnaires to HCP

These are questionnaires containing different sets of questions, organized in a specific order. A

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

The data is analysed quantitatively.

3.2.1 Construction of the questionnaire

Questions were constructed based directly on the categories resulting from the focus groups, with the exception of Section 3 where the topics were related to legislation and patient rights to access their medical record. Section 3 also contained questions about a hypothetical scenario.

3.2.2 Population

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

Healthcare professionals from different healthcare institutions and backgrounds were approached in a random fashion at their working place during working hours. They were asked to answer the questionnaire and they could either refuse to do it, do it immediately or do it later in their own time.

3.2.3 Data collection and analysis

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

4. Results

4.1 The Methodology

A total of 53 healthcare professionals (23 medical doctors, 17 health technicians and 13 nurses) were involved in the discussion and definition of access control policies for EMR systems. 32 participants were female while 21 were male. Only 4 participants of the focus groups were also participants in the questionnaire, all the other participants were different. Both studies were performed within the course of a year (between January 2008 and January 2009).

The results showed that the presented methodology can be used to effectively involve healthcare professionals in the definition of access control policies for EMR systems. The methodology allowed us to explore issues related to access control and users' perspectives and experiences in a diversified and integrated way; diversified because data was generated using different collection methods, with different goals, and integrated because both methods were interconnected and complemented each other in the way they were applied.

The methodology generated large amounts of data within a short time span at the beginning of

the study, and this allowed for a more focused analysis of specific issues later.

The following section presents an initial set of results obtained from the appliance of each method.

4.2 Preliminary results from the mixed methods

4.2.1 Focus groups

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

Table 4 – Healthcare institutions for the focus groups' participants.

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

Figure 2 presents the results obtained from each step of the analysis whilst Figure 3 describes the categories/sub-categories that were generated from the qualitative data collected from each focus group. The categories are sorted alphabetically and newly generated categories from the different focus groups are marked in a different colour. The 8 core categories represented in Figure 3 (from step 7 of the analysis) are: access by patients; access control; access control levels; access control policies; access control solutions; access in emergency situations; paper vs digital; and security.

[1] Organizations that integrate more than 2 hospitals.

