PATIENT EMPOWERMENT BY THE MEANS OF CITIZEN-MANAGED ELECTRONIC HEALTH RECORDS

Web 2.0 Health Digital Identity scenarios

Filipa FALCÃO-REIS a and Manuel E. CORREIA a,b

a Computer Science Department, Faculty of Science, University of Porto, Portugal
b CRACS - Center for Research in Advanced Computing Systems

Abstract. With the advent of more sophisticated and comprehensive healthcare information systems, system builders are becoming more interested in patient interaction and what he can do to help to improve his own health care. Information systems play nowadays a crucial and fundamental role in hospital work-flows, thus providing great opportunities to introduce and improve upon “patient empowerment” processes for the personalization and management of Electronic Health Records (EHRs). In this paper, we present a patient’s privacy generic control mechanisms scenarios based on the Extended OpenID (eOID), a user centric digital identity provider previously developed by our group, which leverages a secured OpenID 2.0 infrastructure with the recently released Portuguese Citizen Card (CC) for secure authentication in a distributed health information environment. eOID also takes advantage of Oauth assertion based mechanisms to implement patient controlled secure qualified role based access to his EHR, by third parties.

Keywords: Digital Identity, Electronic Health Records, Patient Empowerment, Smart Cards, Privacy, OpenID, Distributed Health Information environments

Introduction

Throughout the modern world, healthcare systems are in a crisis, as an ageing population and sky-rocketing costs are putting unprecedented financial and organizational pressure on state and private healthcare providers (1). In response to this crisis, health systems are suffering major changes: focusing more on the patient and what the patient can do to help to improve his own health care. The shift from a paper-based to an electronic media-based society is opening new opportunities that were not conceivable just a few years ago. Cost is no longer a major barrier to the recollection, storage and processing of huge amounts of information. This became common practice for critical businesses processes, major industry sectors and in the health sector, where we are witnessing a large increase on the deployment of Health Information Systems (HISs) and consequentially Electronic Health Records (EHRs) (2).
Market forces and societal pressures are also colluding to improve citizen’s health, which is further acerbating the need for more patient-centric systems. Governments all around the world are currently engaging with their agendas on reforming health care systems, despite great economic constraints. This health care reform is focusing more and more on the patient and encouraging him to assume the role of a pro-active consumer, with the ability to make his own choices and be held accountable for them. One can say that these reforms are making this patient empowerment processes inevitable. Numerous studies can also 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. 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 a patient inner point of view (considered as a process of personal transformation, i.e. empowerment occurs within the patient), or even both. Although the objectives are the same, i.e. to gain more power over one’s life, the nature of the two processes is rather different. Nevertheless both processes must be actively promoted in today’s society (3).

The Patient’s role in the 21st century

To be a patient in the 21st century is to be a ‘patient 2.0’, deeply connected with emergent new technologies and highly motivated to assume control and responsibility over his own health care. However, all this enthusiastic feeling around the ‘patient empowerment’ process must be put into perspective. There are not many studies related to this issue and it is fundamentally important to conduct more studies in order to assess real patient’s desires and motivations for further empowerment: do they wish to be empowered using an EHR? What level of ‘patient empowerment’ will the EHR achieve (4)? What are the main advantages and disadvantages concerning the patient within this approach? How are patients going to be able to express their intentions within Health Information Systems?

All of these issues lead to important questions that need to be answered. Focus group interviews are a good tool to gather patient’s opinions about these matters. In our opinion these interviews could be first steps towards kick starting the ‘patient empowerment’ process. As soon as these proceedings are done, it would become 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 role (just like in the self-service industries, such as fast food chains where the consumers know what is expected of them) and to achieve knowledge about their options (an informed choice will improve patient’s performance and commitment to his healthcare). In order to achieve this plan, some recommendations must be taken in consideration, such as (5):

- **Target health conditions for ‘patient empowerment’ where there exists a significant potential** (patients faced with an acute and urgent medical crisis are less able to gather information and to deliberate than those with chronic conditions).
• **Analyze the treatment process** (conditions should be analyzed to identify the steps in the treatment process where greater patient power would have the largest impact on improving efficient health outcomes).

