Patient empowerment

Information and privacy mechanisms for the 21st century
Patient empowerment

Information and privacy mechanisms for the

21st century

Filipa Falcão Reis

2010
Patient empowerment

Information and privacy mechanisms for the
21st century

Thesis oriented by Prof. Dr. Manuel Eduardo Correia,
Faculty of Sciences, University of Porto

Thesis submitted to Faculty of Medicine and Faculty of Sciences, University of Porto in partial fulfillment of the requirements for the degree of Master of Science in Medical Informatics

Filipa Falcão Reis
2010
“Who gave us eyes to see the stars and did not give us arms to reach them?”

(Florbela Espanca)
Acknowledgments

I dedicate this thesis to my father, whose unconditional support and constant encouragements helped me being focused and to pursue my goals with passion and dedication. The reason is you.

To my mother, for help me during in the survey process. Her contribution was essential to understand the patient’s point of view in such delicate matters.

To my mentor and supervisor, Dr. Manuel Eduardo Correia, whose expertise and understanding were essential in accomplishing this work.

To my husband, José, whose understanding and comprehension was essential to support the foundations of my work. For all those Saturday’s nights we spent at home because I had work to do.

Thanks.
ABSTRACT

Throughout the modern world, healthcare systems are in a crisis. In response, health information systems are going through major changes: focusing more on the patient and what the patient can do to help to improve his own health care. However, in a way, the patient is still being left out, without the ability to decide about his role and impotent to exercise his rights as the owner of his own Electronic Health Record (EHR). Moreover, there exists a general lack of awareness among the general public about the major risks involved in the unbounded disclosure of personal health related data. The continuous growth of privacy incidents, resulting from target profiling and mining off individual health histories, by human resource departments or insurance companies, demonstrates the fragile perception the general public has for these matters. We thus regard as vital to start to raise awareness concerning this matters among patients, caregivers and health professionals, so that the privacy and security of EHRs is considered to be a major concern, and proper priority is given to the research and development of secure computer mechanisms that can effectively help patients to control for themselves the privacy and confidentiality of their own personal health data. We argue informatics has an important and fundamental role in translating, in a secure way, well established real world infrastructures to the virtual world, thus contributing immensely to the ‘patient empowerment’ process and the personalization of EHRs.

The theoretical path used to understand this phenomenon was a key motivator for further work whose development is presented in this thesis. Patients must be given the tools to be able to easily secure for themselves their basic privacy rights regarding their own EHRs. They need to be able to define how much about their health data is publicly known and by whom. As a result, we propose what we think is a user friendly solution regarding EHRs’ disclosure by using the OpenID 2.0 and OAuth protocols and associated security mechanisms. Our solution also combines OpenID technology with the strong authentication provided by the new Portuguese Citizen’s Card. The Extended OpenID project (eOID)
was based on a conceptualization of this solution and its main goal was to provide the enrolled citizen with the possibility of enjoying Internet services in a more secure, user centric and accessible way, by using their Citizen Cards (CCs) to self provision and strongly authenticate an OpenID digital identity. In this dissertation we make a proposal for providing the eOID with the functionalities needed to meet the health care identity, authentication and authorization more challenging scenarios. We also introduce the concept of Health Digital Identity (HDI) for patients and Medical Digital Identity (MDI) for health professionals thus making a contribution to the improvement of the empowerment process.

In what follows, we describe some identity, authentication, authorization and role delegation (IAAR) scenarios with patient and medical staff actors, supported by eOID and OAuth, where the patient empowerment process could be readily enabled: during consultation time and ‘break-the-glass’ mode (for emergency situations). However, at the center of the evolving clinical personal workstation lies the health record with new properties: electronic, accessible, confidential, secure, acceptable to clinicians and patients, integrated with other types of non-patient-specific information and sharable in a web 2.0 context. This can be readily achieved by employing new more flexible security mechanisms and it is extremely important and helpful that it is so, regarding users privacy in the matters of managing their own EHRs. It is our strong belief that web 2.0 could significantly help the patient to embrace the patient empowerment process, thus pushing health care to a whole new level!
SUMÁRIO

Por todo o mundo as organizações e sistemas de saúde estão em crise. Em resposta, os sistemas de informação para a saúde estão a sofrer mudanças significativas: focando-se mais no paciente e naquilo que este pode fazer para melhorar o seu estado de saúde. Contudo, de certa forma, o paciente ainda é colocado de parte, sem a possibilidade de decidir qual o seu papel e sem poder para efectivamente exercer os seus direitos como dono dos seus próprios Registos Clínicos Electrónicos (RCE). Mais ainda, o público em geral está pouco sensibilizado para os grandes riscos decorrentes da divulgação e partilha de dados pessoais relacionados com a sua saúde. Os incidentes relacionados com a perda de privacidade dos dados são uma realidade em constante crescimento, muitos resultam de pesquisas intensivas por parte de departamentos de recursos humanos ou seguradoras, que vasculham episódios clínicos de indivíduos com o objectivo de usar esses dados para fins menos dignos, demonstrando a frágil percepção que o público em geral tem por estes assuntos. Deste modo, consideramos importantíssimo consciencializar todos, desde os pacientes, aos prestadores de cuidados e profissionais de saúde para que a privacidade e a segurança dos RCEs sejam consideradas uma grande preocupação e que seja atribuída prioridade à investigação e desenvolvimento de mecanismos de segurança informáticos que consigam efectivamente ajudar os pacientes a gerir por eles próprios a privacidade e confidencialidade da sua informação pessoal de saúde. A Informática tem, pois, um papel fundamental na tradução ou transformação de infraestruturas do mundo real para o mundo virtual de um modo seguro, contribuindo assim para reforçar o processo de ‘patient empowerment’ e para a personalização dos RCEs.

O caminho teórico utilizado para compreender este fenómeno foi a chave motivacional para o aprofundar do trabalho cujo desenvolvimento é apresentado nesta dissertação. É necessário disponibilizar aos pacientes ferramentas que lhes permitam assegurar por eles próprios os seus direitos mais básicos de privacidade relativamente aos seus RCEs. Estes precisam de ser capazes de definir quanto dos seus dados
clínicos devem ser conhecidos e por quem. Neste contexto, propomos uma solução que consideramos ser user friendly no que diz respeito à partilha e divulgação dos RCEs utilizando OpenID 2.0 e OAuth. A nossa solução também combina a tecnologia OpenID com mecanismos de autenticação forte na forma do Cartão de Cidadão (CC) Português. O Extended OpenID project (eOID) foi baseado na conceptualização dessa solução, sendo o seu objectivo principal permitir ao cidadão desfrutar dos serviços online de um modo seguro, acessível e centrado no utilizador, utilizando para o efeito o seu CC e uma identidade digital OpenID para uma autenticação forte. Nesta dissertação, propomos dotar o eOID com as funcionalidades necessárias para atingir os requisitos de identidade, autenticação e autorização no contexto da saúde. Deste modo, apresentamos o conceito de Health Digital Identity (HDI) para pacientes e Medical Digital Identity (MDI) para profissionais de saúde, contribuindo para o melhoramento do processo de empowerment.

No que se segue, descrevemos cenários de identidade, autenticação, autorização e delegação de papeis, suportados pelo eOID e OAuth, protagonizados por pacientes e profissionais de saúde e onde o processo de ‘patient empowerment’ poderia ser facilmente activado: durante o tempo de consulta ou no modo ‘break-the-glass’ (em casos de emergência). No entanto, no centro reside o RCE, na sua nova manifestação: electrónico, acessível, confidencial, seguro, aceitável para médicos e pacientes, integrado com outros tipos de informações não-esspecíficas de pacientes e compartilháveis num contexto web 2.0. Portanto, é extremamente importante e útil implementar este tipo de mecanismos sobre a privacidade dos utilizadores em questões de gestão de RCEs. É nossa firme convicção de que a web 2.0 pode ajudar o paciente a adoptar o processo de ‘patient empowerment’, elevando a saúde para um nível superior!
# Table of Contents

Abstract ................................................................................................................................................................................... 11

Sumário .................................................................................................................................................................................... 13

Table of Contents .................................................................................................................................................................. 15

Table of Figures ..................................................................................................................................................................... 17

List of Abbreviations............................................................................................................................................................. 19

1 Introduction ........................................................................................................................................................................ 23

1.1. Thesis main objectives...................................................................................................................................... 23

1.2. Thesis motivation.............................................................................................................................................. 26

1.3. Thesis objectives and Research Methods ...................................................................................................... 27

1.3.1. Research questions and objectives ....................................................................................................... 28

1.3.2. Select a research method and set a research instrument .................................................................. 29

1.4. Scientific results and Funding ......................................................................................................................... 30

1.5. Thesis Preview ................................................................................................................................................... 32

2 Electronic Health Records ................................................................................................................................................ 37

2.1. Definition of Electronic Health Records...................................................................................................... 37

2.2. Historical Perspective ....................................................................................................................................... 38

2.3. The Portuguese Electronic Health Record Systems ................................................................................... 44

2.3.1. Registo de Saúde Electrónico (RSE).................................................................................................... 46

2.4. Security, Privacy and Confidentiality ............................................................................................................. 48

2.5. European Directives on data protection and their application in the Portuguese laws.................. 51

3 Patient Empowerment....................................................................................................................................................... 55

3.1. The definition of Patient Empowerment ...................................................................................................... 55

3.2. The road to Patient Empowerment ............................................................................................................... 57

3.3. Healthcare in the 21st century; the changing of roles.............................................................................. 58
3.4. Patient Empowerment by numbers: a Portuguese case study survey ...................................................... 61
   3.4.1. Methodology ............................................................................................................................................ 61
   3.4.2. Results ....................................................................................................................................................... 62
   3.4.3. Discussion ................................................................................................................................................ 63
   3.4.4. Study conclusions .................................................................................................................................... 65
   3.4.5. Recommendations ................................................................................................................................... 66
3.5. Patient Empowerment and health outcomes ............................................................................................... 67
3.6. Challenges ahead ............................................................................................................................................... 69
4 Identity and Privacy mechanisms ............................................................................................................................. 73
   4.1. OpenID, a self empowering identity management system ........................................................................ 74
      4.1.1. OpenID Authentication process .......................................................................................................... 75
      4.1.2. OpenID advantages and future perspectives ..................................................................................... 76
   4.2. OAuth, granting authorizations on the Internet .......................................................................................... 79
      4.2.1. System Architecture ................................................................................................................................ 79
      4.2.2. Introducing OAuth 2.0 .......................................................................................................................... 81
   4.3. Smart Cards ........................................................................................................................................................ 83
      4.3.1. What is a Smart Card? ............................................................................................................................ 84
      4.3.2. Advantages and disadvantages of smart cards in healthcare ........................................................... 84
      4.3.3. The Portuguese Citizen’s Card (CC) .................................................................................................... 85
5 Health Digital Identity Scenarios ..................................................................................................................................... 89
   5.1. Improving Patient Empowerment ................................................................................................................. 90
   5.2. Health care Digital identities ........................................................................................................................... 91
      5.2.1. Health Digital Identity (HDI) ............................................................................................................... 92
      5.2.2. Medical Digital Identity (MedDI) ......................................................................................................... 95
   5.3. Granting secure access to EHRs .................................................................................................................... 97
      5.3.1. Using OAuth to grant secure access to EHRs................................................................................... 98
   5.4. Registo Central de Saúde (RCS) ...................................................................................................................... 99
      5.4.1. Scenario 1: Patient’s authorization to access their EHRs in a HIS during consultation time .......... 102
      5.4.2. Scenario 2: Accessing a patient’s EHRs in an emergency situation ............................................. 106
   5.5. Future perspectives ......................................................................................................................................... 106
6 Conclusions ....................................................................................................................................................................... 109
   6.1. Future Work ..................................................................................................................................................... 111
7 Bibliography ...................................................................................................................................................................... 115
## Table of Figures

- **Figure 1.** Analysis of the administrative data storage in Portugal during 2007 ........................................ 45
- **Figure 2.** RSE reference model ........................................................................................................................ 46
- **Figure 3.** RSE Information Model ................................................................................................................... 47
- **Figure 4.** Patient Empowerment dimensions ................................................................................................ 55
- **Figure 5.** Levels for Patient Empowerment ................................................................................................... 57
- **Figure 6.** Informatics’ role for increasing ‘patient empowerment’ ............................................................. 59
- **Figure 7.** Desirable consequences of greater patient power ........................................................................ 68
- **Figure 8.** OpenID authentication process ...................................................................................................... 76
- **Figure 9.** New approaches to user identity and external data access ......................................................... 78
- **Figure 10.** OAuth process ................................................................................................................................. 80
- **Figure 11.** An individual’s partial identities .................................................................................................... 91
- **Figure 12.** RCS system architecture ................................................................................................................. 99
- **Figure 13.** Accessing information using HDI Provider ............................................................................... 104
- **Figure 14.** Levels for Patient Empowerment ................................................................................................. 115
LIST OF ABBREVIATIONS

CC Citizen Card

EHR Electronic Health Record

GP General Practitioner

HIPAA Health Insurance Portability Accountability Act

HIS Health Information System

MCDT Means of Complementary Diagnoses and Treatments

NHS National Health Service (UK)

PHR Personal Health Record

PKI Public Key Infrastructure

RBAC Role Based Access Control

RNU Registo Nacional do Utente

RSE Registo de Saúde Electrónico

SAM Sistema de Apoio ao Médico

SINUS Sistema de Informação para as Unidade de Saúde

SNS Serviço Nacional de Saúde

SONHO Sistema Integrado para Informação Hospitalar
1 Introduction

“It’s only work if somebody makes you do it.”
(Bill Watterson, Calvin&Hobbes)
1 INTRODUCTION

Recent market and societal forces are forcing health care organizations worldwide to compete for the development of more adequate and versatile information systems. These are nowadays essential to maintain both the private and public health care providers in the game by allowing them to answer in a very efficient way crucial questions related to strategic planning and at the same time improve the quality of the health care that is provided for its clients and/or citizens. This is essential if the caretaker wants to remain competitive with other provider groups that are also leveraging their activities on appropriate and competitive health care information systems. This arms race is leading to major changes in health care. Nowadays, one of the game-changing transformations is related with the role the patient can have in his own health care, particularly when he acts as an active provider, manager and arbiter of health related information. Health care systems that are capable of capitalizing on these assets put themselves into a position of great competitive advantage focusing more on the patient as a major source of useful information and as an intelligent agent that can act as his/her own info-manager for his own benefit.

1.1. Thesis main objectives

The main purpose of our work is to describe major issues related to Patient Empowerment and Electronic Health Records (EHRs) in general, giving special focus and context to some aspects that are considered as more relevant, such as identity and privacy mechanisms in health care.

Electronic Health Records (EHRs)

Traditionally, medical records have been one of society’s most valuable and tightly held personal records hence they are a repository about an individual’s lifetime health status. The obligation to maintain patient confidentiality has always been widely regarded as a fundamental ethical responsibility of the medical professional (1). However, the continuing growth of the popularity of electronic health record
systems that are not only designed to integrate electronic health records (EHRs), but also clinical decision support systems, data storage, prescription applications and administrative tools, the number of individuals that access this information has increased as well. EHR systems are becoming more and more sophisticated and include nowadays numerous applications, which are not only accessed by medical professionals, but also by accounting and administrative personnel, among other professionals. The access control mechanisms have therefore to cope with very diverse categories of users and roles that need to access different parts of the EHR. With so many different groups of people having the ability to access EHRs we argue that it is in the public best interest to have each citizen know who is accessing his medical record and for what purpose. Furthermore, information is power and each individual should be entitled to the right to manage comprehensible access rights to his own EHRs (2).