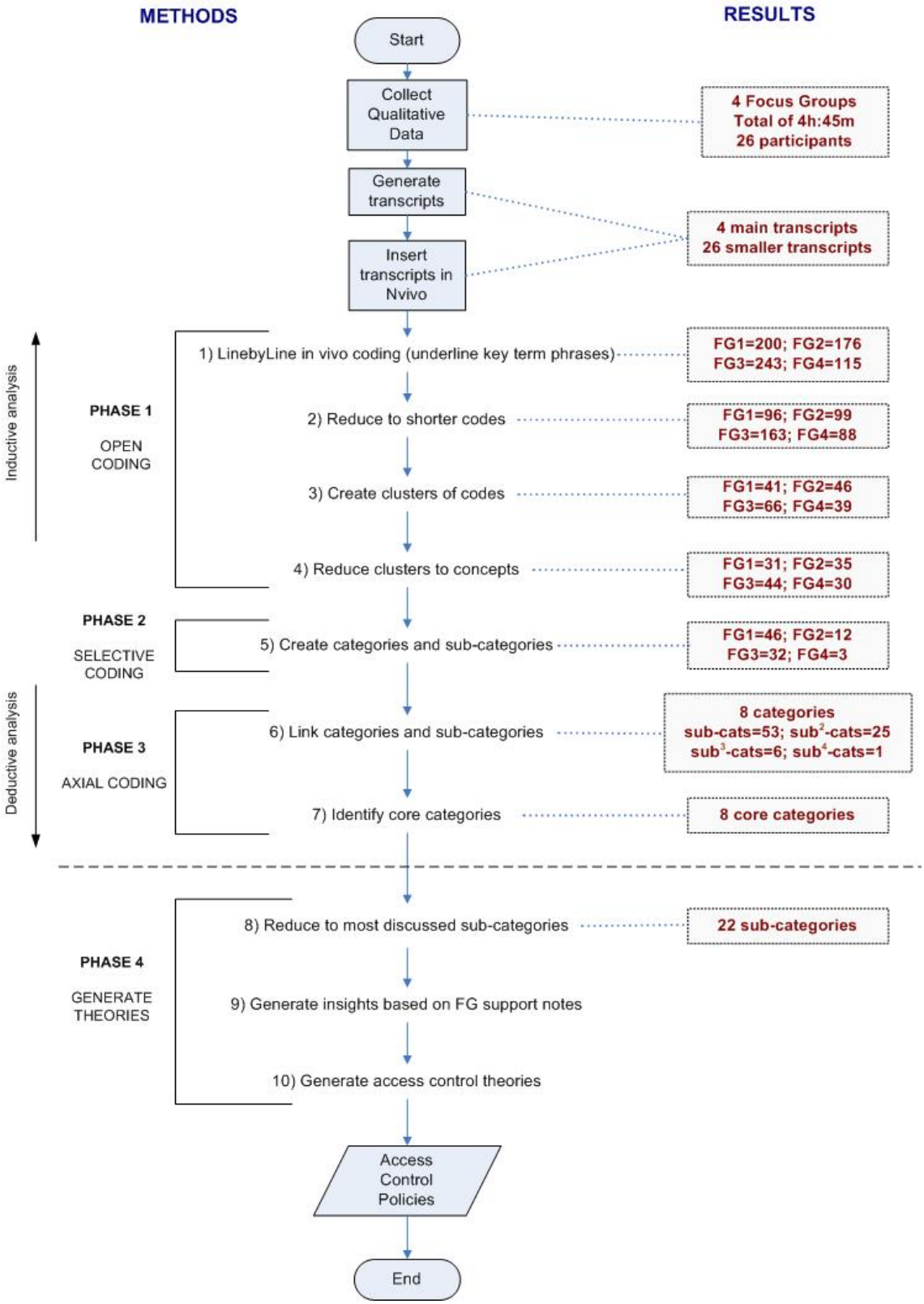

Figure 2 – Results for each step of the analysis.