• **Remove barriers to empowerment** (this may involve redefining and communicating the patient’s role, enhancing both their knowledge about their options, health condition and personal health status as well as their skills to carry out the required proceedings competently by improving their self-efficacy and health literacy).

• **Create a facilitating environment for patient empowerment** (this might include the promulgation of patients rights, a number of choices that are consistent with patients’ needs, easy access to valid information about the choices available, as well as helping patients with information-processing and decision-making by doctors that must be trained to perform different roles, complementing each patient’s preferred role).

• **Ensure equity** (because patients are different, empowerment efforts must be customized to different patient groups, the need to target efforts applies particularly to health literacy, due to the fact that those with better education, better health insurance and higher incomes are in a better position to make choices than those who lack these benefits).

• **Motivate the empowered patient to achieve more efficient health outcomes** (empowering patients may or may not result in improved efficient health outcomes because of lack of patient motivation, so incentives to patient’s commitment to his/her healthcare would result in better and more efficient outcomes).

One should add that these actions must involve both patients and health professionals with interactive health information systems, which must be developed to provide appropriate tools to allow patients to effectively take control of their EHRs at the level they desire and are capable of. Nevertheless, little has been done to involve the patient in the process of designing these tools, although quite a few studies have demonstrated that if the patient is involved in his own healthcare, not only their health will improve, but also fewer patients end up attending hospital emergencies unnecessarily (5). This involvement could be the result of being able to participate in decision-making, being educated regarding health problems and promoting a close relationship with healthcare providers, one that can potentially lead to a reduction in operational costs.

**Extended OpenID for increasing Patient Empowerment**

Nowadays, there are many platforms that are specially designed to help patients to build their own Personal Health Record (PHR) such as Google Health and Microsoft Health Vault or web sites that promote discussions on matters related to patients chronic diseases, for example social networking web sites such as Facebook have more than 500 groups where discussions primarily focusing on diabetes are taking place. Even YouTube is part of this global trend, with 36,000 pages devoted to some aspects of surgery. 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 between patients, their caregivers and health professionals in health (6).
Yet, with the continuing growth of the number of such health web sites and services, patients end up registering personal data into multiple systems throughout the Internet, scattering their identity, duplicating their data and increasing in a most dramatic way the difficulty of managing this data. Eventually users end up losing track of their passwords and account settings if they do not use these 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. Such dangerous behavior is one direct result of the lack of user’s knowledge and service provider’s willingness to acknowledge the existence of mechanisms that can help users manage their own accounts and passwords. The continuous growth of 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, is demonstrating the fragile awareness of the general public for these matters. It is equally important to raise awareness among patients, caregivers, and health professionals, so that the concern over the privacy and security of EHRs becomes a priority. It is thus important to develop systems and processes that can help manage and control the access, and even the disclosure and finality of these resources. These systems should provide identity management tools for the patient to secure for themselves their own privacy. As an example for these potential mechanisms we present a digital identity framework based on the OpenID protocol that could be used to mitigate these problems.

1.1. OpenID contextualization

One could start employing OpenID 2.0 and several of its extensions. OpenID is a decentralized system protocol for user-centric identification and digital identity management in the Internet. It 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 as “service provider”, is a site that wants to determine the end-user’s identity. 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. It allows users to add as much attributes as they believe that best describes them and assume profiles, also called Personas. Patients could easily create their Health Persona with attributes they consider to fit, thus preventing duplication of data across the Internet in an active and built-in way. It is this dynamics of creating and changing one’s character that best defines the essence of the OpenID protocol. The following list outlines the most important features of OpenID (12):

- **Open**: it is based on a community-driven development effort, with many components proposed as IETF (Internet Engineering Task Force) projects.
- **Decentralization**: users may reuse identifiers at any OpenID-enabled website, or provide a list of identifiers or switch in case one provider is unavailable, or even run their own identity provider.
- **Free**: fostering interoperability between multiple vendors’ identity technologies.
- **User-centricity**: the end-user has absolute control over the use and dissemination of his identity information.
- **Ubiquity**: easy to remember, pervasive, with a single password.
• User authentication flexibility.
• **HTTP session protection**: SSL/TLS, client certificates.
• **Identifiers delegation**.