**Privacy management mechanisms in health care**

Our relationship with others is often affected by privacy matters. Privacy can be readily defined as our ability as an individual or as group to seclude ourselves or information about ourselves, allowing it to be revealed selectively and in a controlled way (3). Although the boundaries and content of what is considered to be private are not and cannot be widely defined, it is generally considered to be a matter for the individual, as a member sensitive to the context of a society and integrated into its own culture (2). Privacy is also about autonomy and integrity and each individual’s right to his private live as stated in the Article 12 of the Universal Declaration of Human Rights, established by the United Nations in 1948 (G.A.res.217A(III), U.N. Doc A/810 at 71) (4).

It is well known that current traditional and privacy mechanisms often fails to meet their purpose when used in the health sector, i.e. to grant each individual the right to exercise more control on his own health information and to know who had access to his health record and why. However, one must keep in mind that the record (at least partially) has to be made accessible to the professionals who use the records to provide medical care and save lives. This includes not only the doctor but also nurses, dentists, psychologists, nutritionists, pharmacists as well as other professionals such as accounting and administrative personnel. These professionals do not necessarily possess the same degree of professional
ethics and obligation sensitivities regarding patient private data, which imposes a threat to the confidentiality and privacy of EHRs: with so many different professionals having the ability to access patient’s EHRs, it is in the patient and health providers’ best interest to know who is accessing the patients EHRs and for what purposes. Health Information is critical, and in the wrong hands its misuse can create havoc in the social lives of the individuals thus affected (5).

Therefore, how can an individual assess the disclosure of his private information to a third party, when he is not aware of who wants it, for what purpose and for how long? This incapacity of easily tracking the flow of private data is producing a dangerous imbalance that could lead us towards a world, where some “big brothers” possess an ever increasing ability to “watch” us all the time and no one can watch what they are doing with the private information they eventually collect. Only by empowering each individual with the ability to know in a precise and simple way who and when some entity had access to his private data can this situation start to be remedied and the balance of information distribution can begin to be reestablished (2). Unfortunately the exercise of this human right is often forgotten and society by itself does little to improve individual awareness of these issues.

The importance of creating data access protocols and mechanisms to protect our privacy right and furthermore, to enable us to automatically track the data flows of our own personal information are growing fast. Privacy protection laws have been introduced in most of the developed countries to prevent what are considered to be violations of very fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorized disclosure of such data. Due to the development of automatic data processing, the OECD compiled guidelines (6) on the protection of privacy and trans-border flow of personal data. We considered these guidelines as one of the basic foundations of our research.

Terms like “patient empowerment” are very common these days (7). Indubitably, this is a reflection of our times and represents a noble goal that we should continue to pursue. Behind this concept is the general idea of granting patients the role of pro-active consumers that have the right to make their own choices as well as the ability to act and be responsible for them. Indeed who is better entitled to have
access to his own EHRs than the patient himself? Shouldn’t he have the right to know who had access and modified his EHR, when that happened and for what purpose? These privacy questions should be answered and presented to the EHR owner at least when the individual wishes to know about these issues. For this he should be able to access some kind of reserved online service where he can be provided with this information (2).

1.2. Thesis motivation

In 2007, there were rumors of an incident in which the EHR of former England Football Manager Sir Bobby Robson was illicitly disclosed by members of the National Health System in the U.K., when he was scheduled for brain surgery in August 2006.

An internal hospital memo, leaked to the Chronicle newspaper in Newcastle, stated: "Over the last few weeks the ongoing security reports relating to the access by staff to the PAS (patient administration system) system and to the Casenote Tracker module has identified inappropriate access which has resulted in a formal disciplinary investigation and written warnings being issued to a number of trust staff who have accessed patients' information for no other reason than personal curiosity" (8).

The North Tees Primary Care Trust warned of a new security risk to the confidentiality of patient records under the NHS’s National Programme for IT [NPfIT]. This warning consisted of a paper to trust board in March 2007 which referred to the Care Records Guarantee – which, under the NPfIT, gives an undertaking to patients that their confidential data will be protected from unauthorized access. North Tees Primary Care Trust stated in the paper that: "A new security risk (...) has been identified as part of the Care Records Guarantee. This risk is around staff inappropriately accessing patient’s records that are not part of their care load. It was noted in an audit that a recent admission of a celebrity to a hospital had revealed over 50 staff viewing the patient record. Staff should only access records of patients with whom they have a legitimate relationship" (9).

Audit systems are crucial for the detection of illicit access to EHRs in general. However if system monitoring depends exclusively on people not directly affected by information disclosure, what normally happens is what we have just stated, valuable private information is leaked and in the end no one is
blamed. One problem to solve is to determine whether staff responsible for hundreds of thousands of audits is or is not able to robustly police valuable health information. We believe a much more sensible solution could be found by partly transferring this enormous auditing task into the hands of the truly interested party, the patient (2).

We are currently witnessing the emergence of a new kind of society, empowered by information technology in ways previous generations could only have dreamed off. This digital society can be much more focused on the citizen by providing him with the means to manage his own information, thus contributing greatly to the improvement of his own life conditions. One possible solution could take the form of an intelligent and user oriented web based management system providing an intuitive user friendly analysis of audit trails, thus allowing each patient to have the capacity to monitor the flow of his own health data. Furthermore, the system should be able to allow the patient to grant or deny authorizations accesses for his own EHR, thus nurturing the empowerment process (2). Who but the individual is more worried about his own well being than himself? This question is normally conceptualized as “citizen empowerment”, and is manifested into many different social constructs. One of which appears in the modern conceptualization of “patient empowerment”, whose main consequences and how to achieve them in the future is one of the major motivations and driving forces behind this dissertation.

1.3. Thesis objectives and Research Methods

Although the term research is semantically overloaded due to all the different contexts it can be used, one can define it in an academic context as the activity of a diligent, scientific and systematic inquiry or investigation in a particular area to discover or revise facts, theories, applications, among other conjunctures/hypotheses with the goal to discover and disseminate new knowledge by critically study the subject (10).

Over the last few years, the concept of ‘Patient Empowerment’ has gained increasing prominence and acceptance as the base for a patient-centered reform on healthcare worldwide, resulting on a silent massive revolution on healthcare systems ever since (11). Therefore, in order to understand this process
and how it can contribute for a better-personalized healthcare by means of self-managing accessing control rights to EHRs, which is the main focus of the study, we have established a research process based on the eight-step generic model by R. Kumar as following and accordingly to meet our paradigm needs (12):

1.3.1. Research questions and objectives

Research questions are formal statements of the aims of the study. Therefore, the focus of the questions is to concisely describe variables, their relationship assessment between them and to determine the differences between a set of selected variables. Consequently, we have identified the following questions to address:

- How many patients consider that only the health professionals that are engaged in their treatment should have access to their EHRs?
How digital identities, and other security mechanisms, such as authentication and authorization, can be used to help in nurturing the patient empowerment process?

In addition, the research questions implicitly determine the research objective, and together they indicate the type of research to select. Therefore, we have identified the following specific objectives of the study:

- Set the background for EHRs’ access management, security and privacy.
- Study its impact regarding access policies and the management of EHRs.
- Define an architectural model for provisioning digital identities in healthcare information systems.
- Describe how to combine strong authentication mechanisms with appropriate authorization protocols so that the patient is able to share his EHRs with the health professionals.

### 1.3.2. Select a research method and set a research instrument

We can place our research within the analytical-applied type of research hence we used facts already available, which were analyzed to make a critical assessment of the subject (EHRs), in order to define a solution for a specific problem (how to improve patient empowerment using access rights to EHRs). The facts already available from which we based our research are obtained by reviewing the literature thus giving response to the first two objectives specified on the previous section. As a result, we searched in the PubMed digital library (13) and Google Scholar (14) the articles that met the following criteria:” ("electronic health records"[All Fields] OR "health records"[All Fields] OR "patient empowerment"[All Fields]) AND hasabstract[text]”. We have selected from the list of results the most relevant abstracts and retrieve the full document for further research. These articles constitute part of the bibliography presented on chapter 7. However, in order to define a solution for the rest of the specified objectives, we have determined adequate research methods and instruments to assess each one of them.

Therefore, in order to better understand how patient choices can be used to manage access rights to their own EHRs, we need to investigate how they are perceived from the patient own point of view. This way, it becomes much easier to elaborate a plan to effectively help to establish the patient’s real needs.
for self-empowerment. Moreover, to help patients to understand and accept their role (just like in the self-service industries, such as fast food chains where the consumers know what is expected of them) and to attain knowledge about their options (an informed choice will improve the patient performance and commitment to his own healthcare).

In order to define an architectural model for provisioning digital identities and to describe how to combine strong authentication mechanisms with appropriate authorization protocols, we need to understand the patient’s perception on such matters as privacy and confidentiality of EHRs and its access rights. As a result, we selected a qualitative method hence this kind of approach based on the analysis of non-numerical information can provide significance to human behavior missing in the quantitative approach. The data is collected by interviewing patients older than eighteen years old to determine their opinions on matters regarding ‘patient empowerment’ and their EHRs. The characterization of the sample is obtained by the analysis of the demographic variables, which are attributes of the subjects collected in the first part of the interview (related with personal information). The decision to make a personally interview is related to the fact that it is easier and cheaper to capture the required information than using a telephone approach. In addition, the answers are recovered in a way that can be statistical treated. Furthermore, focus groups interviews also constitute a good tool to gather patient’s opinions about these topics and to support the definition of scenarios needed to validate the approach. By choosing interview as an instrument of measuring we are expecting to be able to determine perceptions, attitudes and common practices regarding today’s healthcare within the patient’s perspective.

1.4. Scientific results and Funding

During the preparation of this thesis we were part of the research team that submitted a project to FCT which has been funded – FCT OFELIA – Open Federated Environments Leveraging Identity and Authorization PTDC/EIA-EIA/104328/2008. We expect part of the results obtained by OFELIA to be useful for the implementation of the proposed usage scenarios of chapter six.
We have also published several refereed papers related to the subject of this thesis in several International Conferences:


Filipa Falcão-Reis, Diana Almeida e Manuel E. Correia, On the strengthening of OpenID authentication mechanisms with the Portuguese citizen card, proceedings of 4ª Conferência Ibérica de Sistemas e Tecnologias de Informação (CISTI 2009), Póvoa de Varzim, 17 - 20 June 2009.


As a result of the publication of Towards Patient Empowerment – can the patient really decide? at the proceedings of World Congress 2009 – Medical Physics and Biomedical engineering, I was invited by the Organizing Committee to prepare an invitational paper to the forthcoming conference 2010 IEEE International Conference on Management Science and Information Engineering (ICMSIE 2010).
1.5. Thesis Preview

This thesis is divided into six chapters, according to the main objectives of the initial project and the adopted research strategy.

Chapter one provides a motivational introduction to the main subject and describes some future perspectives. We also enumerate some of the published scientific papers and other research activities.

The second chapter, entitled “Electronic Health Records” provides a survey of the state of the art on this subject within a perspective of patient empowerment.

In the third chapter we present a definition for Patient Empowerment, its associated principles and a classification for levels of empowerment. We also discuss what should be the patient's role in the 21st century. To substantiate this discussion we have conducted several interviews with patients older than eighteen years old in order to determine their opinion on matters regarding Patient Empowerment and their Electronic Health Record (EHR): particularly who should have access to it and what was the reason for that choice. Its presentation, as well as the discussion of results, occurs in this chapter, along with some pertinent conclusions. In addition, we also discuss health outcomes concerning the 'patient empowerment' approach and how information systems can play a decisive role in patient empowering thus providing an appropriate preamble for the next chapter.

Regarding the fourth chapter we describe how information systems can actively help the patient empowerment process by presenting a tentative solution architecture based on OpenID and OAuth where strong identity and authentication is provided by the employment of smart cards. To give proper context to this technology we also provide a survey of smart card usage and application in health care thus providing an historical context together with some examples of smart card usage in other countries.

Chapter five is concerned about Patient Empowerment mechanisms. Basing our experience on previous work done on the implementation and deployment of an OpenID server and client (eOID project) (15). We discuss and propose the details for an implementation of an Health Digital Identity
(HDI) for patients and a Medical Digital Identity (MedID) for health professionals. In this chapter we also describe some challenging scenarios, as well as technical solutions for their implementation.

The conclusions presented in chapter six summarize the main goals achieved and present planned future work to further promote “Health Digital Identity” into a whole new personal level.
2 Electronic Health Records

“The size of the Universe depends on who is looking.”
(Filipa Falcão Reis)
2 ELECTRONIC HEALTH RECORDS

With the advent of Information Technologies (IT) and the explosion of Internet services, paper-based solutions are no longer sufficient to meet today’s demanding health care requirements in providing and managing life threatening timely access to critical information. The shift from a paper-based to an electronic media-based society is opening new opportunities and providing new challenges that were not conceivable just a few years ago. Cost is no longer a major barrier to the collection, storage and processing of information. As a result, electronic records are common practice at critical businesses, major industry sectors and even within the health sector itself, where we are witnessing the emergence and consolidation of the Electronic Health Record (16) (17) (18).

Different forms of Electronic Health Records (EHRs) have been proposed, developed and implemented, since the early 80’s. Despite the obvious need for a new record-keeping paradigm, most of today’s health care institutions worldwide are currently struggling to plan the introduction of nationwide EHR. Although some have actually implemented some form of EHR, the type and extent of EHRs vary and what one country calls an EHR may not be the same as in another country. Yet, it is still a digital record, therefore subjected to all the adversities and enticing benefits of the digital world (18).

2.1. Definition of Electronic Health Records

Over the years a number of terms have been used to describe the move from paper-based health records to computer managed health records. Some of the better known terms include: Automated Health Records (AHR), Electronic Medical Record (EMR), Computer-based Patient Record (CPR), and Electronic Health Record (EHR). The term EHR is widely used in many countries with variation in definitions and the extent of coverage. Therefore, we adopt this term to address these matters. Its general
definition includes a repository of lifetime health information belonging to a particular individual. This information can be entered, uploaded and accessed electronically by health professionals with the permissions to do so (18) (19) (20) (21) (22).

Although, in some countries the patient is the owner of his EHRs, he cannot be responsible for managing them. It is important to note that an EHR is generated and maintained within health institutions, such as hospitals, integrated delivery networks, clinics, or physician offices (23). Patients nowadays also require access to their own EHR to an extent that permits them to play an active role in their health management. Therefore, EHRs are currently seen as ‘patient empowerment’ process facilitators: by giving patients a source of information that is specific to them (24). Health care providers should support this process and by support we mean the encouragement and promotion of real partnerships among practitioners, patients, and their families (when appropriate) to ensure that decisions respect patients’ wants, needs, and preferences and that patients have the education, support and resources they need to make decisions and participate in their own care (2). Quoting Kalra: “These requirements are becoming more urgent as the focus of health care delivery shifts progressively from specialist centers to community settings and to the patient’s personal environment” (25).

2.2. **Historical Perspective**

The patient health record is an explanation of a patient’s health and disease after he or she has asked for medical help. Usually, the record used in a clinical situation contains the patient’s complaints as well as the clinician’s findings and data from other means of complementary diagnoses and treatments (MCDTs) sources, such as laboratory and imaging test results, among others (26). Also, the record may contain information related with medication and therapeutics, including specific instructions concerned with the patient’s treatments. Yet, there are other functions associated with patient health records than to just document patient care. According to Stanley Reiser (1991), the purpose of a patient record is “to recall observations, to inform others, to instruct students, to gain knowledge, to monitor performance, and to justify interventions”. Although, health records have diverse uses there is a major goal for EHRs – to assist health practitioners
and medical sciences to better serve patients. This includes scientific research activities as well as public health initiatives to better assist health sciences in their quest for improving the well-being of patients (27).