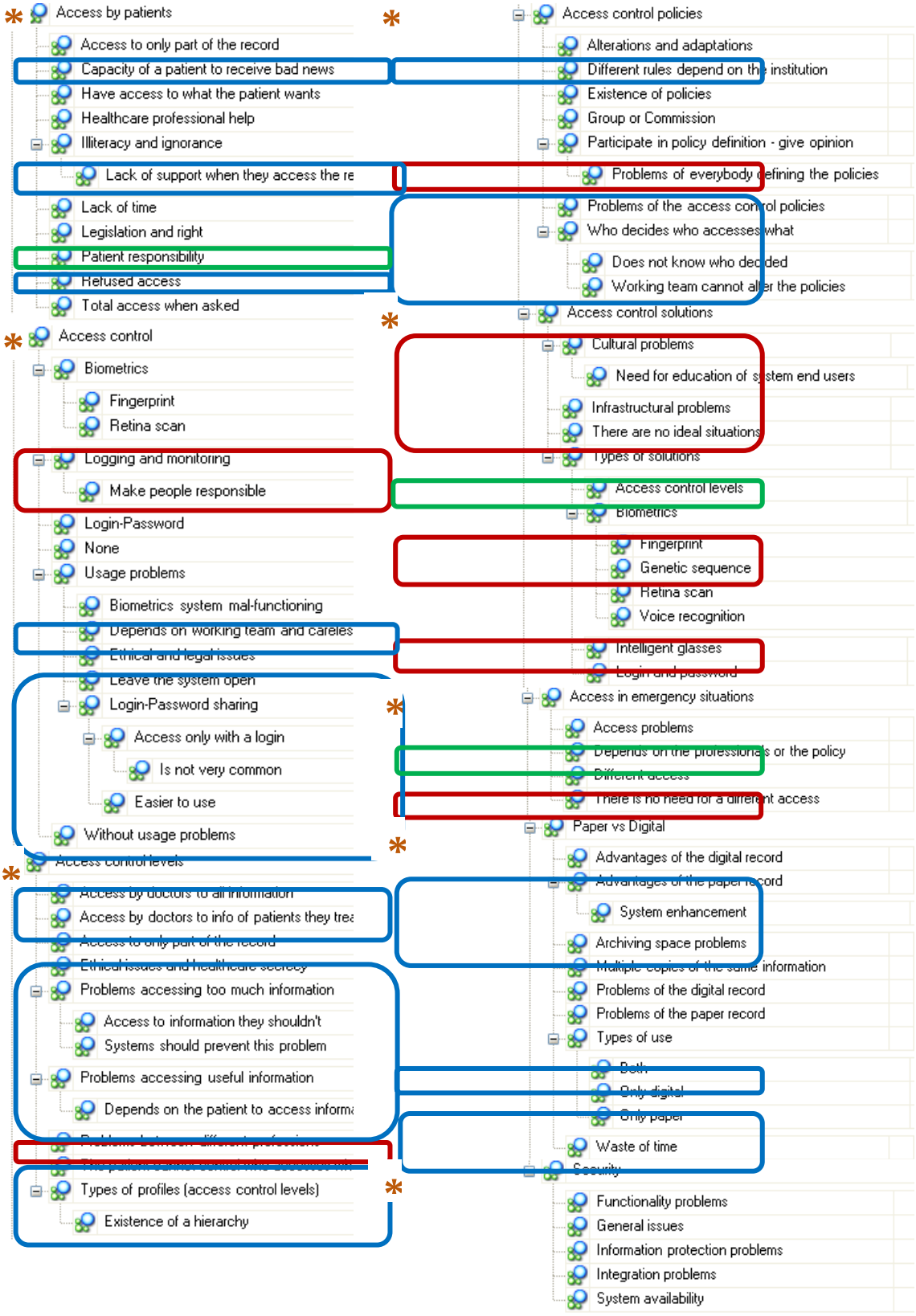

Figure 3- Category/sub-category generation from the 4 focus groups. FG1 are not marked; FG2 generated categories are in ——; FG3 generated categories are in ——; FG4 generated categories are in —— ;

From a closer analysis of the transcripts the most common themes in the discussions (generated in step 8 of the analysis) are presented in Table 5 (PP=No of different people discussing the topic; TR=total number of references to the category). Participants discuss those themes both in negative or positive terms, this degree is categorised accordingly in the shown sub-categories (see Figure 3).

Table 5 - Most discussed categories in the 4 FGs (n=26).

Main categories	PP	TR	Most mentioned sub-categories	PP
Access control	100	146	Login-password	18
			Usage problems	18
			Share logins-passwords	16
Access control policies	75	125	Problems with the policies	16
			Alterations and adaptations	12
			Participate in the policy definition and give opinion	14
Access by patients	61	98	Require HCP support	9
			Illiteracy and ignorance	11
			Legislation and rights	11
Access control levels	59	99	Problems of accessing useful information	11
			Access to only parts of the record	9
			Problems of accessing too much information	8
Paper vs Digital records	58	100	Problems with the digital records	11
			Problems with the paper records	10
			Types of use	10
Access control solutions	48	70	Types of solutions	11
			Biometrics	11
			Fingerprint	6
Security	38	86	Functionality problems	13
			Information protection problems	6
			General issues	8
Access in emergency situations	7	11	Requires different access	4

4.2.2 Structured Questionnaires

27 valid questionnaires were received and analyzed. Questionnaires were received from medical doctors, 6 nurses and 9 healthcare professionals. 16 participants were female while 11 were male. 14 participants worked in a hospital, 5 in a health centre, 1 in a laboratory, 2 in an academic institution, 1 in a public healthcare institution and 4 in a private healthcare institution. In terms of academic education, 23 respondents had a BSc and 4 had an MSc. Also, 16 had some informatics' proficiency, 7 had had some informatics' education and 3 had had none (1 respondent did not answer this question).

The questionnaire was divided into four parts and was based on the categories generated from the focus groups discussions. The questionnaire was designed to further explore some of the issues that are more relevant to this study. Part 1 contained 9 generic questions regarding EMR; Part 2 had 11 questions regarding access control to EMR; Part 3 had 4 questions about a fictitious scenario of patients using an Automatic Teller Machine to access their medical records; and Part 4 had 7 demographic questions (see Appendix).

Table 6 – Mapping the questionnaire sections and questions to the generated categories within the FGs.