The OpenID Authentication process is very simple: when a user wants to sign into a website, which as a "Relying Party" would like to verify the user’s identity, he has to choose an OpenID Identity Provider that he trusts and best meets his operational and privacy needs to create and manage a digital identity. The OpenID Identity consists of a unique Uniform Resource Identifier (URI). These URIs can be used by the owner to identify him at a website that has implemented OpenID and acts as an OpenID relay (13). During normal usage, the user submits his URI to the relying party, who uses the identifier to determine the identity provider’s 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. If the user does not trust the relying party after all, they may choose to reject the login (12). 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 can also take other actions: if the Identity Provider did not return all of the requested parameters, it may grant a lesser level of access to data or if it is the first time that a user has logged in the website, the Relying Party may also go through his own complementary registration process. Nevertheless, the Relying Party actions after the completion of authentication process are out of the scope of the OpenID protocol (14).

![OpenID authentication process](image)

**Figure 2.** OpenID authentication process (13)

The advantage of such a system is that the user does not need to register for any OpenID enabled website once he owns an OpenID identity, 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 passwords or even usernames for the different web sites he registers, thus minimizing the problem of too many multiple identities. There are however some security limitations (12):

- **Trust**: once authenticated the relying party 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, where (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).
- **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 that particular authentication policies be applied by the OpenID Provider when authenticating an End User (13). 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 (12). Also the use of certificates for both the End User and the Identity Provider confers a more trustworthy characterization to both and increases the level of security of the authentication process.

**1.2. Improving Patient Empowerment with smart cards, the use of the Portuguese Citizen’s Card in healthcare**

Today’s ‘patient empowerment’ process is becoming a central issue for healthcare providers worldwide as they face new challenges in achieving better and personalized health outcomes. Therefore, they need to adopt a patient-centered approach if they want to effectively incorporate empowerment into their clinical processes. This requires more personal involvement with their patients and implies a shift in the representation of their roles, moving away from the role of skilled technicians towards roles which underline the importance of people skills, and from knower to facilitator, thus reducing the existing gap between doctors and patients. As a result of their empowerment process, patients are expected not only to better self-manage their illness, by better understanding their choices, but also to be able to share their EHRs with the health professionals they wish or need to, thus allowing a much more distributed approach regarding health care providers. Information systems play a decisive role in empowering patients by providing them with the appropriate tools to help them secure and manage their EHRs.

Keeping this in mind and in order to achieve this desirable goal, one must efficiently translate real world infrastructures to the virtual world starting with patient’s identification. Smart cards enable people's identities to be securely authenticated and communications to be secured, providing mechanisms for implementing strong
security, differential access to data, and definitive audit trails, thus providing the mechanisms to enable trust in healthcare communications and business processes. They contain an embedded microprocessor chip that has the capability of running applications and can also carry data, such as personal details, that can only be accessed 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 moving healthcare towards information management as a public utility rather than a personal millstone (7).

Smart cards are exploding worldwide and are a solid proven technology. In 2008, 5.045 billion smart cards were shipped worldwide — an impressive 13.2% increase over the 2007 figure of 4.455 billion. Because of their size, flexible form factors, and relatively low cost, smart cards are ideal for applications in healthcare where personal identity, privacy, security, convenience, and mobility are key factors (9). Some countries already have smartcard-based healthcare technology, such as USA (since the late 70’s), Germany (since 1989), France (1998), Slovenia (since 2001) and more recently England. 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) (19).

Most agree that the use of this type of technology is essential to achieving many critical milestones for healthcare reform, such as:

- The need to lower costs and create administrative efficiencies
- The need to improve patient outcomes and enhance physician and patient relations
- The need to meet increasing privacy, security and identity concerns, as a result of governments directives mandating increased control over private information

An identity and authentication solution based on smart card technology currently provides a best of breed foundation for improving HISs in a secure, private and sensitive way.