The first known health record was developed in the fifth century B.C by Hippocrates and contained descriptions of events that occurred previously to the disease in a purely chronological order, thus the term *time oriented health record*. According to Hippocrates, a medical record should accurately replicate the course of disease and indicate its probable cause (23). However, with the limited medical insights and cultural shortcomings of the era, the recorded descriptions mainly reproduced the story as told by the patient or his relatives and the practitioners’ observations on what they could hear, feel and see directly with their senses (26). Other civilizations like the Roman adopted from the Greeks the teachings of Hippocrates and consequently the way to record medical patient’s information. This knowledge was passed on throughout centuries to other empires and civilizations such as the Byzantine Empire or the Arabs and Persians meeting its dark period during the Middle Ages and re-surfaced in the 14th century with the Renaissance movement that so profoundly affected European intellectual life in the early modern period – 14th to 16th century. Its ancient Greek and roman influence was visible in the arts, literature, politics, science, religion, philosophy, and other aspects of intellectual inquiry. Although there were major progresses in medical knowledge and scientific methods, the medical records were still mainly based on the patient’s descriptions and sensory based as the ones in Hippocrates time, almost two thousand years earlier (28).

With the arrival of the industrial revolution in the early 19th century, new instruments appeared contributing immensely to the maturity of the available diagnostics techniques. This enabled the patient health record to expand its scope and include the physician and nurse findings. However, hence the records were organized in a chronological order (time oriented medical records) it was very difficult to
obtain a good overview of the complete disease history of a particular patient as they could be scattered accordingly to the space between visits.

The first doctors to adopt the concept of the patient file were the physicians from the Mayo Clinic in Rochester, Minnesota, in 1907. Although, this improvement was the starting point for the patient-centered health record, this first patient file was source-oriented, i.e. compiled according to the origin of the information, and composed as an amalgamation of complaints, physical exams, test results, considerations, therapy plans and findings, and therefore inadequate for clear insight. Only in 1968 was introduced the problem-oriented medical record (POMR) by Lawrence Weed, where each patient was assigned one or more problems (29). Weed was among the first to recognize the importance of an internal structure for health records. Afterward new methods of documenting patient’s encounters became an integral part of the medical practice workflow, such as the notes – organized according to the SOAP methodology (26):

- **Subjective**
  - In this section, the physician:
  - describes his considerations of the patient
  - notes down the complaints as phrased by the patient (symptoms registry)
  - registers pertinent medical history (both family and social)
  - records current medication and allergies

- **Objective**
  - In this section, the physician:
  - reports measurable and observable information obtained during the patient’s visit (vital signs)
  - describes his and nurse's findings

- **Assessment**
  - In this section, the physician:
  - describes the patient’s performance during his visit
  - determines or confirms the diagnosis including a differential diagnosis
  - orders means of complementary diagnosis and treatment (MCDTs)

- **Plan**
  - In this section, the physician:
  - details the course of treatment
  - prescribes medicine, physical therapy, ...
  - orders surgery or any other intervention
With the explosion of computer networks and the Internet in the mid 1960s the limitations of paper-based health records became evident by realizing digital records provide many additional benefits that cannot be accomplished by a static paper based view of events, such as interactive alerts to clinicians, tailored order sets, dynamic flow sheets, guidelines and protocols, among others provided by the usage of EHRs.

We must mention the pioneering EHR work done by Academic Medical Centers (AMCs) and major government clinical care organizations all over the world. Although plagued by many technical difficulties, which remain challenging even today, these first projects set the course for the modern EHR’s conceptualization and deployment. Some of the most notable early projects include (23):

- **COSTAR** (Computer Stored Ambulatory Record), developed at Harvard University, placed in the public domain in 1975 and implemented in hundreds of sites worldwide.
- **HELP** (Health Evaluation through Logical Processing), developed at the University of Utah and notable for its pioneering decision support features.
- **TMR** (The Medical Record), developed at Duke University Medical Center.
- **THERESA**, developed at Grady Memorial Hospital, Emory University, notable for its success in encouraging direct physician data entry.
- **CHCS** (Composite Health Care System), the Department of Defense’s (DoD) clinical care patient record system used worldwide.
- **DHCP** (De-Centralized Hospital Computer Program), developed by the Veteran’s Administration and used nationwide.
- **TDS**, developed by Lockheed in the 1960s and 1970s.

The World Wide Web emergence in the nineties, made the inefficiencies and frustrations associated with the use of paper-based health records increasingly clearer. Since then, technology overcame some of the last barriers for fully computer-based health records and new applications that operated on many different computer systems became a reality as EHRs provided the opportunity for healthcare organizations to improve the quality of care and patient safety (30). Although, the
implementation of an EHR’s systems can be a daunting task, many health care advocates as well as governments worldwide are actively promoting EHRs to become an integral part of health care due to their enticing benefits (31). However, even though there are currently available technologies that allow for the easy implementation of EHR’s systems, there are still several human barriers and obstacles that must be overcome before it can be fully successful. Quoting Young: “Technology has continued to move forward at a rapid pace, but many organizational and human issues have slowed the pace of implementation of automated systems for an electronic documentation record” (16).

### 2.2.1. From paper to electronic based health records

When we compare EHRs with their paper counterparts there are indubitably some key features that put EHR’s systems in the line of the very best emergent technologies available in today’s digital era. Quoting Schloeffel, currently the paper record represents a “massive fragmentation of clinical health information” which not only causes the cost of information management to increase but also “fragmentation leads to even greater costs due to its adverse effects on current and future patient care” (16). EHRs constitute thus a better structured and more organized record with more accurate and updated information, displayed in a more readable and user friendly way. This is mainly achieved by the fact that structure and organization are imposed immediately upon data entry, thus allowing for the customized views of information relevant to the needs of its different users. In addition, it can also reduce medical errors due to illegible notes as well as eliminate data entry duplication of the same information on multiple forms. Hence storage cost and communication networks are no longer a barrier to the collection, transmission and processing of EHRs, they became immediately accessible from remote sites to any unit workstation whenever it is needed while the records are continuously updated and available concurrently for use everywhere (32) (16).

Another important feature of EHR’s systems is concerning decision support tools since they can provide medical alerts and reminders that could assist physicians in their activity. Furthermore, EHRs can swiftly link physicians to protocols, care plans, critical paths, literature databases, pharmaceutical information and other databases of healthcare knowledge in a way that is impossible for a paper based-record to perform such a task. Yet, computer systems should not take the place of physicians’ critical
judgments however they could assist the medical professional in the decision making process, ultimately obtaining better healthcare outcomes (16).

2.2.2. Web 2.0 health records

The term Web 2.0 first appeared in the end of the twentieth century (1999) in an article called “Fragmented Future”, written by a consultant on electronic design named Darcy DiNucci. In her article she argues about the widespread use of portable web-ready devices that are “fragmenting” the web (33).

However, she used the term in the context of web design, aesthetics and interconnectivity, with a semantics not related to its current usage. Only in 2003 has the term resurfaced and its current meaning obtained in the O’Reilly Media Web 2.0 conference of 2004. The evolution from static information-retrieval of the “Web 1.0” to a more collaborative and dynamic “Web 2.0” has enabled the common people, who are not technologically experts, to generate and share content in new and previously unforeseen ways as is manifested by the current social networks popularity. This has created the opportunity and the means to leverage current Internet technologies and explore their capabilities within health related contexts. This way the patient becomes an active producer of quality health information by actively participating in his own treatment and thus helping on achieving more measurable and better outcomes.

Current EHRs include sophisticated applications that can also take the patient’s input directly from the web. Social sites based on web 2.0 technology are in a sense training people and making them more comfortable on the Internet to be more participative thus expanding, empowering, engaging, and educating potential health care consumers and providers to be more active participants in the production of more meaningful health data. While consumers use social media – including social networks, personal blogging, wikis, video-sharing, and other formats – for emotional support, they can also, if properly educated and oriented, rely on these same technologies to better manage their health conditions. There are already many of patient’s blogs and web pages, where patients tell about their medical condition and share
their experiences, fears and concerns. Some of these are already becoming reference websites for other patients with the same medical conditions (see for example e-Patient Dave’s blog) (34). More recently, Twitter added new forms of communication for patients for example posting links to health web sites that have information about a particular chronic disease or simple to allow them to expose a particular health problem and get help from other patients that suffered from the same medical condition or problem.

2.3. The Portuguese Electronic Health Record Systems

By the late 80s, early 90s, the need for fulfilling organizational requirements led the Portuguese Health Administration into the development and implementation of SONHO (“Sistema integrado para informação hospitalar”). SONHO is the dominant administrative system for managing patients’ data in today’s Portuguese hospitals, along with another system for primary care designated by SINUS (“Sistema de informação para as unidades de saúde”).

SONHO's purpose was to "ensure the interconnection of all patient’s data and associated processing, to get a more integrated patient management that could minimize data redundancy" (35). Furthermore, SONHO strives to improve the quality of care for patients, to eliminate the traditional division between medical and administrative information through a common system, to facilitate quick access to data on the earlier history of the patient with more accuracy and to improve the administrative and financial management of hospitals thus increasing the personnel productivity.

The need to create an EHR led SONHO's team to develop a medical module (SAM - Sistema de Apoio ao Médico) and a module for nursing. Moreover, a new clinical module was developed for SINUS. However, these modules are not widespread both in hospitals and healthcare facilities and SAM is mostly used in some hospitals as departmental EHR (35).

Nowadays, the Portuguese government is struggling to develop the appropriated infrastructures to accomplish European Union (EU) technological trends and good practices. In general terms Portugal is within the EU average in terms of availability and use of infrastructure and technological solutions available for eHealth. The same cannot be said about Portugal’s position regarding the provision and use
of next generation networks. According to a study (RSE,2009) presented by the Portuguese Health Ministry and ACSS ("Administração Central do Sistema de Saúde") regarding EHR’s deployment and by analyzing the functional eHealth component, 64% of institutions use computers and their applications, 60% use decision support systems and 74% storage administrative information about their patients. Regarding health data exchange, Portugal is far from the EU average, only 10% of institutions exchange laboratory, administrative and medical results. Figure 1 shows the analysis of the state of administrative storage data in Portugal during 2007 (36).

![Figure 1](image_url)

Figure 1. Analysis of the administrative data storage in Portugal during 2007 (36).

However, in the last few years we have been witnessing a significant improvement concerning the availability of infrastructures and services (such as the RNU – Registo Nacional de Utentes, and the e-Agenda – Marcação de Consultas on-line) as well as the introduction of the national health card (Cartão Nacional de Utente) with the current connection to the Portuguese Citizen’s Card (36). According to the Portuguese Health Secretary – Manuel Pizarro, the Portuguese EHR’s Systems have to suffer major changes if we want to reduce the gap between Portugal and the EU regarding eHealth. In his interview to the “Hospital do Futuro” Health magazine he stated that the Portuguese EHR System has to be centered on the citizen, his needs and his mobility (37). Hence the need and opportunity presented themselves to set a working group representing different experiences and point of views (professional, technical and scientific) with industry representatives (for example public and private hospitals, professional orders, universities, among others).
Many recognized experts were invited by the health secretary as announced by the Ministry of Health Dispatch n.º 10864/2009. The main objective of the working group was to discuss five strategic points taking into account the EU directives and PTSIS – Plano de Transformação dos Sistemas de Informação da Saúde: architectural concerns, information model to apply, ontology, terminologies, security and privacy related issues and a progressive model to help manage the changing process (37). Some of the conclusions were related with the urgency in adopting a patient-centric approach regarding the national EHRs implementation and deployment – Registo de Saúde Electrónico (RSE), based on a distributed federated architectural (36).

2.3.1. Registo de Saúde Electrónico (RSE)

The guidelines for the functional and technical specification of the RSE system were presented publicly in Lisbon during the eHealth 2009 event, as a result of work done by the working group. These constitute a starting point for the RSE’s national planning and implementation processes.

Concerning the Application and Technological framework, it was agreed to adopt a federated reference model sub-divided into 3 levels of abstraction (38):

![Figure 2. RSE reference model (38)](image-url)
N1 – **Common core**: centralized systems that rely on a central management entity

N2 – **Sharing level**: allows for a large degree of openness regarding its implementation and management thus assuming a distributed nature resulting from the federation of areas that might be available by central or regional entities (for example ACSS, ARS, among others), or by care providers.

N3 – **Specific level**: systems that already exist or will exist within the care providers that are directly involved in operational support to its activities and health services

The relations between each one of these sub-levels should be based on rules that will allow for the integrity of information workflows to be secured and assuring the management domain in each level. In addition, it was discussed that interoperability and communication among the different physical and logical systems that will be part of RSE must be guaranteed, either from a technical or functional point of view, as well as concerning transversal and national systems.

Regarding the Information Model, the working group presented also a three level structure according to the architectural orientations discussed above:

- **Common core**: dataset containing general information including general identification, clinical alerts, problems/diagnosis, episodes, procedures/interventions, immunizations, analysis/exams and medication as well as a link to other data residing in the sharing level.

- **Sharing zone**: set of shared content such as reports, discharge notes, transfer letters, exams, among others.

- **Specific zone**: set of data in each entity

Concerning ontology, standards and classification systems the RSE will adopt ICD 10 as the clinical classification system and CIPE 2.0 as a classification standard for nursing. This will allow for interoperability among different systems to be achieved as well as promote data integrity.
However, one must call attention to the fact that this architecture needs to include strong qualified identity and authentication to doctors, nurses, or even dentists, otherwise unauthorized individuals could gain access to sensitive and private data thus seriously jeopardizing the system. This must be provided by professional orders hence one of their purposes is to acknowledge and certify professionals in their areas of expertise. Therefore, it is fundamental to use digital identity certificates and federated identity systems not only for strong authentication but also for security reasons hence health professionals usually work in different institutions and therefore have different credentials to access the different Health Information Systems (HISs). This amount of credentials is very difficult to handle. Consequently, this provides the means to assure health professionals the opportunity to use their credentials in multiple health environments from different health institutions or within the same health institution but across different HISs.

2.4. Security, Privacy and Confidentiality

EHR systems are becoming more and more sophisticated and nowadays include numerous applications, which are not only accessed by health professionals, but also by accounting and administrative personnel that do not necessarily possess the same degree of professional ethics and obligation sensitivities regarding patient private data. The threat to the confidentiality and privacy of EHRs is a major critical issue: with so many different professionals having the ability to access patient’s EHRs, it is in the patient and health providers’ best interest to know who is accessing the patients EHRs and for what purposes. Health Information is critical, and in the wrong hands its misuse can create havoc in the social lives of the individuals thus affected (5). However, the patient must also remember that the record has to be made accessible to the professionals who use the records to provide medical care and save lives. This raises the question of ownership of clinical data, which is prone to several misconceptions. Depending on the place it is gathered, it may have different exclusive owners or be subject to a “joint ownership”. The information may either be regarded as property of the one who gives, receives or pays for care. This leads to confusion on rights to access, change, destroy or transport any given clinical information. There are major differences in the way this type of information is ruled in the USA and EU.
And within these legislations on/or recommendations, confusion often arises (39). There are mechanisms to tackle unauthorized access to protected health information, which might include firewalls, passwords and properly designed and monitored audit trails that can enhance user accountability by detecting and recording unauthorized access to otherwise confidential information. Therefore, system designers must consider how individually identifiable medical information will be protected and also meet regulatory requirements. Quoting Dick, Steen, and Detmer: “Whereas stringent security measures should be applied to protect the confidentiality of patient information, it is also in the patient’s best interest for the [EHR] to be accessible for appropriate, legitimate uses by authorized users” (30). It is therefore of great importance to raise awareness for these matters and ultimately, if he so desires, enable the patient himself with the power to control the dissemination of his own EHRs.

In addition, Web 2.0 interactive content as well as web applications enable and promote greater patient online participation, providing significant benefits for individuals in terms of mutual support, which might be essential regarding specific chronic conditions, such as diabetes, asthma, depression, among others (40). However, the lack of awareness among the general public of the risks involved with the unbounded disclosure of personal data can be dangerous, particularly data concerning their health. Privacy incidents involving personal health data, such as profiling and mining an individual's health history on profile sites by human resource departments or insurance companies, are demonstrating the fragile awareness of the general public for these matters. With the continuing growth and spreading of the use of personal data on the Internet, it is difficult to be conscious of all the vulnerabilities that information could be subjected to (41).