SECTION	QUESTION TOPIC	RELATED CATEGORIES	Questions
1	Generic EMR	• Access control • Access control policies • Paper vs digital • Security	{4,5,6} {7,8,9} {1,2,3,5,6} {6}
2	Access control to EMR	• Access control • Access control levels • Access control policies • Access control solutions • Access in emergency situations	{1,2,3,4} {5,6,7,8,9,10} {10} {6} {11}
3	ATM patients' access	• Access by patients	{1,2,3,4}

A summary of the analysis results is presented below.

A. Results from Part 1

The answers obtained from Part 1 of the questionnaire showed that 21 HCP had used EMR during the course of their work whilst 6 respondents never had. All the results to the questions that relate with the use of EMR focus only on those 21 professionals. More generic questions take into account the total number of respondents (27).

17 HCP used the EMR daily or almost everyday whilst 3 used EMR between 1 and 3 times per week, and 1 respondent did not know. The most common uses were Consultation 15; Data input 18; Decision support 5; Prescription 11; Emergency or Intensive Care Unit 8. Twelve respondents agreed that the EMR was very important for their work, 8 thought it was indispensable while 1 respondent considered that EMR was a necessary evil.

Although many of the participants accessed EMR on a daily basis there were still many problems associated with its use, as shown in Table 7.

Table 7 – Number of respondents for the question about EMR problems.

EMR problems	No respondents
Required previous education or training	18
EMR allows sharing of sensitive information	17
Access control can be a problem	15
Required change in tasks HCP needs to perform	13
EMR allows distributed online access to potentially anyone	7
They are not secure	6
May affect doctor-patient relationship	5
Do not trust the system	5
Wastes time of user	4
No opinion	3

In response to the question about participating in the development of EMR, 22 respondents said they had never participated in this whilst 5 said they had. When asked if they thought HCP should participate in the development of EMR, 22 respondents said they should, 3 said they should not whilst 2 did not know. When asked which parts of the development they ought to participate in, 21 said they would like to participate in the conceptualization phase; 14 in the definition of access control policies; 15 in the implementation; 16 in the testing process; and 2 did not know.

B. Results from Part 2

The second set of questions focused on controlling access to the EMR. 19 respondents said they logged in to the EMR with a password, 4 of whom used passwords together with biometrics. 1 respondent used biometrics alone, 1 did not use any kind of mechanism. The respondents were asked what the most common issues when authenticating to the EMR with username and password were. Table 8 summarises the responses.

Table 8- Issues regarding the use of login and password as authentication mechanisms

Issues of login-password	No of respondents
Accesses easily the system using a login and a password	15
Sharing passwords among users	4
Forget the password many times	2
No opinion	2

The respondents were asked about the time taken to access the EMR. 7 said that it took too long to access the EMR, whilst 14 said it did not. When asked if they had any difficulties in accessing the EMR, 4 answered never, 11 said a few times, 5 said regularly whilst 1 respondent said many times.

The respondents were then asked various questions about access control levels: should different staff be given different levels of access, did their systems support different levels of access for different staff, and if so, were these the correct levels, and finally, did the respondent participate in the setting of those access levels. 13 respondents agreed with the existence of different access control levels in general, whilst 12 agreed with this but only for some of the information in EMR, and 2 participants thought all staff should have the same level of access. 15 respondents said that their EMR had different access control levels, 3 said theirs did not support this, and 3 did not know. Further, 8 respondents said they were not the correct access levels while 5 said they were. Just 1 of the respondents said to have participated in the definition of the access control levels while 25 said they had not, and 1 respondent did not have an opinion on the subject.

Table 9 presents the responses for the types of access control levels that the participants think should be used together with what they currently do use on a regular basis.

Table 9 – What types of access control levels exist or should exist.

Types of access control level defined by	Should exist	Do exist
Professional category	19	13
Type of information (+- sensitive)	15	2
The dept where the HCP works	11	6
The patients themselves	4	0
Do not know	2	2

Finally, the respondent was asked if HCPs should be provided with access to patient information in emergency situations, and if so, when was this justified. 9 respondents answered yes but only for those professionals participating in the emergency care; 8 answered yes depending on the emergency situation; 1 participant answered yes for everybody; 1 participant said yes as long as the HCP was authorized; another participant said yes for the team that is assisting the patient at that moment; 2 respondents said yes but did not justify this; and 4 respondents said no (1 participant did not answer this question).