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 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 (8). Briefly, to translate real world national authentication mechanisms to the digital world, in a well elaborated and secure way, which creates an opportunity window to leverage the OpenID framework with a strong PKI national infrastructure supported by smart cards, in this case the Portuguese CC. For healthcare providers, the challenge is not only to secure the funding for new technology, but also
to weigh the potential benefits of new and emerging technology against the costs. Thus to embrace the Portuguese CC in healthcare is to exploit a new opportunity to simplify and provide secure access to patients’ EHRs simultaneously reducing costs and budgets.

The Extended OpenID project is a conceptualization of this opportunity and the idea is to provide every Portuguese citizen with the possibility to enjoy Internet services in a secure, user centric and accessible way, by using their CCs to provision and strongly authenticate an OpenID digital identity. To walk towards this goal we have adapted and deployed an OpenID IP server, in which the authentication process makes use of the CC as a verifiable nationally deployed secure token (16).

1.3. Identity Services for Healthcare

Digital identities can play a great role in assisting citizen’s to manage EHRs. Digital identity can be defined has a set of characteristics that uniquely describes a digital subject and its relations with other digital subjects (17). These characteristics or attributes can eventually change over time or even be certified by third parties thus adding a trusting character to it. In the digital world we are building a virtual society based on these principles and concepts. Although, the principles and concepts may not be new, the means in which they are processed and used 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 a digital identity based society, but also how much control individuals will be able to take – or will want to take – over their digital identities (17). As a result, we investigated several complex scenarios with an OpenID identity provider based on the eOID project (16). Our goal is to employ this Identity Provider (IP) in a healthcare context and to extend the OpenID protocol to meet several healthcare challenging scenarios related to role delegation and authorization.

We thus consider the following attributes as critical and in need of being integrated into a patient Health Digital Identity (HDI):

<table>
<thead>
<tr>
<th>Table 1. Patient’s Health Digital Identity basic attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Personal Data</strong></td>
</tr>
<tr>
<td>Full Name, Date of birth and Gender</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Home Address, Telephone, Cellphone, Email</td>
</tr>
<tr>
<td>Emergence Contacts (Name, Cellphone, Kinship)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>National ID number, Tax payers’s number, Social Security</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

The authentication process within the eOID server is made by using the digital authentication certificate stored in the Portuguese Citizen Card. First, the user needs to register a digital identity on the eOID identity provider. The system then checks the validation of the authentication’s certificate and consults the list of revoked certificates provided by the Certificate Authority (CA) responsible for the issuing and managing of the Portuguese Citizen Card certificates. If the user certificate is valid the eOID’s
authentication system associates the received certificate with the user’s internal credential (16).

In order to create this service one must denote that health computing environments need to be modular, secure, and web-enabled. Much of the current thinking on distributed computing environments in health is based on the excellent previous works of the (then) OMG Corbamed taskforce, and the Distributed Healthcare Environment (DHE) work done in Europe in EU-funded projects such as RICHE and EDITH, and the HANSA and PICNIC implementation projects (22). Nevertheless, our proposal does not intent to create a framework that can have a single EHR for every Portuguese citizen. Building such a system is an enormously challenging task, involving several major research and development challenges. Instead, our proposal is to maintain the different EHRs as they are, while provisioning identity and authorization through the means of digital identity services. Our approach is thus to help enable the development of a truly distributed, scalable, and reliable healthcare 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 an 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 and thus producing a more productive cooperation between the parts.

We have identified relevant stakeholders among the different Portuguese Health organizations to start implementing the proposed system architecture. We consider that the patient Health Digital Identity (HDI) could start to be deployed by the Portuguese Regional Health Administration (ARS – Administração Regional de Saúde) within their five regional health administrations (ARS Norte, ARS Centro, ARS Lisboa e Vale do Tejo, ARS Alentejo and ARS Algarve).

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 leads to a central point of failure that needs to be remedied by the use of expensive high availability equipment supported by a very expensive system administration infrastructure. Our proposal is to partition data geographically (according to the locations of the different Portuguese ARSs), by 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 (21). Suitable database partitioning algorithms will have to be devised for geographical distribution of patients HDI, while ensuring that data access is efficient and within acceptable time limits.