Therefore, it is necessary to define how much aware the individuals are and their perception of the vulnerability when they are online. It is common knowledge that younger people are savvier in the use of new technologies than older ones. Therefore, we might be tempted to agree that in the near future this problem would be solved as the new generation of teenagers gets older. However, according to a study we have conducted and present at the EUKids Online Final Conference in 2009 (41), many young people use the new technologies and the Internet without conscious knowledge of what they are actually doing. The lack of instruction about these new technologies and how to use them in young people leads them to be
potentially exposed to dangers derived from bad and dangerous usage. If not quickly clarified in their questions and doubts, young people can develop bad habits in their relations with the new technologies and the Internet in particular (41).

Further studies should be conducted to assess other age groups. The awareness of such right must be provided to the individuals to facilitate their own enforcement of security and privacy, especially concerning their EHRs. It will also provide them with the knowledge of the ways that their personal data can be misused.

Some of the survey results were quite interesting as they raise some important questions that need further studies and attention. In addition, we can conjecture about its impact regarding access policies and the management of EHRs.

The continuous growth of new online health web sites that require user registration is increasing, in a most dramatic way, the difficulty of managing data. Eventually users end up not only duplicating data but also losing track of their passwords and account settings if they do not use these health web sites on a regular basis. Under this context it is only inevitable that sooner or later users end up compromising their security by using the same set of credentials for the different health related web sites. According to our study, the Portuguese youth usually uses the same password for different purposes and does not change their passwords often (41). Such dangerous behavior is one direct result of the lack of user’s knowledge and health service provider’s willingness to acknowledgment the existence of mechanisms that can help users manage their own accounts and passwords. Some of the conclusions of the survey allow us to depict a challenging scenario.

It is thus important to develop systems and processes that can help manage and control the access, and even the discloser and finality of these resources. These systems should provide user friendly identity management tools for the patient to secure for himself his own privacy in an accessible and easy way. In the fourth chapter we will describe some protocols and some security mechanisms that can be used as solid foundations for the proposed work.
2.5. **European Directives on data protection and their application in the Portuguese laws**

To implement a national EHR’s System is to endure a long process that presents a set of challenges not only related with national needs but also related with ensuring alignment with European and International directives, especially regarding mobility and interoperability matters (38). Nowadays, the Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services (42). With the continuous growing of electronic communications services over the Internet, that allows for individual personal data to travel across the world with greater ease, and the evidently emergence of a new digital society, new aggravated risks for their personal data and privacy are greatly enhanced. As a consequence, the European Union (EU) and its members took some important actions regarding the flow of personal data and digital identity for European citizens, comprising regulations on data transfers concerning appropriate data protection (*Directive 95/46/EC, Directive 2002/58/EC, Directive 2006/24/EC*) (43) (44) (42).

To remove obstacles to the free flow of data without diminishing its protection is the main goal of Directive 95/46/EC (the data protection directive) (45). As a consequence, personal data has now equivalent protection across the Union and its member states are required to convey their national legislation into line with its provisions. The Portuguese government has already complied by having applied this orientation as requested (46). In addition, to enforce such directive each member state must set up a supervisory authority, an independent entity that not only will monitor the data flow and its protection level in that member state, but also give recommendations to the government about administrative measures and regulations, and start legal proceedings when data protection regulation has been violated. Although some penalties are fore coming in this directive, regarding the violations of the data protection rules, it are not heavy sanctions and therefore is preferable being caught violating the data protection law than to comply with it. Perhaps a directive concerning the enforcement of the law is something to take in consideration in future directives.
The fast growth of Internet services and its increasing number of users as well as the huge amounts of transmitted data through the network were foremost the reason for the EU to add some new directives to complete the data protection law. One of these directives is concerned with the protection of data in the electronic communications sector (42). The rules and specifications concerned to the protection and confidentiality of data transmitted across the network were collected and presented as the Directive 2002/58/EC (45).

However, this Directive was not sufficient regarding the use of electronic communications to prevent, investigate, detect and prosecute criminal offenders, in particular organized crime, as the Justice and Home Affairs Council concluded (44). In this new age of events, particular after September 11th, it is essential to ensure that retained data is available to law enforcement authorities, therefore, the Council has examined measures for establishing rules on the retention of communications traffic data by service providers. Although, everyone has the right to seclude information relating with his private life and matters, as stated in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), public authorities may interfere with this exercise only in accordance with the law, in the interests of national security or public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others (44).

A second line of EU action has been concerned with privacy and security matters related within the context of digital identity management (Digital Agenda for Europe) (47). Most recently, the European Commission has promoted several programs regarding these matters, by promoting a few projects in several areas, like EuroSOCAP (QRLT-2002-00771), a funded project (2003-2006) established to attend the challenges and pressures of the health care sector thus providing ethical guidance on confidentiality and privacy to both health care professionals and provider institutions (48). But most important is the fact that the EU is focusing on the individuals by empowering them with tools and mechanisms to manage their own personal data in a secure way.
3 Patient Empowerment

“Do the difficult things while they are easy and do the great things while they are small. A journey of a thousand miles must begin with a single step.” (Lao Tzu)
3 Patient Empowerment

Over the last few years, the concept of ‘Patient Empowerment’ has gained increasing prominence and acceptance as the base for a patient-centered reform on healthcare worldwide, resulting on a silent massive revolution on healthcare systems ever since (49).

3.1. The definition of Patient Empowerment

Numerous studies can be found in the literature defining what ‘patient empowerment’ is. According to its very nature and underlying philosophy one can denote the existence of two ‘patient empowerment’ distinct dimensions, one inter-personal and another intra-personal, properly accompanied by the development of patient’s digital skills (Figure 3).

Therefore, ‘patient empowerment’ may be perceived either from a provider–patient interaction point of view (considered as a process of communication and education in which knowledge, values and power are shared, i.e. an interactive process where power is ‘given’ by someone to the patient) or from just
a patient point of view (considered as a process of personal transformation, i.e. power is ‘created’ within, by a particular patient), or even, as is often the case, both. Although the main objective remains the same, i.e. to gain more power over one’s life, the nature of the two processes is very different (31).

But one can ask if the concept ‘patient empowerment’ is something new in today’s society or if it is simply a new term to apply to old theories concerning human behavior and motivation within an health care scenario. There are indubitably some key features that lead us to conceive ‘patient empowerment’ integrated within a humanistic approach of human motivation and development, such as choice and responsibility, as well as the development of skills dealing with one’s disease. This postulates Maslow’s theory that there is an intrinsic propensity in humans towards self-growth or ‘self-actualization’, furthermore, the features described are very similar to the features defined in Deci & Ryan’s Self-Determination Theory (SDT), as contributing to intrinsic motivation, namely competence, relatedness and self-determination (31). Indeed, the nature of this concept is not entirely new, and many theories concerning human behavior and motivation can explain the ‘patient empowerment’s’ nature and adjacent philosophy.

Nevertheless, regarding patients’ choice and responsibility for one’s choices, one would expect the indicators of empowerment to be defined by the patients themselves, rather than by a health professional. However, some of the expected outcomes of ‘patient empowerment’ that can be found in the literature are still very medically oriented and prescriptive. As a result, they are not compatible with the principles of self-determination and responsibility, which is the case of most disease and treatment-related outcomes (31). Therefore, patients’ choice is serious affected by the fact that patients are not comfortable with today’s medical approach, which is still far from being patient-centric. Although, theoretically Healthcare Systems are focusing more on the patient and walking towards ‘patient empowerment’, in practice it is a very complex process that takes time and needs support. And by support we mean the encouragement and promotion of real partnerships among practitioners, patients, and their families (when appropriate) to ensure that decisions respect patients’ wants, needs, and preferences and that patients have the education and support they need to make decisions and participate in their own care (2).
3.2. The road to Patient Empowerment

Once health professionals accept and embrace the empowerment principle, their relationships with patients as well as the structure and process of their practices changes dramatically (49). Although implementation strategies may vary: how to tell if a patient is empowered? How to differentiate and assess empowered patients? ‘Patient empowerment’ is an extended and very demanding process; in fact it can be seen as a pyramidal leveling process as illustrated by the figure:

![Levels for Patient Empowerment](image_url)

**Figure 5. Levels for Patient Empowerment**

Access to information is the first initial step towards ‘patient empowerment’. We can only be empowered if we have access to enough quality information to be able to acknowledge and make decisions about our own condition (Level 0). Without complete access to their own health data, patients cannot assume their responsibility in an equal footing partnership relation, as they would be placed in a lower position when compared with their health professionals’ counterparts. Therefore, ‘Accessing’ information (Level 0) differentiates empowered patients from those who are ‘underpowered’. Only by being properly informed can a patient start to set goals and attain outcomes that are personally and clinically meaningful, even when not under the direct supervision of health professionals. Patients are more likely to achieve and sustain their chosen goals than those imposed by health professionals (49),
however, time is often needed to allow for patients to make their own decisions, not only about their role in today’s medical decisions but also about the privacy and confidentiality of their EHRs. Having this in mind, the power obtained by the patient in controlling the access to his own information can be exercised by actively granting or denying authorization to others to access it. Yet if this power is not exercised parsimoniously with great care, it can lead to ‘underpowerment’ as the access to privileged information loses its exceptional character, thus becoming ordinary. Therefore, granting information access authorizations in a selective and controlled way is an important prerequisite for empowerment (Level 1). Achieving this kind of patient empowerment is an act of trust that can only contribute greatly for the strengthening of the health professionals-patient partnership relation. Patients become more enthusiastic and comfortable about providing information about feelings, values, needs and abilities and therefore become a more active partner, producing relevant information that can be more effectively used by the health professional (Level 2). One can say that this sort of patient is an advanced user as they have not only some clinical knowledge but are also quite savvy in the use of Information Technologies (IT). Their experience and their knowledge are most helpful, if shared with other patients, and could even be a source of inspiration for other less advanced users (Level 3).

However, as we go up in the pyramid, the number of patients that achieves higher levels of proficiency decreases. This illustrates how arduous the journey to empowerment can be. First one needs to have the means to understand and control access to clinical information, then one need to get proficient in the use of Information Technologies (IT) and lastly, one needs to become knowledgeable about clinical content and feel comfortable about assuming some degree of control and responsibility over one’s own health care.

3.3. Healthcare in the 21st century: the changing of roles

The ‘patient empowerment’ process is transforming the conventionally assumed roles of both health professionals and patients. Quoting Anderson and Funnell: “The paternalistic approach traditionally assumed by physicians, and the maternalistic approach traditionally assumed by nurses and educators, is not effective for a
self-managed illness. Rather than a parent–child relationship, a partnership needs to be established between health professionals and the patients” (50). Therefore, nowadays the role of the health professional is to actively listen, helping the patient to understand health related self-care problems, feelings and goals, collaborate and provide information (for instance by sharing their insights about a particular patient’s medical episode), offer support and refer outside resources (for example by indicating relevant digital media health related content) (50).

Some authors consider that the patient of the 21st century accumulates various roles namely as a decision maker, as his own health manager, as an evaluator, a potential agent of change, an active citizen whose voice must be taken into account by policymakers and health care providers (51). However, one can add that the role of the patient in the 21st century is to become a ‘patient 2.0’, deeply connected with emergent new technologies as well as highly motivated to assume control and responsibility over his own health care. Web 2.0 interactive content as well as dynamic web applications are a natural means to nurture greater patient participation, thus providing more significant benefits for individuals in terms of mutual support, which might be essential regarding specific chronic conditions, such as diabetes, asthma, depression, among others (40). Information Technology therefore plays a decisive role in empowering the patient and at the same time assists the health professional, thus ultimately assuring sustainability of the empowerment process (Figure 6).

![Figure 6. Informatics’ role for increasing 'patient empowerment'](image)

- **Level 0**
  - provides secure access to EHRs and health related information

- **Level 1**
  - allows to grant authorizations to access EHRs in a secure and controlled way

- **Level 2**
  - offers tools to securely input sensitive health related information

- **Level 3**
  - provides the means to share information and experiences in a secure way
There is however one big remaining obstacle. Most of the patients that frequently need healthcare services are elderly and really do not know how to handle today’s modern technologies. So the ‘patient empowerment’ process needs to include an adjustment stage to let the patient learn to master these technologies, like for instance to access his EHRs (Level 0), before he can act and be held responsible for their own choices. Otherwise, due to elderly patient’s lack of experience working with new technologies, they would express the wish to delegate the responsibility for decision-making, mainly because they are not comfortable with the technology being used and thus failed to be empowered.

Unquestionably, in an empowerment-based approach, the focus is on how the behavior is defined as an objective to be achieved by a specific individual rather than on defining a particular type of behavior. Therefore, one can consider empowered patients not a synonym for the activist patients who, as a result of rejecting “the passivity of sick role behavior and assuming responsibility for their care (...) are more knowledgeable about, satisfied with, and committed to their treatment regimens” (31). Nevertheless, one must add that if the patient in question is not aware of the new capabilities provided by modern user-centric healthcare system’s and does not know how to work with them, can we really argue that if he does make the choice of delegating decision-making in this particular case, it was an informed and fulfilled decision? Is it legitimate to ask someone to choose or even to give an opinion on such matters when he is not aware and so could not fully comprehend the full extent of the implications of his choice? Therefore, National Healthcare Systems should not only promote actions to educate patients regarding healthiness and wellbeing but also to provide them with the knowledge about new technologies, by promoting a closer partner relationship between patients and health professionals with the involvement of both in the use of interactive electronic health systems.

All this enthusiastic feeling around the ‘patient empowerment’ process must however be taken with a ‘grain of salt’ and put into perspective by appropriate quantitative research. Further studies should be conducted in order to determine how the ‘patient empowerment’ process can be better nurtured and further actions must be taken to better motivate both patients and doctors to work in a more closed partnership to improved health care. Moreover, one needs to assess real patient’s desire for empowerment: do they wish to be empowered using an EHR? What level of ‘patient empowerment’ can
be achieved with an EHR (24)? What are the main advantages and disadvantages concerning the patient within this approach?

Focus groups interviews constitute a good tool to gather patient’s opinions about these matters. Also important is the need to assess the patients’ level of digital and health literacy, by employing appropriate questionnaires and surveys. In order to better understand patient choices we need to investigate their knowledge and skills regarding not only the use of new technologies but also how they are perceived from their point of view. This way it becomes much easier to elaborate a plan to effectively help to establish the patient’s real needs for self-empowerment. Moreover, to help them to understand and accept their appropriate role and to better understand and manage their expectations (just like in the self-service industries, such as fast food chains where the consumers know what is expected of them) and to attain knowledge about their options (an informed choice will improve the patient performance and commitment to his own healthcare).

### 3.4. Patient Empowerment by numbers: a Portuguese case study survey

In order to assess how the ‘patient empowerment’ process is being held in Portugal, we have conducted a study by the means of an interview with patients older than 18 years old. The main objective of this study was to identify and assess the Portuguese level of patient empowerment according to our pyramidal classification.