C. Results from Part 3

Part 3 of the questionnaire related to a fictitious scenario of patients accessing their own medical records via an AMT machine. The majority of HCPs (17) did not agree with this method of

access. When asked if ATMs were secure, 18 did not think they were, although the vast majority of the respondents (25) often use ATMs to perform their banking operations on a regular basis.

Table 10 – Access to EMR via an ATM

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

The main problems envisaged with this type of access to patients' healthcare information were: it raises ethical questions (13) and is not secure enough (13).

5 Discussion

5.1 The methodology

The use of grounded theory, together with mixed methods, applied to information security (access control in this case) is an appropriate methodology for this research as it helps in exploring healthcare professional's daily workflows, experiences, perceptions, tasks and procedures while facilitating and understanding how these may or may not affect access control and vice-versa. This knowledge is essential in order to involve healthcare professionals in the definition and improvement of access control policies to EMR. This methodological approach allowed for the collection of richer data, both contextual and statistical, so the access control issues could be explored in a diversified and integrated way. Thus, it is possible to confront what happens in practice with what should happen in an ideal world. The generation of large amounts of data over a short time period at the beginning of the study helped to get information about issues for which there is very little published information available. It also helped to direct where further exploration was needed using a more focused analysis of specific issues.

The description of the methodology we applied and our preliminary results confirm why this methodology works well for this research topic. The preliminary results provide a first glimpse of the theories that need to be generated and tested in future research about access control policies. Our first hypothesis is that a new access control model is needed for supporting HCPs who access EMRs.

5.2 Interpretation of the results

The interpretation of the preliminary results was performed by relating them to the following four categories: usability, access control levels, access control policies and emergency access.

We compared focus groups' results with the questionnaire results for the same categories.

The focus groups' results focused mostly on usability problems and the sharing of logins and passwords. Exploring these issues further, the questionnaires showed that most respondents required previous education and training and a change to the working patterns in order to use the EMRs. This is something that needs to be improved in the future, and on which further research is needed. Also, they stated that the access controls were not always well defined and a few said that the use of EMRs may affect the doctor-patient relationship. About the sharing of logins and passwords, only a small percentage said they did it (confirming what came up within the FG discussions) while the majority said they accessed the system quite easily with this authentication mechanism. The abuse of logins and passwords by a few is still an issue that needs to be further explored.

Regarding different access control levels (ALs), focus groups' participants discussed how these usually had a large effect on how HCPs can access the EMR. Discussion focused on the wrong definition of ALs. Participants were concerned about the problems of accessing too much or too little information, or which parts of the record to access. Exploring these issues further, the questionnaires revealed that access levels should be more flexible and defined not only according to the professional category of the HCP, but also by the type of information being accessed and even by the department where the HCP works. Just over half of the respondents said that they use EMR with ALs but more than a half of them concluded that the ALs were not correctly defined. As expected, almost all of the respondents said they did not participate in the definition of ALs. We conclude that ALs need to be better thought through and analysed when they are being defined. They should depend on the environmental, cultural as well as human characteristics of the system, as well as the tasks to be performed and the place where the EMR is to be deployed. We note that only a few HCPs mentioned that patients should also take part in the definition of the ALs. This is another interesting issue to pursue as patients are now legally required to give their consent for HCPs to access their EMR. This may require a large reformulation of existing EMRs, ALs and access control policies that are currently being used.

Focusing on access control policies (APs), focus groups' participants argued that they had many problems with the existing policies because they are very difficult to alter or adapt. The participants had a strong interest in participating in the definition of APs in the future as well as giving their advice to AP developers. A detailed analysis of the questionnaires showed that HCPs would mainly like to participate in the conceptualization phase of an EMR, whilst around half would be happy to participate in the testing and implementation phases of the EMR, as well as in the definition of the APs. It is worth exploring why more HCPs did not want to participate in the development of an EMR when it is obvious they have so many problems in using them

and adapting them to their daily practices.

