Envisioning secure and usable access control for patients

Ana Ferreira[1,2,3], Gabriele Lenzini[1]
SnT[1] and COSA[2], University of Luxembourg
Luxembourg
ana.ferreira@uni.lu, gabriele.lenzini @uni.lu

Cátia Santos-Pereira[3], Alexandre B. Augusto[3,4], Manuel E. Correia[4]
CINTESIS[3]-Faculty of Medicine and CRACS/INESC LA[4] – DCC, Faculty of Science, University of Porto, Portugal
catiap@med.up.pt, {aaugusto, mcc}@dcc.fc.up.pt

***Abstract*— Several pilot tests show that patients who are able to access their Electronic Health Records (EHR), become more responsible and involved in the maintenance of their health. However, despite technologically feasible and legally possible, there is no validated or standardized toolset available yet, for patients to review and manage their EHR. Many privacy, security and usability issues must be solved first before this practice can be made mainstream. This paper proposes and discusses the design of an access control visual application that addresses most of these issues, and offers patients a secure, controlled and easy access to their EHR.**

Keywords*— *Visual access control; electronic health records; patient empowerment; security and usability.

I. INTRODUCTION

Both the European Recommendation and American Legislation for the protection of medical data agree that patients should be allowed to access personal medical records and take decisions regarding their content and distribution [1][2]. Some European countries implement those directives even more openly. The Portuguese legislation, for instance, allows patients to access their medical data without intermediaries [3]: it considers patients the legal owners of their data whereas it regards healthcare institutions the responsible guardians of the patient data that they produce and store.

If those directives were implemented today, patients would be ready to take more interest and control over their medical data [4]. Accustomed to a widespread communication technology, most of them are already seeking out in the Internet information about their pathologies, driven by curiosity to know more about their conditions and urged by the need to find ways to improve their treatments [5].

On the other side, healthcare professionals and health institutions are already organizing medical data in Electronic Health Records (EHR). EHR, which can be shared over different institutions, keep track of the medical history of patients, together with medical exams, lab tests and demographics. Presently, excluding specific cases of research or of some experiments in defined medical specialities [6][7], patients have no means to regularly access their EHR. But several professionals agree that letting patients reviewing and commenting their EHR, for instance prior to a consultation, would be highly beneficial [8]. Recent studies show that patients who review their EHR are more informed, proactive and responsible over their healthcare treatments and are generally more satisfied with the outcomes of their therapies [6][9][10]. Such informed patients are expected to communicate better with doctors, to commit more faithfully to their rehabilitation, and be more inclined to follow medical recommendations [6][7]. These positive reactions are believed to ameliorate how professionals and organizations approach healthcare [11][12].

However, unless protected by adequate data access control mechanisms and policies, opening access to EHRs is risky. Its careless usage may seriously compromise data integrity and privacy [13][14]. At present, likely to avoid such a risk, there are no institution independent, dynamic (always updated) yet secure applications offering patients the possibility to review their integrated EHR collected from different institutions at any moment in time. However, the challenge of developing such an application is not only technological. Because it should work both for the medical professionals and for the uneducated laymen, that challenge is *socio-technical* [15]. A toolset accessing EHR should provide trustworthiness while offering user-friendly human computer interactions (HCI) that infuse users, particularly the non-experts, with an honest sense of trust.

This paper proposes and discusses a preliminary design of a patient's access control visual application called "*Patient Access Control Visualization & Monitoring*" (PACVIM), meant to provide patients with an easy but controlled access to their EHR, over the Internet. In this way, PACVIM educates patients to be prepared to follow their therapies and puts health informatics at the service of the society.

Architecturally, PACVIM integrates with OFELIA (Open Federated Environments Leveraging Identity and Authorization), a prototype system to perform registration, authentication and authorisation to EHRs [16]. From the human interaction's point of view, PACVIM uses visual access control tools commonly employed nowadays to browse social networks. It is designed to be easily understandable and usable by non-experts and integrates, where possible, touch gestures. PACVIM relies on future research in HCI security and usability (with both qualitative and quantitative methods) to face access control, usability and security requirements regarding different end-users' communities.