#### 3.4.1. Methodology

We have conducted an interview with patients older than eighteen years old in order to determine their opinions on matters regarding ‘patient empowerment’ and their EHRs: particularly who should have access to it and what were the reasons for those choices. The interviews were individual and were conducted by a General Practitioner (GP) on his daily consultation, in an Oporto’s Health Center in Portugal, during the last fifteen days of August 2008.
During these interviews, the GP explained what EHRs were and discussed privacy and security related issues with the patients given that we consider access to information as the first level towards empowerment. At one point the GP asked the patient the following exact question:

- If you could decide, who should have access to your EHRs?
  - Only doctors (Answer A)
  - Doctors and nurses (Answer B)
  - Any health professional (Answer C)
  - Only the health professionals that are taking care of me at the moment (Answer D)

### 3.4.2. Results

We have interviewed 100 patients: 70 female and 30 male. The graphic below (Chart 1) shows the distribution of the 70 females according to their age and education:

![Chart 1](chart1.png)

**Chart 1.** The distribution of the 70 females according to their age and education.

Chart 2 shows the distribution of the 30 males according to their age and education:

![Chart 2](chart2.png)

**Chart 2.** The distribution of the 30 males according to their age and education.
The answers given by both the women and men to the first question are presented in the following table (Table 1):

<table>
<thead>
<tr>
<th>RESULTS (women/men)</th>
<th>Answer A</th>
<th>Answer B</th>
<th>Answer C</th>
<th>Answer D</th>
</tr>
</thead>
<tbody>
<tr>
<td>18 – 24 years old (12 answers/0 answers)</td>
<td>1/0</td>
<td>0/0</td>
<td>9/0</td>
<td>2/0</td>
</tr>
<tr>
<td>25 – 30 years old (7 answers/6 answers)</td>
<td>0/0</td>
<td>0/0</td>
<td>4/5</td>
<td>3/1</td>
</tr>
<tr>
<td>31 – 40 years old (11 answers/5 answers)</td>
<td>3/0</td>
<td>0/0</td>
<td>6/2</td>
<td>2/3</td>
</tr>
<tr>
<td>41 – 50 years old (15 answers/4 answers)</td>
<td>0/2</td>
<td>0/0</td>
<td>7/1</td>
<td>8/1</td>
</tr>
<tr>
<td>51 – 60 years old (10 answers/7 answers)</td>
<td>2/0</td>
<td>0/0</td>
<td>5/7</td>
<td>3/0</td>
</tr>
<tr>
<td>61 years old or more (15 answers/8 answers)</td>
<td>8/3</td>
<td>0/0</td>
<td>4/4</td>
<td>3/1</td>
</tr>
<tr>
<td>TOTAL</td>
<td>14/5</td>
<td>0/0</td>
<td>35/19</td>
<td>21/6</td>
</tr>
</tbody>
</table>

Table 1. Survey Results

3.4.3. Discussion

The main motivation behind this study is to start to understand what Portuguese patients think about privacy issues related to access to their EHRs within a ‘patient empowerment’s’ perspective (corresponding to Level 0 and Level 1 illustrated in the pyramidal classification of empowerment levels). This could be a first step to determine what level of empowerment the Portuguese patients think they currently have restricted to and what they wish to have in the future. One must add that patients were generally very willing to participate and express their opinions about who should be granted access to their EHRs. They were also very eager to participate; some even gave personal testimonials concerning this matter, showing that most of them are well aware of their rights to privacy and the confidentiality status of their own EHRs.

By analyzing the results, Table 1 shows that 50% of the women answer that, if they could decide, *any health professional would have access to their EHRs*. Most of them commented on this choice saying that they chose this option because they think this way they would get better health care, showing some concerns regarding what could happen lest they had chosen otherwise. Some said they felt pressured to comply with all the requests made by any health professional even if their right to privacy is violated. They said that
they renounce their right to privacy mostly because of what is happening in the Portuguese NHS: a growing overloaded system (not only with patients, but also with people and processes) that is not able to respond efficiently to all of its patient’s needs and expectations. Some even added that they felt they really do not have a fair choice due to pressure on getting the best possible healthcare services: “If we get picky on choosing who should have access to our own EHRs, no health professional would treat us nicely. If I could freely choose I would prefer to keep my own EHRs private and to make it only accessible to the health professionals that are really taking care of me. But I am in no position to decide what is best for me because what really counts at the end is the doctor’s opinion. Perhaps I should not generalize this, but sometimes it is the scary truth” (70 years old). About 20% of the women answer that, if they could decide, only doctors would have access to their EHRs. They chose this option because they only trust doctors with the confidentiality of their EHRs. Some even suggested that they felt compelled to give this answer due to the social unequal relationships between health professionals and patients, with the patients standing in a lower social ranking. This behavior was more common when we analyze Chart 1 and identify that 30% of the women only have the 4th grade, thus considering themselves to be in a lower social ranking. Education level has a significant impact on people’s behaviors and affects severely their own decisions: “It’s not a fair relationship from the beginning; I could never be at the level of my doctor!” (72 years old) this behavior constitutes one of the big obstacles of the ‘patient empowerment’ process, especially for elderly people with a low level of education, because they do tend to put themselves on an inferior position thus failing to develop a collaborative partnership with their doctor, which is essential for ‘patient empowerment’.

As for men, almost 64% answer that if they could decide, any health professional would have access to their EHRs. They choose this option because they think by choosing this way they will get better health care, although a significant majority of the male patients have suggested that they did not want to control their health records. Unlike women, some men did not show empathy towards this ‘patient empowerment’ process. Nevertheless, this male tendency towards lack of care and interest is a particular characteristic of the patient sample and geographic region; we cannot extrapolate and generalize it to the rest of the male Portuguese population.

One can conclude, from the demographic variables investigated that age and level of education were the only ones that had a significant impact on the patient’s ambition to be empowered and on their
desire to have controlled access to their EHRs (Level 0 or 1). Although these results only have local implications, due to the fact that the sample extension was too diminutive to portray a national opinion, they are nevertheless relevant indicators for the development of patient oriented EHRs. Furthermore, the ultimate acceptance of such records may be related to the general extent of computer literacy within the population at large rather than the views of individuals about their health. It is however important to discuss how the patient should be involved in his/her own health care and how significant is the computer literacy impact to determine his level of involvement in the patient empowerment process.

3.4.4. Study conclusions

Further analysis uncovers the truth behind such behavior, 53% of the patients said that they answered that any health professional could indeed have access to their EHRs because they think they would be provided with better healthcare services by accepting any health professional access. Other analysis was made by searching for any significant correlation between respondents’ answers to questions, including demographic information. Some important findings were identified: 18% of the patients answer that only doctors could have access to their EHRs and within this group, 95% only have the 4th grade and 61% are more than 61 years old.

Although, we cannot extrapolate the results to the general Portuguese population, due to the diminutive sample of individuals, these numbers show that a significant part of the inquiries only trust doctors with their EHRs, not only due to the doctor-patient confidentiality’s relationship, but also because these patients believe that doctors have a higher status in the Portuguese society, unlike them who have modest qualifications. This perceived societal difference creates a gap between doctors and patients, who in fact should be partners and be working as equals for the patient’s benefit on healthcare. One can say that these patients are difficult to be empowered due to their deepest believes, social perceived status and education. According to our scale, their level of empowerment is 0 as they only have access to information.

Healthcare providers need to adopt a patient-centered approach if they want to effectively translate empowerment into their clinical practice: which requires that they get personally involved in the
relationship with their patients and implies a shift in the representation of their roles, from skilled technicians to persons, and from knower to facilitator, thus reducing the gap between doctors and patients. With empowerment, patients are expected to better self-manage their illness and be able to better ponder on their choices: some patients may decide to delegate to their doctor the responsibility for some aspects of their treatment (corresponding to Level 0 or 1), while other patients under similar circumstances would prefer to learn to self-manage some if not all aspects of their illness and treatment (corresponding to Level 2 or 3). However, this does not mean that patients should be left alone to decide what is best for them: it is the health care providers’ responsibility to provide guidance and motivation for patients to learn how to effectively self manage their illness and their lives (40). Patient empowerment is unquestionably a long process, which involves not only the collaboration of patients, health professionals and the society at large, but also appropriate integrated health information systems.

3.4.5. Recommendations

According to the European’s union report “Financing sustainable healthcare in Europe: new approaches for new outcomes” by Reinhard Angelmar, it is important to take under consideration some recommendations in order to increase patient empowerment and efficient health outcomes (52):

- **Focus ‘patient empowerment’ targets** (patients with chronic conditions are more able to assemble information and deliberate than those with emergency situations).
- **Identify critical moments in the treatment process** (analyze the treatment process in order to identify the steps where greater patient power would have the largest impact on improving efficient health outcomes).
- **Eliminate obstacles to empowerment** (which might include restructure the patient’s role by enhancing his self-efficacy and health literacy in order to better understand their options and consequentially improve his health status while developing skills to carry out the required proceedings).
- **Create a facilitating environment for patient empowerment** (this might request helping patients with information-processing in order to create the ideal environment to allow them to make informed decisions).
- **Promote equity among patients** (patients are different, and consequentially the empowerment process must be customized to attend the different patients’ needs, however one must drive efforts to help those who have lower education, bad health insurance and lower incomes who are not in a position to make informed choices than those who enjoy these benefits).

- **Motivate the empowered patient to achieve more efficient health outcomes** (by promoting a closer relationship between doctors and patients to incentive patient’s commitment to his health care).

### 3.5. Patient Empowerment and health outcomes

In recent years, the technological evolution of healthcare systems allowed doctors to perform their work in a fast and more accurate way. Although the investments on such systems were quite high, the benefits from their implementation are widely known as a paper free hospital that tends to reduce costs on material and human resources while at the same time it increases the number of patients, consequentially augmenting their incomes. In addition, the concept of ‘Patient Empowerment’ has gained increasing prominence as a solution for the needed healthcare reforms worldwide. Yet despite growing recognition of its importance, as well as evidence of its success in contributing to other system goals such as efficiency and effectiveness, worldwide healthcare systems are failing to achieve effective patient empowerment. Several studies indicate that patients often rate hospitals and medical care providers highly (as we observed in our interviews where the patients placed the doctor in a higher position), however report other significant problems concerning with how they receive responsive, compassionate service from their caregivers. Moreover, problems related with gaining access to critical information, understanding treatment options, getting explanations regarding medications, where also appointed (53). These studies indicate that there is still much work to be done in adopting ‘patient empowerment’ concepts and approaches into clinical practice. Therefore, it is imperative to properly plan this process in order to obtain the finest possible achievable outcomes involving both patients and health professionals with interactive health systems. However, little has been done to involve the patient in the process of designing these tools, although quite a few studies have demonstrated those benefits (52). This involvement could be the result of being able to participate on the decision-making, being educated
regarding his health problems and promoting a close relationship with his healthcare providers, thus leading to a substantial reduction of costs.

But does greater patient involvement necessarily lead to more efficient health outcomes? This is a reasonable question to rise because it is a question whose answer will in the end determine how much governments will be willing to invest on ‘patient empowerment’ in order to increase the general perceived quality of healthcare services. Can we really put a price on our health? The distressing true is that like all in real life, healthcare has a price too and by a simple economics calculation this can be easily estimated. We can start by considering three possible scenarios that can lead to more efficient health outcomes (Figure 7): better health outcomes with no increased cost, the same health outcomes at lower cost or better health outcomes at lower cost (52).

Figure 7. Desirable consequences of greater patient power (52)

‘Patient empowerment’ does not necessarily produce these desirable results, for instance it may lead to better health outcomes at higher costs. In a certain this could be also desirable, but it depends on the incremental costs per unit of health outcome gained, which may be unacceptably high for a healthcare system. However, better health outcomes at higher costs are easier to achieve than the three desirable outcomes specified above. Arnold Relman, former editor of the New England Journal of Medicine, and others have argued that the business model is anathema to medicine and the medical care system. Quality patient care and profits are incompatible (54). However, patient power may also result in higher costs without necessarily better health outcomes (52). Although the current field experience does not projects good future perspectives, it is a question of balancing patient’s needs, health care costs and health outcomes, in order to achieve a satisfactory and efficient solution. Further comparative studies must be conducted in order to assess the benefits gained from such approach.
Society does little to promote this type of interactive studies thus it is urgent to be more interventionist. One can wonder why the patients have not yet been asked to provide their opinion in these matters: how the ‘patient empowerment’ process should be conducted, what kind of medical needs could benefit from patient-centric systems, what kind of information they would like to be given, what are their expectations and fears, as well as to determine how and what kind of information systems can effectively help them to improve their own health care and control the privacy and confidentiality of their own EHRs (Level 1).

3.6. Challenges ahead

We are witnessing a major change in the way health care institutions are dealing with EHR’s Systems deployment and implementation: focusing more on the patient and his role. Therefore, to be a patient in the 21st century is to be deeply connected with new technologies and actively participating in his own treatment thus sharing responsibility with the physician, while pursuing medical knowledge not only about diseases but also concerning fitness and wellbeing.

According to the Healthy People 2010 report (55) health literacy is defined as: "The degree to which individuals have the capacity to obtain, process, and understand basic health information and services needed to make appropriate health decisions" (56). Health literacy is not necessarily related with one’s education level or even the ability to read or to listen, it requires that patients are able to articulate their health concerns, describe their symptoms accurately and discuss their treatment directions thus combining analytical and decision-making skills towards health situations. In addition, according to the American Medical Association, poor health literacy is "a stronger predictor of a person’s health than age, income, employment status, education level, and race" (Report on the Council of Scientific Affairs, Ad Hoc Committee on Health Literacy for the Council on Scientific Affairs, American Medical Association, JAMA, Feb 10, 1999) (57). The improvement of health literacy levels is essential not only to secure the transmission of knowledge but also to ensure that patients develop the required skills fundamental to empowerment (58). Several studies demonstrate an association between low levels of literacy and adverse health outcomes (59). One can find evidence of this for diseases
such as Diabetes, Cancer HIV and Asthma where there is a clear correlation with mortality rates (60) (61). Therefore, Health illiteracy is a major obstacle for this new type of emergent patient care hence it blocks the possibility of making informed choices.

As a result patients are expected to develop interest in their own health, seeking health related information and elaborate thoughts on what their treatment directions should be (62). Thus truly establish a partnership relation with their physician. On the other hand physicians need to take time to support their patients direct needs of health information by providing materials that are culturally appropriate and easy to read, and to teach patients how to evaluate health information resources, especially those found on the Internet (63). Therefore, we need to start training and preparing student physicians at the medical schools so that they are able to properly support and teach their patients.

This scenario is highly favorable to the patient empowerment process thus health care providers should promote the patient’s knowledge and training in new technologies as well as making them aware of their rights and responsibilities. Many observers believe that planning for the new healthcare environments of the 21st century requires not only a profound understanding of the role that information technology is likely to play in those environments but also how the patient should be active participant in the managing of his healthcare (64). Recently developments regarding these matters are facilitating the patient to manage access to his EHRs thus assuming the role of pro-active consumer, with the ability to make his own choices and be held responsible for them. We can help to make major improvements on health care services by developing EHRs systems that allow patients to control and help the flow of their own health data and to promote a closer relationship between patients and medical professionals involving both in the practical everyday usage of user-centric interactive health systems (65). Quoting Charles Safran: “… [When patients] participate more actively in the process of medical care, we can create a new healthcare system with higher quality services, better outcomes, lower costs, fewer medical mistakes, and happier, healthier patients. We must make this the new gold standard of healthcare quality and the ultimate goal of all our improvement efforts: not better hospitals, not better physician practices, not more sophisticated electronic medical systems. Happier, healthier patients” (66).
4 Identity and Privacy mechanisms

“Begin at the beginning and go on till you come to the end; then stop.”
(Lewis Carrol, Alice in Wonderland)
4 Identity and Privacy Mechanisms

Quoting Schloeffel et all (67): “The greatest challenge in the new world of integrated healthcare delivery is to provide comprehensive, reliable, relevant, accessible, and timely patient information to each member of the healthcare team, whether in primary or secondary care and whether a doctor, nurse, allied health professional, or patient/consumer”. Therefore, it is important not only to ensure secure access to EHRs but also strong identification and authentication mechanisms so that patients can begin their empowerment journey with strong confidence that their privacy can be safeguarded in the whole process. Such mechanisms are currently available, the question is what mechanisms to choose, how to use them and in what context. Although it does not exist an unique answer and solution for the deployment of these health self empowering mechanisms, in what follows we present the rationale behind what can be considered an acceptable implementable approach that could function as the foundation for a technical solution for such mechanisms. We start by provide background information on the OpenID user centric identity management system (which can be used to empower patients in level 0 of the pyramid of empowerment levels) and OAuth authorization standard, which allows to authorize third-party applications to access web resources upon token’s verification and approval (and therefore be used to empower patients in level 1 of the pyramid of empowerment levels). In addition, we describe how smart cards can be used to allow for strong authentication mechanisms to be applied in health care scenarios (thus it can be used to empower patients in level 0 and level 1 of the pyramid of empowerment levels).
4.1. **OpenID, a self empowering identity management system**

OpenID is a decentralized system protocol for user-centric identification and digital identity management in the Internet. It was created in the summer of 2005 by an open source community. Soon after, the OpenID Foundation was created to assist the open source model by providing a legal entity thus contributing to help and support the general worldwide adoption of OpenID (68).