Concerning emergency access to EMRs by HCPs, focus groups' participants raised the possibility of having a different type of access for these situations (i.e. different from what is stated in the policy for normal situations). A more detailed analysis of this issue with the questionnaires revealed that a vast majority of the respondents agree that HCPs must be able to access medical information in emergency situations even if they were not the HCP normally treating the patient. Emergency access may depend on the situation, location, type of emergency, time of access and so on. We propose that in such unanticipated situations, a "Break the Glass" policy must be created so that HCPs can temporarily have a controlled, justifiable and monitored access to the required information, and this should be integrated within the existing AP [22].

When asked about patients accessing their own medical records, focus groups' participants mainly discussed that patients had the right to do this, since it was stated in the data protection legislation, and they could not go against it. However, many HCPs were worried that this could affect their work as most patients are not ready to understand the medical record and they might require the HCPs time to help them with it. To analyse this from a different perspective the questionnaires introduced the ATM scenario. More than half of the respondents said that accessing a medical record through an ATM machine was not a good idea because it was not secure enough or raised ethical issues. It is worth exploring further why a vast majority of the respondents are willing to trust their money to the ATM machines but not the EMR information. Furthermore, the ATM solution would also allow the patients to view their EMR information using help provided by the system itself, without requiring the HCPs to spend time on this.

In summary, the results reflect the need for EMRs to come closer to the HCPs, and for the APs to better mirror the HCPs workflows and tasks. Further, there is a need to provide a more flexible and adaptable AP to the EMR for both normal and unanticipated situations. The research method described in this paper could be one way of getting more appropriate APs.

5.3 Limitations

A limitation of this study is that the analysis of all the collected data was done by just one person, due to time and also knowledge constraints. In the areas of healthcare informatics and information security there are not many experts with the combined knowledge that would qualify them to collaborate in the coding and analysis processes.

Time constraints also limited the amount of flexibility we had in arranging focus groups with the HCPs. It is very difficult to setup meetings with healthcare professionals and put them all together in the same room for at least one hour, especially when they have many variable and incompatible timetables. Setting the focus groups meetings at the time of their lectures was a

shortcut to hasten this process. To minimize the bias of this selection process, the focus groups' discussions were undertaken before any lectures whose content might have influenced their thoughts and experiences about the subject of discussion.

5.4 Further research

In or future research we plan to generate further theories and rules from a more prolonged systematic analysis of the collected data. These will then be translated into access control policies that can be integrated into a more adaptable and flexible access control model for EMR than is available today. A similar research methodology will be applied to patients so that their needs will be integrated into the same model. Patients should benefit from accessing their medical information and taking more control and responsibility for their healthcare (i.e. patient empowerment) [23].

6 Conclusions

Although GT is commonly used in social and political research as well as in medicine and nursing, published material shows that it has never been applied in the domain of access control to EMR (which integrates 3 different and complex domains: healthcare, informatics and security), and certainly not in the same way that was applied and described in this paper. The same methodology can also help with research that needs to focus on the interactions between humans and technology and bridging this gap by bringing closer together the users' needs and the systems' functionality.

Even though information security is usually more related to technological issues, security is mostly about people and processes. GT, together with mixed methods research can, in this case, be one solution to involve healthcare professionals in the definition of access control policies to EMR in order to make information security more grounded into their workflows and daily practices.

Summary Points

What was known before?

- EMR has integration problems into existing workflows
- Healthcare professionals do not participate in the EMR design, implementation process and access control policy definition
- HCPs usually have workflow and education problems when using the EMR

What has this study added to knowledge?

- Grounded theory and mixed methods:
    - Can be used to involve healthcare professionals in defining access control policies to EMR
    - Can be used to explore access control and users' perspectives and experiences in a diversified and integrated way
    - Can help to adapt access control to healthcare professionals' needs in terms of EMR workflows with a goal to minimize EMR integration barriers
    - Can be used in similar research for the information security domain

o
Acknowledgements

The authors would like to thank the (ISC)2 Organization and the Portuguese Calouste Gulbenkian Foundation for their support.

References

[1] Gollman D. Computer Security. 1st ed: John Wiley & Sons 1999.

[2] Harris S. CISSP All-in-One Exam Guide. 2nd ed: McGraw-Hill Osborne Media 2003.

[3] Waegemann C. EHR vs. CPR vs. EMR. Healthcare Informatics online. 2003 May 2003.