The next section presents related work while section III describes an overview of OFELIA and its integration with PACVIM. Section IV describes PACVIM's main requirements and features for a first stage of its design. Section V discusses PACVIM's proposed design and suggests future work. Section VI concludes the paper.

II. Related Work

There has been some interest in patient's empowerment regarding his/her healthcare data, however, this has been hard to implement as well as integrate with existing EHRs and other healthcare institutions' databases. Some sporadic applications have been proposed to help patients accessing and maintaining their medical records. These are called Personal Health Records (PHR). PHR are systems that allow patients to insert and access both demographic and medical data, often with the possibility to share information with healthcare professionals [17]. But PHRs are stand-alone patient-oriented systems, not meant to being integrated with existing EHRs. Likely, this means redundancy of data, potential inconsistencies and management problems. No integration means also that the records stored by patients are not ruled by the same policies that regulate, by law, how health institutions should handle medical information. Consequently, data privacy can seriously get out of any control.

The lack of regulation and legislation about who owns and who is responsible for medical data is also a serious limitation of PHRs. Let us take for example "Google Health" [18]. This PHR was introduced by Google in 2008 but, because its adoption had been very sporadic and only among certain groups of users like the tech-savvy patients and their caregivers, it has been discontinued since 2011. Patients were invited to withdraw their (possibly sensitive) healthcare data, but from 2013 this is not possible anymore. Google claims that all data have been destroyed but patients cannot control that claim. They can only trust what Google tells them.

In general, PHR's security and privacy policies are not as clear as they should [19]. This lack of clarity, together with the fact that most PHRs run over the Internet and permit patients to share information with whomever they want, has the drawback to leave users unaware of who eventually can see those records and ignorant of the risk of losing control altogether over their data. The adoption of mobile technology makes this situation even frailer [20].

Regarding now the use of visual tools, this work [21] shows that users perform more accurate access control policy analysis with social network's style visualization tools, than without them. Such a strategy may be of use in PACVIM, because it is difficult for a user to mentally keep track of the topology of his/her constantly changing healthcare EHR network. Other works propose visual languages for specifying role based access control rules for web systems [22], or describe visual approaches to manage access control for distributed research ecosystems based on a multi-purpose collaborative graph structure [23]. Individuals are enabled to visually interact with the graph and contribute to access control decisions by jointly modelling the environment's structures and policies. The burden of project management can be eased with an integrated view of complex environments.

The authors did not find similar research to the one proposed in this paper, in the healthcare domain, except for this recent study [24] whose main goal is to help doctors and medical staff to configure access control rules reliably and quickly. To do this, they introduce a human-centric, visual, and context-aware access control system for distributed clinical data management and health information systems. They also propose to extend the tool in the future to let patients participate in the access control process, to choose different levels of data privacy for their medical data and having security in their hands. But not many details were provided regarding this subject and, so far, there has not been a follow up of this work to a more practical research.

III. OFELIA's integration with PACVIM

OFELIA (Open Federated Environments Leveraging Identity and Authorization) [16] is an identity management framework that entrusts patients with the possibility to exert some control over personal medical data by allowing them to register to an existing EHR, and be authorized to access the data therein maintained, according to the policies of the healthcare institution that runs that EHR.

The framework consists of a set of services including: an *XMPP* (Extensible Messaging and Presence Protocol) *server* to establish communication with a mobile device, an *external web application* that provides a graphical interface for patients in order to reply to requests from external computers (e.g., patient's computer), an *internal management service* to allow patients' initial registration and to establish communication between the *health institution's EHR database*, an *external web application* and the OFELIA client - a mobile application used to provide a strong authentication by granting discretionary access rights to the requested EHR [25]. The OFELIA client offers patients the following functionalities: registration, authentication and authorisation.