Regarding the patient empowerment process, it is essential to provide patients with tools that will help them not only to provide secure authentication and access to their health care information spread among different HISs across the Internet, but also to act upon that information, ultimately sharing it with the health professionals they wish to.

Therefore, we consider that OpenID embodies the ideal self empowering tool for patients to secure manage their identity in HISs across the Internet. First, because it is based on a community-driven development effort, with many components proposed as IETF (Internet Engineering Task Force) projects. Therefore, anyone can become an OpenID consumer (service) or an OpenID provider (IdP). In addition, all OpenID providers can authenticate users for all consumers without the need for groups/federations/circles of trust. This will allow health institutions to easily comply with the OpenID authentication process. Besides, OpenID is a “single sign on” (SSO) system, thus it eliminates the need for multiple user names and passwords across different security domains, i.e. in the OpenID universe relying parties. A relying party, sometimes designated has “service provider”, is a website that wants to determine the end-user’s identity.

Hence patients have their health information scattered among different HISs across the Internet it is difficult to remember all the multiple usernames and passwords and therefore security is often compromise since they regularly use the same password for different HISs or “123” alike passwords. With OpenID, patients and health professionals can use a single, existing account to sign in to different HISs without ever needing to memorize another. In addition, since conventional passwords are not centrally managed, if a security fail occurs in a particular HIS, a third party could gain access to the patient’s
password. With OpenID, passwords are never shared with any HIS, only with the patient’s identity provider (IdP), which then confirms the patient’s identity to the HISs he visits. However, if a compromise does occur, the patient can merely modify his OpenID credentials, thus instantly preventing the attack.

Also, OpenID allows for the simplification of the user online experience. Indeed it constitutes a very good approximation of real life identity brought to the digital world. The use of digital personas (which are subsets of attributes and credentials for the user across multiple services) could be applied regarding health identities (69). Patients could easily create their Health Personas (HPs) with attributes they consider to be fitted (such as blood type, known allergies, immunizations, among others), which can then be stored through their OpenID and used to pre-populate registration forms thus simplifying the process. Because OpenID is a decentralized protocol, it is not controlled by any website or service provider. It allows the user to control how much personal information he wants to share with HISs that accept OpenIDs, and multiple OpenIDs can be used for different HISs or purposes as well (70) (71).

4.1.1. OpenID Authentication process

The OpenID identity and authentication operational mechanisms are simple and work in the following way: when a user wants to sign into a website, a “Relying Party” (RP), he/she has to choose an OpenID Identity Provider that is trusted by the RP and best meets the user operational and management requirement for his digital identity. The OpenID Identity consists of a unique Uniform Resource Locator (URL). This URL is used by the owner to identify him at a website that relies on OpenID for identity and authentication and acts as an OpenID relaying party (68). During normal usage, the user submits his OpenID (URL) to the relying party, who uses the host DNS address on the identifier to locate the OpenID identity manager in the Internet. This corresponds to the identifier’s home address and constitutes one of the nice features of OpenID, namely the identity home address is embedded into the identity itself, something that is not so common on other identity management systems, like shibboleth for example, where the user has explicitly indicate his home address. The relying party optionally associates and establishes a shared secret with the identity provider (both shared secret and session should be encrypted). The relying party then redirects the user’s browser to the identity provider site. The user
then logs in with the identity provider with his actual credentials, which are then verified (70). The verification between the Relying Party and the Identity Provider is processed by using a mechanism that verifies the assertion: the check_authentication message. The check_authentication is a direct, out of band, communication that uses HTTP POST method between the Relying Party and the Identity Provider. Once the Identity provider has received this message, it will determine the validity of the assertion and reply back with a “yes” or “no” answer. The “is_valid” parameter present in the message shows the success or failure of an assertion. Once the Relying Party has received this success message, the authentication process is complete and can then allow the End User to login to the Relying Party web site.

The Relying Party (RP) can also take other actions: if the Identity Provider did not return all of the requested parameters, it may grant lesser level of access to data or if it is the first time that a user has logged into the web site, the RP may also go through his own complementary registration process. Yet, the RP actions after the completion of authentication process are out of the scope of the OpenID protocol (72).

![Figure 8. OpenID authentication process (68)](image)

### 4.1.2. OpenID advantages and future perspectives

The advantage of such a system is that the user does not need to register on any OpenID enabled website as soon as he owns an OpenID identity on a reliable OpenID provider. He just has to select or even pre-select the attributes he wishes to share in different web sites for registration purposes. These
attributes are “attached” to his digital OpenID personas, thus eliminating the need for memorizing different passwords or even several usernames for the different web sites he uses, thus minimizing the problem of too many multiple identities. There are however some well known security issues that need to be addressed (70):

- **Trust:** once authenticated the RP can only assume the user owns the identifier, but not whether both the user and the identity provider are trustworthy enough.

- **Security:** OpenID can be susceptible to Phishing/Spoofing attacks (users are tricked into entering their password in a forged identity provider webpage or vulnerable to man-in-the-middle attacks via cross-site scripting requests) or even denial-of-Service attacks hence the OpenID Identity Provider is a single point of failure.

- **Spamming:** spammers can register a large number of throwaway identities.

The OpenID community is developing solutions to mitigate these problems: the development of Firefox plugins that allow users to authenticate themselves in their OpenID identity provider is one solution for combating phishing and spoofing. Another useful security mechanism is also being developed: OpenID Provider Authentication Policy Extension (PAPE). This extension to the OpenID Authentication protocol provides a mechanism by which a Relying Party can request a particular authentication policy to be applied by the OpenID Provider when authenticating an End User (68). This extension also provides a mechanism by which an OpenID Provider may inform a Relying Party which authentication policies were used, thus a Relying Party can request that the End User authenticate, for example, using a phishing-resistant or multi-factor authentication method, such as the use of security tokens, smart cards or biometrics (72). Also the reliance on trustworthy PKIs and the use of X509 certificates for both the End User and the Identity Provider can confers a more trustworthy characterization for both and increase the level of security for the identity and authentication process.

Nowadays OpenID is rapidly gaining acceptance on the Internet. Over 50 000 websites already accept OpenID and there are more than 1 billion OpenID enabled user accounts (68). The tendency is that these numbers keep on rising for some time to come. One can say this is mainly due to the fact that
the big worldwide Internet players, like Google, Microsoft, Sun Microsystems, MySpace, AOL, IBM, and Yahoo!, among others have already adopted and are actively promoting OpenID as a practical and viable distributed Identity management framework for the Internet.

However, one of the major social network websites (Facebook), instead of employing OpenID, is deploying a proprietary web identity framework, the Facebook Connect, very similar in concept to OpenID but antagonistic in terms of the open standards being promoted and developed by the Web community (73). This framework is part of a general web trend manifested by the concept of social identity. A social identity is composed not only by the user’s individual digital identity but also by its associated social graph, i.e. the list of connections the user has established online in social networking sites, together with the activity stream resulting from their inner communications (74).

Social identity is thus becoming essential regarding online applications. Nowadays it is no longer sufficient for a user to be simply registered in a website, without enjoying the social services being offered for communication that result from the site integration with the services provided by social networking sites and that can take advantage of social identity. Social identity systems permit the user to login and then be able to refer to and access his social connections and communicate with them (74).

On the other hand, there are other social web mechanisms for managing authorizations that can be combined with an open web identity, such as OpenID, which ultimately will allow users to share resources with other socially enabled websites.

![Figure 9. New approaches to user identity and external data access (74)](http://example.com)
4.2. OAuth, granting authorizations on the Internet

OAuth (Open Authorization) is an open standard for authorization and delegation created in 2007 by a group of OpenID enthusiasts (75). OAuth 1.0 was published in December 2007 and rapidly become the standard for web-based access delegation. In April 2010, OAuth 2.0 was published as RFC 5849.

Unlike OpenID, OAuth is completely transparent to the users, which is very important concerning usability issues and user experience. When a user wants to make some resource available to a third party, instead of disclosing its own credentials, OAuth allows the user to provide a third party with an authorization in the form of a special token that gives conditional access to a specific resource. The general idea is that the resource owner grants limited access to the bearer of a certain valid token, without having disclosed his own credentials that would provide unlimited access to everything. Just like a ‘valet key’ that comes with many luxury cars, which allows the parking attendant to park the car while the owner has the regular key, only allowing him to drive a short distance, blocking access to the trunk and other onboard utilities (75).

In an eHealth context, OAuth can be employed to allow the patient to provide limited access to his EHR (lab tests, x-rays, medication lists, discharge notes, among others), without having to disclose his own username or password. This functionality is critical for the empowerment process hence it allows the patient to securely share with whom he wants, when he wants, a specific subset of the EHR. This corresponds to level one of the empowerment levels’ pyramid.

4.2.1. System Architecture

OAuth is an authorization delegation protocol, and therefore it was conceived to allow the service provider to trust the consumer and validate the token granted for gaining access to the resources. In order to accomplish that, OAuth describes a method for validating the authenticity of HTTP requests, which is designated by Signing Requests (75).
An example of usage could be when a user wants to post in his blog a video stored on another site, for example Youtube. This delegated access scenario (known as the 3-legged scenario), involves three parties: the Service Provider (who has the resources), the Consumer (who makes the requests), and the User (who owns the resources). In addition, OAuth includes two kinds of tokens regarding its delegation workflow: Request Token (needed for requesting access to a specific resource) and Access Token (need to access the requested specific resource) (75).

Therefore, the consumer (in this case the user’s blog web page on Blogger) places the request for accessing the resource (a specific previously selected video by the user) by sending a request_token to the service provider (in this case Youtube) (Figure 8). In order to be granted access to the resource (the
video), first the consumer (Blogger) has to authenticate itself with the service provider (Youtube). Therefore, the service provider (Youtube) sends back a grant request_token that the consumer (Blogger) redirects to the authentication web page of the service provider (Youtube). The user authenticates himself in the service provider (Youtube) and authenticates the authorization token or not by accepting or refusing the request made by the consumer (Blogger). If the user accepts the request, an authorized request_token and an acknowledge authorization message are exchanged and the user’s browser is redirected to the consumer web page (Blogger), otherwise it will not be granted access and the token is revoked without the need to change passwords. The consumer (Blogger) uses his access_token, which was authenticated by the user, to be granted access to the requested resource (the video), which now the service provider (Youtube) complies. At this stage the authorization delegation process is complete and the consumer (Blogger) can initiate the access to the protected resource (video) stored in the service provider (Youtube). At no point did the user share his username and password with the consumer (Blogger). This was done by using two sets of credentials: the Consumer Key and Consumer Secret (used by Blogger), and the Token and Token Secret (used to identified the user), which allows for greater user control and flexibility in granting access to resources.

We can summarize the benefits of using OAuth as follows (74):

- **Secure third party data access**: the user will be able to give consent for a specific application to access his data on another website without having to share his credentials in the process.

- **Revoking third party access**: the user can also refuse access to a third party that he previously authorized without the need to authenticate in its application.

- **Transparent use of third party applications**: many applications do not handout user’s credentials to websites they do not trust, therefore by using APIs to comply with security impositions; third parties can become trustable to the user’s eyes.

### 4.2.2. Introducing OAuth 2.0

In May 2010, the IETF OAuth Working Group published the first draft of the OAuth 2.0 protocol, which is a completely new protocol and is not backwards compatible with previous versions (76). Some of OAuth 1.0 main areas were re-engineered and improved since they proved to be incomplete.
or confusing. OAuth 2.0 overcame some of the main issues by introducing an authorization layer and separating the role of the client from that of the resource owner. As a result, when the client requests access to protected resources, which are controlled by the resource owner and hosted by the resource server, instead of using the same set of credentials for client and resource owner, he obtains a different access token issued by an authorization server with the approval of the resource owner denoting a specific scope, duration, and other access attributes (76).

OAuth 2.0 offers the following new functionalities (76):

- The cryptographic requirements of the specification were simplified.
- Introduction of bearer tokens with a cryptography-free option for authentication which is based on existing cookie authentication architecture.
- Introduction of short duration tokens with the option of renewing them periodically.
- Separation of roles between the authorization server from that of the resource server handling API calls.
- New methods for obtaining access tokens (flows):
  - **User-Agent Flow** – for clients running inside a user-agent (typically a web browser).
  - **Web Server Flow** – for clients that are part of a web server application, accessible via HTTP requests.
  - **Device Flow** – for clients executing on limited devices, but where the end-user has separate access to a browser on another computer or device.
  - **Username and Password Flow** – used in cases where the user trusts the client to handle its credentials but it is still undesirable for the client to store them.
  - **Client Credentials Flow** – the client uses its credentials to obtain an access token.
  - **Assertion Flow** – the client presents an assertion such as a SAML assertion to the authorization server in exchange for an access token.
4.3. Smart Cards

Smart cards are exploding worldwide and are a solid and proven technology. In 2008, 5.045 billion smart cards were shipped worldwide — a 13.2% increase over the 2007 figure of 4.455 billion. Because of their size, flexible form factors, and relatively low cost (hence it is needed a smart card reader and a communication device to be able to actually read their data), smart cards are ideal for applications in health care where personal identity, privacy, security, convenience, and mobility are key factors (77). Therefore, smart cards can be used to implement strong authentication (hence establish one’s identity is crucial in any secure system), differential access to data (ensuring patient’s EHR confidentiality while conferring access to resources to authorized users), store important information (not only certificates to verify one’s identity but other data that can be share upon the PIN introduction), and definitive audit trails (allowing the patient to effective control the flow of his EHR), thus providing the mechanisms to enable trust in communications (78). Moreover, smart cards have the ability to dissociate data and encrypt information thus protecting individual’s right to privacy while still allowing multiple health care institutions to share patient information more efficiently by having the card act as an unique identifier. Smart Cards are indubitably among the few electronic devices that enhance control, confidentiality and privacy, which are generally recognized as being pillars of ethical practice and therefore essential for improving patient empowerment when combined with other confidential-control-privacy driven technology (79).

Some countries already have smartcard-based healthcare technology, such as USA (since the late 70's) (79), Germany (since 1989) (80) (81), France (1998) (82), Slovenia (since 2001) (83) and more recently England (84). It is important to denote the Taiwan health care smart card project, which is one of the largest health care smart card solutions (since 2001) (85). Therefore, one can say that this technology is becoming an important tool for implementing paperless systems in health care worldwide since they can be used to provide strong authentication for both patients and health professionals.
4.3.1. What is a Smart Card?

Smart cards are memory only or processor-enabled semiconductor based technology that enables identities to be securely authenticated and communications to be protected. Moreover, smart cards can also carry data such as personal details as they have bi-directional data flow: data is read from, as well as written to the card (“read-only,” “added-only,” “updated-only,” or not accessible), which can therefore prevent data from being altered or temperate with (86). The access to the data can only be performed with the user’s permission by entering a PIN code settled at the time of issuance. As this information is encrypted, it ensures that only authorized personal have access to the stored data in case the card is lost or stolen. Smart cards can additionally increase the level of identity verification by storing other identity information as qualified digital signature and biometric fields (78). Therefore, they are extremely common on mobile communications (SIM – Subscriber Identity Module - cards), or even on banking transactions (Credit and Debit cards), as well as on physical access control management, transportation and digital identity (Library and Citizen’s cards) (87).