[4] Cruz-Correia R, Vieira-Marques P, Costa P, Ferreira A, Oliveira-Palhares E, Araújo F, et al. Integration of Hospital data using Agent Technologies – a case study. AICommunications special issue of ECAI. 2005;18(3):191-200.

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

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

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

[8] Ana Ferreira, Ricardo Cruz-Correia, Luís Antunes, David Chadwick. Access Control: how can it improve patients' healthcare? Studies in Health Technology and Informatics. IOS Press. 2007. 127:65-76.

[9] Blobel B. Authorisation and access control for electronic health record systems. Int J Med Inform. 2004 Mar 31;73(3):251-7.

[10] Strauss A. Qualitative analysis for social scientists: Cambridge University Press 1987.

[11] Marvasti AB. Qualitative research in sociology: an introduction. London: Sage 2004.

[12] Dey I. Grounded theory.The SAGE handbook of grounded theory: Sage 2007.

[13] Delamont S. Ethnography and participant observation. The Sage Handbook of Grounded Theory: Sage 2007.

[14] Bamberger M. Integrating quantitative and qualitative research: lessons from the field. Washington DC. World Bank 1999.

[15] Borkan J. Mixed Methods Studies: a foundation for primary care research. Annals of Family Medicine. 2004;2(1):4-6.

[16] Moffatt S, White, M., Mackintosh, J., Howel, D.,. Using quantitative and qualitative data in

health services research – what happens when mixed method findings conflict? BMC - Health Services Research. 2006;6(28).

[17] Morgan DL. Practical Strategies for Combining Qualitative and Quantitative Methods: Applications to Health Research. Qualitative Health Research. 1998;8(2):362-76.

[18] Brewer J, Hunter A. Foundations of Multimethod Research. Chapter 1: The Multimethod Approach and Its Promise: Sage Publications 2005.

[19] Morgan D. Focus Groups. Annual Review of Sociology. 1996;22:129-52.

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

[21] Charmaz K. Constructing Grounded Theory: A Practical Guide through Qualitative Analysis. Sage Publications Ltd. 2006.

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

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

Appendix

Questionnaire to the HCP

Electronic Medical Record (EMR)

Part 1

Generic questions about the EMR

1. Have you ever used an EMR?
   (Choose only one option)

   a. ☐ No *(go to question 4)*
   b. ☐ Yes *(go to question 2)*
   c. ☐ Don't know *(go to question 4)*

2. How regularly do you use an EMR?
   (Choose only one option)

   a. ☐ Daily / almost everyday
   b. ☐ 1 to 3 times per week
   c. ☐ 1 to 3 times per month
   d. ☐ Don't know

3. What is (are) the objective(s) of that use? *(Choose all necessary options)*

   a. ☐ Consultation/search
   b. ☐ Data Input
   c. ☐ Decision Support
   d. ☐ Prescription
   e. ☐ Emergency / ICU
   f. ☐ Don't know

4. Do you think EMR is:
   (choose only one option)

   a. ☐ Not Useful
   b. ☐ Necessary evil
   c. ☐ Important for my work
   d. ☐ Indispensable
   e. ☐ Have no opinion

5. What are the problems of the EMR?
   (choose all necessary options)

   a. ☐ They have no problems
   b. ☐ They require education
   c. ☐ They require changing your tasks
   d. ☐ They are not secure
   e. ☐ Affect doctor/patient relationship
   f. ☐ They are a waste of time
   g. ☐ Have no opinion

6. What are EMR security problems?
   (choose all necessary options)

   a. ☐ Access control
   b. ☐ You do not trust the system
   c. ☐ Share sensitive information
   d. ☐ Distribute online access
   e. ☐ None
   f. ☐ No opinion

7. Did you ever participate in EMR development?
   (Choose one option)

   a. ☐ No
   b. ☐ Yes
   c. ☐ Don't know

8. Do you think you should participate in that process? *(choose one option)*

   a. ☐ No
   b. ☐ Yes
   c. ☐ No opinion

9. In which part of that process did you participate or would like to participate? *(choose all necessary options)*

   a. ☐ Idealization/conceptualization
   b. ☐ Define policies
   c. ☐ Implementation
   d. ☐ Test
   e. ☐ Don't know