The mains advantages in using distributed databases are that they are very economical and reflect organizational structure, while maintaining local autonomy, since a department can control the data about them. Also it provides protection of
valuable data (in case of disaster, such as a fire, all of the data would not be in one
place, but distributed in multiple locations) and improves performance, as the data is
located near the site of greatest demand, and the database systems themselves are
parallelized, allowing load on the databases to be balanced among servers (a high load
on one module of the database won't affect other modules of the database in a
distributed database). Moreover, these systems perform more reliable transactions due
to the replication of the database and are modular, which allows for systems to be
modified, added and removed from the distributed database without affecting other
modules (systems).

As a result we have identified the requirements for our HDI Provider (20):

- high data availability even in the presence of faults in the network or computer
  hardware (eg due to power outages, environmental disasters and regional
  strife)
- high performance to ensure the system can function even under the high loads
  that may arise in emergency situations (such as a pandemic, large-scale
  accident or war)
- security to protect patient data and digital identity from misuse, unauthorized
  access or attacks.

As part of this distributed approach, it is our intention to develop data replication
algorithms to ensure that security, performance and data availability requirements are
met. Our replication algorithms must take into consideration Brewer's Conjecture: it is
impossible for a data store in an asynchronous network to simultaneously provide (i)
partition tolerance, (ii) availability and (iii) consistency. Typically, systems can be built
that simultaneously provide two of these three properties and it is generally assumed
that designers of new systems should pick the two properties that are most important to
their requirements (21). Further developments in our work will include a model for
implementing the presented HDI Provider and we will investigate the design of
partially synchronous networks that can enable us to overcome this limitation.

1.4. MedID – Digital Identity for health professionals

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 (5). Simultaneously, this will
allow certifying health professionals with the secure credentials to translate their
physical world role to the digital world. Our proposal is to adapt the eOID Identity
Provider to meet the requirements for providing health professionals with a Medical
Digital Identity, which ultimately will allow them to access the data they require to
provide the best quality care at any given time.

We thus considered the following attributes to integrate a health professional
Medical Digital Identity (MedID):

<table>
<thead>
<tr>
<th>Table 2. Physician's Digital Identity basic attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Personal Data</strong></td>
</tr>
<tr>
<td>Full Name, Date of birth and Gender</td>
</tr>
<tr>
<td>Naturality, Nationality</td>
</tr>
</tbody>
</table>
The authentication process within the eOID server is made by using the digital authentication certificate stored in the MedicalID Card. The MedicalID card is not deployed yet and is based on a proposal for a smart card to provide health professionals’ with strong PKI X509 qualified digital signatures and authentication certificates.

To use this service, the health professional needs to register a medical digital identity on the eOID identity provider. The system then checks the validation of the authentication’s certificate and consults the list of revoked certificates provided by the Certificate Authority (CA) responsible for the issuing and managing of the MedicalID Card certificates. If the user certificate is valid the eOID’s authentication system associates the received certificate with the user’s internal credential.

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). Regarding the Identity Provider it should be federated among their three regional sub-sections (Secção Regional do Norte, Centro and Sul) for better management and reliability.

**Granting secure access to EHRs – the patient’s choice**

In the Portuguese legislation the patient can access is health related data with the consent of his GP and upon his request. Regarding EHRs several efforts are being made so that the patient is entitled to have a copy of his own EHRs upon his request. This will permit patients to access their own EHRs scattered among the different healthcare institutions thus allowing them to share them with the health professionals they wish to. The key feature in our vision is to provide the patient with the tools to share his EHRs in a fast and secure way, without having to reveal his access credentials in the process. We thus present a simple and flexible solution that enables the patient to easily grant authorizations to his own EHRs that can be scattered among several different health information systems.