Smart cards communication is made via an interface by contact, contactless or both as defined in the international standard ISO 14443 or ISO 7816 for smart cards with contacts (88). To a contact smart card communicate with a computer, it is required a smart card reader that is often connected via USB (Universal Serial BUS). As for contactless smart cards, they communicate with a card reader through a known wireless interface protocol designated by radio frequency technology (89). This type of smart cards enable fast transactions with devices, and are used, for example, in mass transit systems (such as toll charge systems) and transportation as in the Oporto subway system (Metro do Porto) where it acts as a central unique system of purchase, validation and supervision (90).

4.3.2. Advantages and disadvantages of smart cards in healthcare

An identity and authentication solution based on smart card technology currently provides one of the best options for improving HISs in a secure, private and sensitive way, moving healthcare towards information management as a public utility rather than a personal millstone. Most agree that the use of this
type of technology is essential to achieve many critical milestones for health care reform. The need to meet increasing privacy, security and identity concerns, as a result of governments’ directives is one of these milestones (91) (92) (93) (94). We can argue that we can have other benefits regarding administrative efficiencies and reducing medical errors from duplicated or overlaid patient records. However, the main advantages of such an application in health care are related with enabling patients’ and health professionals’ identity to be authenticated and the communications between HIS to be secured thus settling the conditions for the patient to grant health professionals access authorizations to his EHRs. Therefore, smart cards can act as a key for providing the required mechanisms to improve the patient empowerment process however not in a standalone conception.

On the other hand, smart cards usage can produce serious disadvantages, mainly because it introduces a point-of-failure in the system. This way the systems becomes more vulnerable to technical problems such as power or network failures, software bugs, equipment malfunctions and damaged cards, among others. Therefore, this is not an acceptable situation on critical services like in health care. Furthermore, the hardware and software costs to implement such a system can be quite considerable as it is required a card reader and the existence of a public key infrastructure.

4.3.3. The Portuguese Citizen’s Card (CC)

Many governments worldwide are currently making huge efforts for technological modernization and innovation. This is also becoming a reality in Portugal, where the Portuguese government has also realized the strategic need to innovate and modernize public’s administration infrastructures. One key ingredient is the new national identity card, the “citizen card” (Cartão de Cidadão – CC), which is basically a smart card that provides
identification (ID number, Tax payers number, Elector’s ID number, National Health System number and Social Security number) to all Portuguese as well as support for strong PKI X509 digital signatures and authentication certificates. This technology creates a perfect opportunity for the government to review public administration information, processes and applications architecture, both locally and centrally, especially in the area of user provisioning, authentication procedures, role based authorization and digital signatures of documents and associated processes (95).

Our proposal is to use the CC combined with Digital Identities to provide strong authentication for patients and even health professionals so that patients are able to grant health professionals access authorizations to his EHRs scattered among different HISs.
5 Health Digital Identity scenarios

“Divide each difficulty into as many parts as is feasible and necessary to resolve it.” (Rene Descartes)
5 Health Digital Identity

Scenarios

Today’s ‘patient empowerment’ process is becoming a central issue for health care providers worldwide as they face new challenges in achieving better and personalized health outcomes. By being more focused on the patient, health care institutions can gain the collaboration of an important active player and help to revolutionize the way health care is provided.

In this chapter we describe how digital identities, and other security mechanisms, such as authentication and authorization can be used by both patients and health professionals to help in nurturing the patient empowerment process. We can combine strong authentication mechanism with appropriate authorization protocols so that the patient is able to share his EHRs with the health professionals he desires to. This will allow him to be empowered into level one of the empowerment levels’ pyramid. We have identified two usage cases where the patient empowerment process could be readily enabled using current technologies: during consultation time and emergency situations. In such case, a 'break-the-glass’ (BTG) policy can be applied to override access controls mechanisms in a secure and auditable manner (96). In any of these scenarios the patient is notified of who had access to his EHR, for how long and what was the purpose of such consultation. This allows the patient to audit and directly monitor access to his EHRs, ultimately finding unsolicited requests and act on them. This should enhance the need for changing health behaviors but it requires strong efforts in patient’s education, information provision and supportive tools, more suitable to help the patient in better personalizing his health care interactions and better define the way his EHRs can be applied on his own best interest.
5.1. Improving Patient Empowerment

Health care providers worldwide are adopting a patient-centered approach to effectively incorporate patient empowerment into their clinical processes (52). This requires more hospital staff involvement with patients and implies a gradient shift in the representation of their professional roles, from skilled technicians to persons, and from knower to facilitator, thus reducing the existing social gap between doctors and patients. By being empowered, patients are expected not only to be able to better self-manage their illness by better pondering their choices. One of the manifestations of patient empowerment, is the ability to self manage who can access EHRs, with or without the help of HISs. This enables a much more decentralized approach regarding health care management (Level 0 and 1), where information systems play a decisive role in empowering patients by providing them with the appropriate tools to help them better manage their interactions with medical staff and help secure their EHRs.

The path to patient empowerment crosses patients and medical staff identity systems, strong authentication mechanisms and appropriate role management for clinical settings. The Portuguese citizen’s card (CC) is an identification document that can be used by patients as a means to transpose real world national authentication mechanisms to the clinical world, in an economic and secure way. We have also the opportunity to leverage popular, proven identity management systems to provide in a flexible way the identity infrastructure we need to put in place for the development of more effective patient empowerment systems. We argue that the OpenID framework with the support of a strong PKI national infrastructure based on smart cards for strong authentication could constitute such a base. One possible instantiation for this scenario could be the employment of the Portuguese CC for the secure authentication into decentralized trustful OpenID patient identity management systems. For health care providers, the challenge resides not only in securing the funding needed for the deployment of new technologies, but also in weighing their potential benefits against their costs. We argue that to embrace the Portuguese CC in health care together with flexible proven identity management infrastructure is to exploit a new opportunity to simplify the secure self management and provide secure access to patient’s clinical identity attributes thus helping in securing EHRs in a very flexible and economic way.
The Extended OpenID project (eOID) is a conceptualization of this opportunity and the project's main goal was to enroll the citizen with the possibility to enjoy Internet services in a more secure, user-centric and accessible way, by using their CCs to self-provision and strongly authenticate a OpenID digital identity (97). We have adapted and evolved eOID for health care scenarios, therefore contributing to the empowerment process by increasing the security of Level 0 and 1 of the empowerment levels' pyramid.

5.2. Health care Digital identities

Digital identity can be defined as a set of characteristics that uniquely describes a digital subject and its relations with other digital subjects (69). We can partition the full set of entity attributes to produce a multitude of “partials identities” or personas, one for each relevant partition and according to different “day-to-day” situations or roles, just like what happens in the real world (Figure 11). These characteristics or attributes can eventually change over time or even be certified by third parties thus adding a trusting character to it. Although each individual can have a multitude of personas, a different one for his day-to-day activities, we are particular interested in identifying what are the most relevant health care related personal attributes. These we designate as his Health Digital Identity (HDI). We argue that the HDI can play a very fundamental role in assisting patients to manage their own EHRs.

Figure 11. An individual’s partial identities
In the digital world we are building a virtual society based on our relations with others. Although, these principles and concepts may not be new, the means in which they are processed is used to produce a distinctive impact on its application, thus conferring a whole new dimension to it. Therefore, it is not only important to understand the mechanisms and roles behind the creation of an HDI, but also how much control patients will be able to take – or will want to take – over their HDIs (69). In what follows, we describe some identity, authentication, authorization and role delegation (IAAR) scenarios with patient and medical staff actors, supported by eOID and OAuth.

5.2.1. **Health Digital Identity (HDI)**

We consider that a patient HDI needs to have three main sets of attributes: the personal data, clinical information and special attributes. The patient personal data is often requested for registering or billing purposes and it is always a part of a clinical episode. According to doctors, the clinical information that is more relevant to be part of HDI is the set of attributes described below. In addition, we consider that the patient should have special attributes: the ability to add as much attributes to his HDI as he is pleased, as well as to have authentication and signature certificates stored. Therefore, with the help of a group of physicians, we considered the following attributes as to be integrated into a patient Health Digital Identity (HDI):

<table>
<thead>
<tr>
<th>Personal Data</th>
<th>Clinical Information</th>
<th>Special Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Full Name, Date of birth and Gender</td>
<td>• Preference hospital, preference health center (designation, GP name)</td>
<td>• Authentication and signature certificate</td>
</tr>
<tr>
<td>• Home Address, Telephone, Cellphone, Email</td>
<td>• Medication in current use</td>
<td>• Extra attributes (Attribute Designation, Value)</td>
</tr>
<tr>
<td>• Emergence Contacts (Name, Cellphone, Kinship)</td>
<td>• Known Alergies</td>
<td></td>
</tr>
<tr>
<td>• National ID number, Tax payer's number, Social Security number, National Health System number</td>
<td>• Known Chronic illness (Designation, Date)</td>
<td></td>
</tr>
<tr>
<td>• Insurance or care plan information</td>
<td>• Imunizations (Designation, Date)</td>
<td></td>
</tr>
<tr>
<td>• Surgical procedures</td>
<td>• Medical devices (Pacemaker, prostheses, among others)</td>
<td></td>
</tr>
</tbody>
</table>

**Table 2.** Patient's Health Digital Identity basic attributes
The eOID authentication is made by using the digital authentication certificates stored in the Portuguese citizen card (CC). In the server we validate the certificate and compare its attributes with the ones that have been saved when the identity was first created. The patient can self enroll by registering a digital identity on a pre-approved eOID identity provider. This step could be performed at home by previously requesting to join this service at the patient’s primary care center or at the primary care center. Upon registry, the system then checks the validation of the authentication’s certificate. This includes the consultation of the revocation list provided by CC PKI. If the user certificate is valid the eOID’s authentication system associates the received certificate with the user’s internal credential and copies several identity attributes from the certificate to the patients HDI (97).

Health Information Systems need to be modular, secure, and nowadays web-enabled. Much of the current thinking on distributed computing environments in health care is based on previous work and results produced by the (then) OMG Corbamed taskforce, and the Distributed Healthcare Environment (DHE) research done in Europe by several EU-funded projects such as RICHE and EDITH, and the HANSA and PICNIC implementation projects (98). We do not believe it is a good idea to build a national health framework based on the notion of a single EHR for every Portuguese citizen. Building such a centralized system would prove to be enormously challenging, not to mention the substantially increased risk of major health information disclosures and very serious privacy risks associated with such an amount of centralized available sensible health information. Instead, we argue that from the security point of view, and from a privacy point of view, the best interest of patients is served by maintaining the different EHRs as they are, distributed throughout several providers, but with access control based on the provisioning of identity and authorization through the means of trusted federated nationally recognizable digital identity.
services. Our approach is thus to help nurture the development of a truly distributed, scalable, and reliable health care information system that can take advantage of a federation of Health Identity Providers for patients. The notion of a distributed health computing environment is a key part of our vision. Our intent is to develop a distributed modular system to provide each Portuguese citizen with a Health Digital Identity (HDI) that could enable them to securely access their EHRs, scattered throughout different heterogeneous healthcare institutions. This infrastructure would enable patients to use their health information in the most convenient way, at their own discretion and at the same time to share it with health professionals as needed, ultimately providing them with important health information that will certainly help them in achieving much better health outcomes.

It is essential to stress the importance of developing an appropriate architectural model for provisioning digital identities in healthcare information systems. It is vital to identify and define exactly each stakeholder’s responsibilities, by providing guidelines by which the process must be conducted thus nurturing a more productive cooperation between the parts.

We have identified relevant stakeholders among the different Portuguese Health organizations to start to define appropriate system architecture. We consider that the patient Health Digital Identity (HDI) could start to be deployed by the Portuguese Health Administration (ACSS – Administração Central do Sistema de Saúde) (99).

Nowadays, relational database technology has grown to the level where systems can store hundreds of terabytes of data in a database cluster using Storage Area Networks. However, the centralization of all information in a single system, besides raising serious privacy and increased risk related issues, leads to a central point of failure that needs to be remedied by the use of expensive high availability equipment supported by very expensive system administration infrastructures. Our proposal is to partition data geographically (according to the locations of the different Regional Portuguese Health Administrations, ARSs – Administração Regional de Saúde, which are supervised by ACSS), using a user-specific identifier, so that user-specific data is located within the same administrative domain, thus preventing data queries that span multiple, geographically distributed partitions (100).
5.2.2. Medical Digital Identity (MedDI)

The use of digital identity certificates and federated identity systems provides the means to assure health professionals the opportunity to use their credentials in multiple health environments from different health institutions or within the same health institution but across different HISs (52). Simultaneously, this will allow certifying health professionals with the secure credentials in order to be authenticated on different HISs. Our proposal is to use the eOID Identity Provider to meet the requirements for providing health professionals with a Medical Digital Identity, which ultimately will allow them with one sign-in, hence it is an OpenID identity, to securely access the data they require to provide the best quality care at any given time.

Moreover, it is common knowledge that physicians dislike the login schemas that are usually imposed by HISs. The main consequence is that systems become vulnerable as physicians find ways to circumvent and shortcut the security system by (101):

- Sharing their passwords among themselves or with other members of the health staff.
- Using one universal login that is written directly on all monitors.
- Writing usernames and passwords in notebooks, on pieces of paper, and even directly on the monitors.
- Using easy to remember passwords, such as “123”.
- Leaving the session open without logout thus avoiding login again.

These are well-known security problems (102) which of course imply that non-repudiation and associated action responsibility is lost. It is thus fundamental to simplify not only the authentication process but also to increase the security of HISs in a more transparent way to its users. We believe that the use of digital identities and smart cards can help achieve this goal by the reasons we have previously mention and discussed: the improvement of the patient empowerment process and promoting the secure access to EHRs.
Nowadays, medical ID cards issued by the Medical Order have already a set of attributes that are important to attest a genuine doctor, therefore we considered that these attributes need to integrate an health professional Medical Digital Identity (MDI):

- **Personal Data**
  - Full Name, Date of birth and Gender
  - Home Address, Telephone, Cellphone, Email
  - National ID number, Tax payers’s number, Social Security number

- **Academic Data**
  - Education (degree, institution, date of conclusion)
  - Date of entry in the Medical Order

- **Occupational Data**
  - Name used in clinical practice
  - College of specialty
  - Regional Health Section

- **Special Attributes**
  - Authentication and signature certificate
  - Extra attributes (Attribute Designation, Value)

**Table 3.** Physician’s Digital Identity basic attributes

As the main sources of truth for the identity attributes composing the MedDI, the professional orders (Medicine, Nursing and Dentistry) are being challenged and pressured to deploy a MedID smartcard or make temporary use of the CC card (as is being done in other European countries (84) (94) (95)) to create the conditions for a strong authentication mechanism to be employed for the MedID. Health information is perhaps the most critical information about an individual and in the wrong hands it would certainly create havoc into their lives. Therefore, we need to be able to authenticate an health professional in a secure and highly indisputable way before being able to trust the attributes present on a MedID.
The authentication process within the eOID server could be made by using the digital authentication certificate that could be stored in a health smart card (medID card) or take advantage of the authentication certificate already available at the health professional personal CC to authenticate the owner of the MedID into a trusted health professional identity provider, thus avoiding the need to issued yet another smart card.

To enroll into the eOID as an health professional, he/she needs to authenticate and register a MDI. Upon registry, the system then checks the validation of the certificate and consults the list of revoked certificates provided by issuer PKI. In the case of using the certificate stored in an health professional CC card, the system needs to validate the certificate in the professional order PKI.