Part 2

Questions about access control

1. Which mechanisms you normally use to access an EMR? *(choose one option)*

   a. ☐ It has no mechanisms
   b. ☐ Login / password
   c. ☐ Biometrics (fingerprint)
   d. ☐ Other _____
   e. ☐ Someone else accesses for me
   f. ☐ Don't know

2. If you use login / password: *(choose all necessary options)*

   a. ☐ You forget it many times
   b. ☐ You share your password
   c. ☐ Accesses the EMR easily
   d. ☐ Other _____
   e. ☐ No opinion

3. Do you take a long time to access the EMR? *(choose one option)*

   a. ☐ No
   b. ☐ Yes
   c. ☐ Don't know

4. Do you have difficulties accessing the EMR? *(choose one option)*

   a. ☐ Never
   b. ☐ A few times
   c. ☐ Regularly
   d. ☐ Many times
   e. ☐ Always
   f. ☐ Don't know

5. Do you agree with the existence of access control levels to access the EMR? *(choose one option)*

   a. ☐ No *(go to question 7)*
   b. ☐ Yes
   c. ☐ Yes for only some information
   d. ☐ No opinion

6. What type(s) of access control levels should there exist? *(choose all necessary options)*

   a. ☐ Professional category
   b. ☐ Defined by the patients
   c. ☐ Depending on the department where you work
   d. ☐ Type of information (+- sensitive)
   e. ☐ Others _____
   f. ☐ Don't know

7. Are there any access control levels in the EMR you normally use? *(choose one option)*

   a. ☐ No *(go to question 10)*
   b. ☐ Yes
   c. ☐ Don't know

8. Do you think those access control levels are adequate? *(choose one option)*

   a. ☐ No
   b. ☐ Yes
   c. ☐ No opinion

9. The access control levels within the EMR were implemented according to: *(choose all necessary options)*

   a. ☐ Professional category
   b. ☐ Defined by the patients
   c. ☐ The department where you work
   d. ☐ The type of information (+- sensitive)
   e. ☐ Others _____
   f. ☐ Don't know

10. Did you participate in the definition/choice of those access control levels? *(choose one option)*

    a. ☐ No
    b. ☐ Yes
    c. ☐ No opinion

11. Should there be mechanisms to allow any healthcare Professional to Access medical data in emergency situations? *(choose one option and/or sub-option)*

    a. ☐ No
    b. ☐ Yes
       1. ☐ everybody
       2. ☐ only professional in emergency
       3. ☐ depending on the emergency
       4. ☐ other _____
    c. ☐ No opinion

Part 3

Questions about ATM scenario

1. Do you agree with patients accessing their medical records through an ATM machine in the same way they access their bank account details? *(choose one option)*

   a. ☐ No
   b. ☐ Yes
   c. ☐ No opinion

2. Do you think ATM is a secure system? *(choose one option)*

   a. ☐ No *(go to question 3)*
   b. ☐ Yes *(go to question 4)*
   c. ☐ No opinion

3. Which are the problems of such a system (ATM)? *(choose all necessary options)*

   a. ☐ Don't know
   b. ☐ Raises ethical issues
   c. ☐ Is not secure enough
   d. ☐ Other _____
   e. ☐ No opinion

4. With what regularity do you access your bank details through an ATM machine? *(choose one option)*

   a. ☐ Daily or almost everyday
   b. ☐ 1 to 3 times per week
   c. ☐ 1 to 3 times per month
   d. ☐ Never
   e. ☐ Don't know

Part 4
Demographical questions

1. Professional category _____
2. Dept/Service _____
3. Healthcare Institution:

   a. ☐ Hospital
   b. ☐ Health Centre
   c. ☐ Laboratory
   d. ☐ Other _____
   e. ☐ Private sector
   f. ☐ Public sector

4. Working years _____
5. Academic proficiency:

   a. ☐ BSc
   b. ☐ MSc
   c. ☐ PhD
   d. ☐ Prof. Catedrático (a degree in the academic carreer that exists in Portugal)
   e. ☐ Other _____

6. Technical proficiency:

   a. ☐ None
   b. ☐ Some
   c. ☐ I have education
   d. ☐ Don't want to answer

7. Sex:

   a. ☐ Female
   b. ☐ Male