**1.5. Using OAuth to 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 (15). 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 protocol 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 (15). While OpenID can be used to allow a patient to sign on into many health web sites or applications with the same identity, OAuth can be used to grant conditional access to patient data without having to share his identity at all (or his credentials). Using this type of protocol is extremely important regarding users privacy in the matters of managing EHRs. More generally, OAuth creates a freely-implementable and generic
methodology for API authentication. By combining the OpenID protocol with OAuth we can arrive at a simple solution, more centred 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 (18). We are currently exploring the concept of ‘valet key’ with an implementation combining OpenID with the OAuth protocol (15).

Case studies

In order to better understand the numerous advantages provided by such a model, we present and discuss a simple scenario where this type of technology could be applied to improve healthcare outcomes.

1.6. Patient’s authorization to access their EHRs in an Health Information system during consultation time

The 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 his first time they met. Patient X does is best to explain all the treatments he has been subject to by the other 2 doctors. He describes is back pains the better as he can and even shows some X-rays he has in his possession. But 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 using an installed application in his desktop that allows the display of the requested information. Patient X accepts Doctor Y’s request and grants him an authorization for one session to access his EHRs by both ‘asked’ HISs.

OAuth authorization for installed applications involves a sequence of interactions between the third-party application (which only purpose is to display EHRs information), the Health Digital Identity Provider, and the end user (the patient). This diagram illustrates the sequence where the doctor has previously logged in with his MedicalID card (11):
1. The installed application contacts the HDI Provider Authorization service, asking for a request token for 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.

3. The installed application invokes a web browser.

4. In the browser, the installed application sends an OAuth request for token authorization, referencing the received request token.

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 his HIS service data by the third-party application that will allow the doctor to visualize the patient’s EHRs.

6. The user (patient) decides whether to grant or deny access to the third-party application. If the user denies access, they are directed to the home page and not back to the application.

7. If the user (patient) grants access, the HDI Provider Authorization service redirects the user back to a web page designated by the third-party application. The redirect includes the now authorized request token.

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

9. The installed application 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 third-party application sends a request to the HIS service in question. The request includes the access token.
12. If the HIS service recognizes the token, it supplies the requested data.

Once the process is completed, Patient X removes the CC and the logout is automatically done. Now, Doctor Y is able to access important information on the two HISs his patient has 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 diagnoses decision. The information was available in the right time, to the right person and much more important in a secure way, thus preserving doctor-patient’s confidentiality.

In an emergency situation, there is no need for the patient to allow access. 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 doctor to act in this way (23).

Conclusions

Nowadays Electronic Health Records are seen as ‘patient empowerment’ process facilitators: by giving patients a source of information that is specific to them (4). 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, a shift that will place increased emphasis on improving the equity of the doctor-patient relationship, reducing the reliance on instruction and building more on partnership. As a result of their empowerment process, patients are expected to better self-manage their illness, by better pondering their choices: some patients may decide to delegate to their doctor the responsibility for some aspects of their treatment, while other patients under similar circumstances would prefer to learn to self-manage some if not all aspects of their illness and treatment (3). Although this behavior might be correlated with several different aspects of each patient, like age, gender, qualifications, education, as well as some aspects concerning today’s society, every patient is an unique case and if well guided and motivated can achieve a better self-manage of himself. However, this does not mean that patients should be left alone to decide what is best for them: it is the healthcare providers’ responsibility to provide guidance and motivation for patients to learn how to manage effectively their illness and their lives (3).

Information technology plays a decisive role in empowering patients by providing them with the appropriate tools to help them to secure and manage the self disclosure of the data regarding their health, such as their PHRs or even their EHRs. Although there are a variety of solutions available to effectively help patients within their privacy, making extensive use of the OpenID protocol together with smart cards, ‘valet keys’ or even biometrics constitutes a tentative approach that should be further explored and promoted. Also, it is critical for doctors to have accurate and complete information about their patients’ health in the right moment in order to provide more efficient health services. Therefore, time and access are indubitably key factors. Keeping this in mind, the solution we presented could effectively enabled patients to share their EHRs with the health professionals they desire in a secure and practical way. However, patients need time to adapt and adjust to these new emergent technological solutions. Patient empowerment is unquestionably a long process, which
involves not only the collaboration of patients and health professionals, but also appropriate integrated and supporting digital health systems, thus promoting health to a whole new level.

References