We suggest that the entity responsible for the deployment of both the Certificate Authority and the Identity Provider should be the Portuguese Medical Order (Ordem dos Médicos) and others for nursing and dentistry.

5.3. Granting secure access to EHRs

In the Portuguese legislation the patient owns his EHR and can access it with the supervision and guidance of his GP, upon patient request (Article 11º, n.º 5 of the Law n.º 67/98, 26 October – Personal Data Protection Law, and Law n.º 94/99, 16 July Documents Access Law) (103). Regarding EHRs several efforts are being made so that the patient is entitled to have a copy of his own EHRs when required (103). This will allow patients to have access to their EHRs that are normally scattered among several different healthcare institutions, thus allowing them to share their EHRs with the health professionals they need and wish to. The key feature in our vision is to provide the patient with the tools to share his EHRs in a fast, reliable and secure way, without having to reveal his access credentials in the process. It is indubitably an essential contribution to the empowerment process – level 0 and 1. We thus present the basics for a simple and flexible solution that enables the patient to grant authorizations to his own EHRs.
5.3.1. Using OAuth to grant secure access to EHRs

Current health-oriented websites offer innovative services integrating functionalities from very diverse systems. This interoperability among different applications is highly desirable, but the same cannot be said about some of the interoperability implementations available today in the way they handle patient sensitive data and credentials, like user name and passwords (104). When a patient inadvertently shares his secret credentials with someone else he gives him full access to his account and personal data.

The OAuth security mechanism allows the user (patient) to grant access to his private health data residing on one site or application, often called a Service Provider, via an API to another site or application, often called a Consumer (104). While OpenID can be used to allow a patient to sign on into many HISs or applications with the same digital identity, OAuth can be used to grant conditional access to patient data without having to share his identity at all (or his credentials). Employing this type of security mechanisms is extremely important and helpful regarding users privacy in the matters of managing EHRs. More generally, OAuth creates a freely-implementable and generic methodology for API delegation of authorization. By combining the OpenID protocol with OAuth we can arrive at a simple solution, more centered on the individual that can effectively help patients to be empowered by gaining an easier, more flexible and secure control over the dissemination of their own personal health data.

Moreover, we want to explore new ideas in the use of ‘valet key’ authorization mechanisms for the issue and user-centric management of temporal automatic access authorizations for strongly identified entities on a federation of trusted identity providers. The ‘valet key’ concept is a specially issued credential the owner of the data gives to another entity, in order for this entity to have conditional access to his data. Regardless of what restrictions the valet key imposes, the idea is that the owner gives limited access to his data to the bearer of a certain ‘valet key’, while he continues to use his regular key to access everything. We are currently exploring the concept of ‘valet key’ with an implementation combining OpenID with the OAuth protocol (104).
5.4. Registo Central de Saúde (RCS)

In order to employ such delegation of authorization scenarios, we considered that it is essential to have a centralized system that could not only link the EHRs to the patient, thus enabling the health professionals to search the information they need in a centralized way, but also that provides authorizations management mechanisms for patients and auditing tools, for both health professionals and patients to monitor either who access his EHRs for what purpose and for how long, in the patient’s case, or in the health professional’s case, who had access to the information they have entered about a particular patient. We argue that this system could be based on the Portuguese RSE (36), thus becoming a central health system – Registo Central de Saúde (RCS). The RCS must accept HDI and MDI, thus ensuring strong authentications and delegation mechanisms.

![RCS system architecture](image)

**Figure 12. RCS system architecture**

In order to better consolidate our proposal we now present and discuss two simple web eHealth scenarios (doctor-patient) where OpenID combined with OAuth and the other discussed authentication mechanisms could be employed with advantage to implement them.
In all of these scenarios the doctor is confronted with the need to know more information about the patient he is assisting. Our suggestion is that he can login into RCS to search and access the needed information. Therefore, to be able to use such a system, the doctor has to strongly authenticate himself. To do this he must perform the following steps:

1. The doctor logs-in into RCS System using his MedID card.

   ![Certificate Verified]

2. The doctor searches for the patient in the RCS database (this operation could be done by entering the patients RNU number, his name or national ID number). Selects the patient and asks permission to list all health care institutions where the patient has EHRs (configured by default) by clicking “Request Patient authorization”

   ![RCS]

Regarding the first step, the doctor can choose not to employ is MDI, however he must always use his MedID card in order to authenticate into the RCS system, because of the strong authentication mechanisms required to act as a medical professional and the non-repudiation properties that need to be ensured for his actions. On the second step, the operation for searching the patient could be extended to use authentication based on remote biometric recognition mechanisms (105), such as fingerprint or iris scans, which can be extremely helpful when the patient is alone, without any kind of identification and unconscious, therefore unable to provide any information about his identity (a situation common on emergency situations).
When the doctor clicks in the “Request Patient Authorization” button a pop-up appears asking to provide information about the purpose of the request. In order to proceed, the doctor has to select one of the two scenarios or cancel the operation:

If the patient grants access or in an emergency situation, the list shown is by health institution by default, however the doctor can apply different views and organize the information by date or episode thus allowing for better and refined searches.

In both cases (during consultation time or emergency), the RCS system creates an entrance in the audit mode so that both the health professional that produced the information (as well as the HIS system administrator) and the patient who owns the information can monitor it. In addition, regarding the emergency case scenario, the patient could also be notified via email, fax or SMS about the occurrence.

At any given time the patient can alter his authorizations by using the ‘manage authorizations’ mode in the RCS system. This mode allows not only to revoke access but also to re-define the duration and manage the renewal of already issued authorizations. This can be easily accomplished if using OAuth 2.0 (76).
5.4.1. Scenario 1: Patient’s authorization to access their EHRs in a HIS during consultation time

Patient X has severe pains regarding his back. He has been treated in two different hospitals by two different doctors, but his problem has not yet been solved. Now he seeks another medical opinion for his problem and makes an appointment to another doctor, who has been referenced by a good friend, Doctor Y.

Doctor Y has no knowledge about Patient X medical history as it is the first time they meet. Patient X does is best to explain all the treatments he has been subject to by the other two doctors. He describes is back pains the better as he can and even shows some X-rays he has in his possession. Unfortunately the given information is not enough for Doctor Y to have a clear idea of the treatments and diagnoses Patient X has been submitted to. Doctor Y then asks for permission to access Patient X EHRs in those two different HISs by accessing the RCS system that allows Doctor Y to find and list the necessary information. Patient X accepts Doctor Y’s request and grants him a limited authorization for one session to access his EHRs in the two different HISs.

There are several steps that have to be performed by the Patient X in order to grant this authorization:

3. Patient X logs-in into RCS system using his CC card.
4. Patient X answers the question “Do you authorize Doctor Y to access your list of attended Health care Institutions where you have EHRs?”

5. Doctor Y can now access the list of Health care Institutions where Patient X has EHRs and click on the link of the one he wishes to consult thus entering that HISs with a special set of credentials (token) given by Patient X.

We now proceed to describe step 5 in detail. The delegation of authorization access in OAuth involves a sequence of interactions between the requester of information (the doctor), the third-party application or consumer (the RCS system, which displays the list of Health care Institutions that have patient's EHRs information by default), the HIS (that contains the requested information), the HDI Provider, and the information's owner (the patient).
This diagram illustrates the full sequence of events for step 5 (106):

1. The RCS (consumer) contacts the HDI Provider Authorization service, asking for a request token to access information in one or more HISs. The request is signed using the "anonymous" consumer key/secret.

2. The HDI Provider verifies the request and responds with an unauthorized request token that needs to be validated.

3. The RCS web application invokes another window in the same web browser to authenticate the patient in order to validate the request.

4. In this new window, the RCS sends an OAuth request for token authorization, referencing the received request token.

Figure 13. Accessing information using HDI Provider
5. HDI Provider displays an authorization page and prompts the user (the patient) to log into their account using his CC’s card (for verification) and then either grant or deny limited access to the requested information by the RCS application (consumer) that will allow the doctor to access the patient’s EHRs provided by the requested HIS.

6. The user (patient) decides whether to grant or deny access to the RCS application. If the user denies access, they are directed to the RCS home page and not back to the service application and the attempted failed request is registered for auditing purposes.

7. If the user (patient) grants access, the HDI Provider Authorization service redirects the user back to the RCS application. The redirect includes the now authorized request token.

8. The RCS auto-detects that an authorized token has been received, retrieves the token, and reclaims focus from the browser.

9. The RCS sends a request to the HDI Provider Authorization service to exchange the authorized request token for an access token.

10. The HDI Provider verifies the request and returns a valid access token.

11. The RCS sends a request to the HIS (service provider) in question. The request includes the access token.

12. If the HIS recognizes the token, it supplies the requested information to the RCS.

Once the process is completed, Patient X removes his CC and the logout is automatically done. Now, Doctor Y is able to access important information on the two HISs his patient have granted access to and learn more about the patient’s medical history. Accessing reports made by other doctors saved Doctor Y time and simplified his diagnostics. The information was available at the right time, to the right person and much more important in a secure way under the control of its legitimate owner, thus helping to preserve doctor-patient’s confidentiality and confidence.
5.4.2. **Scenario 2: Accessing a patient’s EHRs in an emergency situation**

In an emergency situation the patient is not able to grant access to his EHRs. In this case the information can be displayed at the doctor’s request by using some “break the glass” mechanism with proper auditing activated for later investigation on the reasons that lead the health professional to act in this way (96). Moreover, we argue for biometrics to be applied as proof of the patient physical presence. In addition, the patient is also later notified about who broke the glass to access his EHRs and the emergency reason behind its activation. The patient is therefore empowered to act in case of misuse (available in the audit mode).

5.5. **Future perspectives**

The presented mechanisms can be extended into asynchronous scenarios. This might be proven useful when the doctor needs to access the patient EHRs but the patient is no longer present or the authorization that was given was exceedingly limited and thus insufficient for the doctor to perform what he intended. This could be more efficiently done by having the patient using a mobile smart phone application with Internet connectivity in order to reduce the doctor’s waiting time for the authorization request to be processed. In this scenario the doctor places the request for authorization access into the RCS system (this would be an entire new functionality entitled “Request Authorizations Management”) and waits asynchronously for the answer. Meanwhile the patient would receive an SMS notification with a link to enter the request for authorization and act on it, either by denying or granting limited access to the requested resource. The doctor is notified via email, fax or SMS that he was granted or not access to the requested resource. If the patient has authorized the access, the doctor can authenticate himself in the RCS system and can click in the authorization link available in the “Request Authorizations Management” section, thus accessing the requested resource.
6 Conclusions

“All the interests of my reason, speculative as well as practical, combine in the three following questions: 1. What can I know? 2. What ought I to do? 3. What may I hope?” (Immanuel Kant)
6 CONCLUSIONS

The rapid adoption of computing systems and network technologies in the health sector is already causing serious behavioral changes (4). The threat to the confidentiality and privacy of EHRs is a major critical issue: with so many different professionals having the ability to access patient’s EHRs, it is in the patient and health provider’s best interest to know who is accessing the patients EHRs and for what purposes.

As a first step towards this goal we have proposed a user friendly solution, regarding health identity management, by leveraging the OpenID protocol. Our solution combines OpenID with the new Portuguese citizen’s smart Card and presents them as an interoperable, accessible, easy to use and deploy identification and authentication framework (Level 0). In addition, by further combining OpenID with OAuth we can implement an authorization framework that allows patients to securely grant access to their EHRs, scattered among different HISs, to health professionals in a much more controlled, shall we say, empowered way (Level 1). Moreover, patients can be notified who had access to their EHR, for how long and for what purpose, thus having the ability to act quickly upon any unauthorized data access.
These mechanisms contribute immensely to the empowerment of patients as designated in our pyramid of empowering levels as level 0 and 1. Furthermore, it is our vision that this pyramid of empowering levels can become a circle of conquered stages:

![Circle of Conquered Stages](image)

**Figure 14. Levels for Patient Empowerment**

Ultimately, the circle of conquered stages is not leveled but a sum of emotional stages that the patient needs to run to achieve full empowerment. First, the patient must be aware that he has the right to access his EHRs as well as the right to make them private. By acknowledging this the patient has the option of either to access or not his EHRs thus achieving some degree of power that enables him to delegate authorizations to access his EHRs in an informed way. If he delegates authorization to someone, it implies that the patient trusts the entity to which he is granting the access rights. This reveals a personal desire for achieving better health status. As a result, the patient is expecting to become more interested in health information thus contributing more for his treatment process and striving to make better informed choices. This is a clear indication that the patient is competent to acknowledge his own health status and consequentially able to act upon improvement. However, to achieve full empowerment the patient has to set the example to other patients by sharing his achievements and his failures, which indicates openness. These characteristics define a new patient that is equipped for the health care challenging scenarios of the 21st century.
6.1. Future Work

Healthcare can be shaped by government policy, it can be driven by the market forces or by a combination of both, but all these agents of change are being stressed and challenged. An aging populations and skyrocketing costs are putting unprecedented financial and organizational pressure on state and private healthcare providers as well as on the tax payers (12). In response to this crisis, health systems are suffering major changes: focusing more and more on the patient and on what the patient can do to help to improve his own health care.

To be a patient in the 21st century is to be deeply connected with the new information technologies and be an active participant on his own treatment thus sharing responsibility with the physician for health care while at the same time pursuing medical knowledge not only about diseases but also exploring new venues concerning fitness and wellbeing. One of the most evident applications for true participatory healthcare is the use of Personal Health Records (PHRs). Although there are several definitions, PHR refer to a set of collected, inputted, transferred electronic records that come from different sources: the patient, his physician or other health applications/devices.

Currently there are many platforms specially designed to help patients to build their own PHR such as Google Health (107), Microsoft HealthVault (108) and Dossia (109). In addition, the Internet is becoming the ideal a platform for convening people with shared interests. The increasing number of blogs and websites that promote discussions on matters related to patient's chronic diseases are an example of this: in 2007 social networking websites such as Facebook had more than 500 groups where discussions primarily focusing on diabetes were taking place. Even YouTube is part of this global trend, with 36,000 pages devoted to some aspects of surgery (2007). Moreover, innovative online collaborations are changing the way patients and health care providers learn about therapeutic regimens and disease management, ultimately driving the evolution of social media in health (110).

These occurrences characterize the popular phenomenon of Health 2.0 that is based on the use of social software and its ability to promote a partnership relation between patients, their caregivers free and health professionals in health (110). However, the key notion to retain is that at the centre of the evolving
clinical personal workstation lies at the modern personal health: electronic, accessible, confidential, secure, acceptable to clinicians and patients, integrated with other types of non-patient-specific information and sharable in a web 2.0 context (64).

These platforms are putting us at the doorstep of a much more personalized health care, enabled by dynamic health web tools that allows the patient to access reliable health information about his disease, learn what he could do to prevent other illnesses, search for other patients experiences, explore better treatments/therapeutics options and interact as a partner in health with the medical professionals among other activities related with his own health (share opinions or provide information about his own health status). Therefore, it is our strong belief that the just discussed web 2.0 technologies will play a major role in the patient empowerment process by being the scaffold on which the conceptual approach envisioned by Level 2 and 3 of empowerment levels’ pyramid is going to be constructed.
7 Bibliography
7 BIBLIOGRAPHY


17. PRIME White Paper version 1. *PRIME - Privacy and Identity Management for Europe*. [Online] July 2005. it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive..


85. Hildebrand, C. Currente state and future smart cards in Europe. Institute for Biomedical and Medical Imaging. s.l. : German Research Center for Environmental Health.


91. Alliance, Smart Card. A healthcare CFO’s guide to smart card technology and applications. February 2009.


110. **The wisdom of Patients: Health care meets online social media.** *Sarasohn-Kahn, Jane.* s.l. : California Health Foundation, 2008.