Patient's registration: allows a patient to register to an existing EHR hosted by a healthcare institution. Fig. 1 presents the six steps to establish a secure patient's registration: (step 1) the patient authenticates to the health institution's computer using his/her electronic citizen card or electronic health institution card; (step 2) a pair of Quick Response (QR) codes [26] is retrieved by the health institution's computer, where they can be read with the patient's mobile device.

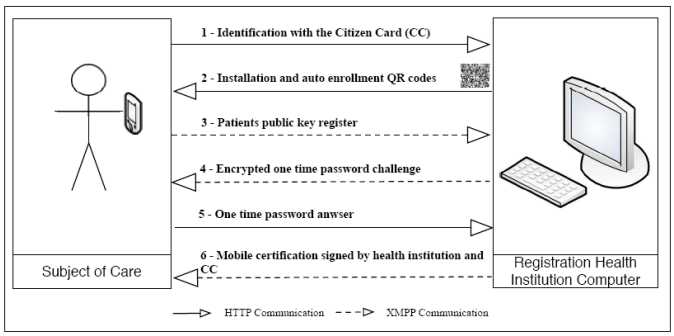

Fig. 1 - OFELIA: Patient's registration.

When the first QR code is read, it installs in the patient's device the OFELIA client with the necessary services to proceed with the registration. The second QR code uses OFELIA Client to complete the registration process described in steps 3 to 6 where the patient's device and the healthcare institution's registration computer establish a secure session, which relies on PGP (Pretty Good Privacy) certificates, including digital signatures and one time passwords (OTP). More details in [16].

Patient's authentication and authorization: handles the necessary steps that allow the patient to securely access his/her EHR from a registered health institution. This functionality is responsible for the process schematised in Fig. 2.

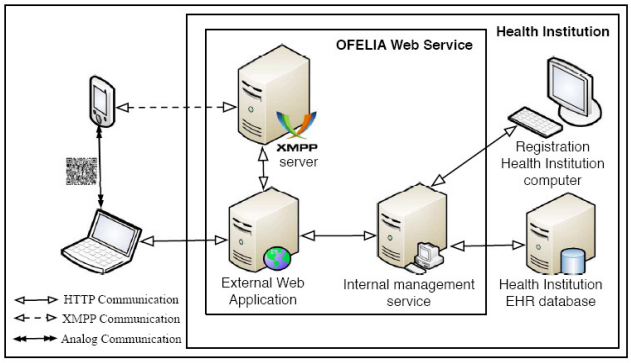

Fig. 2 - OFELIA: Patient's authentication and access.

Users can request access to an EHR from any network running the OFELIA web service. They connect to the OFELIA *external web application*, which replies with a QR code that encodes a session key. This key needs to be activated by the patient before being validly used to access the EHR. The patient reads the QR code session key with the OFELIA client (by using his/her mobile device), which electronic signs the session key with the patient's PGP certificate, and sends it back, via the XMPP server, to the OFELIA *external web application.* This application validates the electronic signature and authenticates the patient. It links him/her to the QR code session key, and automatically refreshes the external web application interface with the patient's information containing the list of roles/access control permissions. After this authentication process, the patient is authorized to securely access his/her medical records. Gathering these records and enforcing the security of the accesses is handled by OFELIA's web service running at each institution's site. Such background activities are completely transparent to the patients.

A patient that has registered to an EHR is likely to go browsing the content of that EHR. This task may not be straightforward, since patients may not be familiar with access control models or even EHR content. They need a user-friendly interface to visualize, in a comprehensive manner, the rights that each role has upon the records and what information is inside each record. PACVIM adds exactly such a visual interface to OFELIA's secure infrastructure. Patients can therefore transparently see all the connections and parts of EHR that are shared among different healthcare institutions (more on section IV.B).

OFELIA's client has been prototyped on android-based devices and tested for usability, especially its use of QR codes in the registration process [27]. The prototype has been judged positively by the participants for its good appearance, information content and usability. Fig. 3 shows two screenshots of this application.

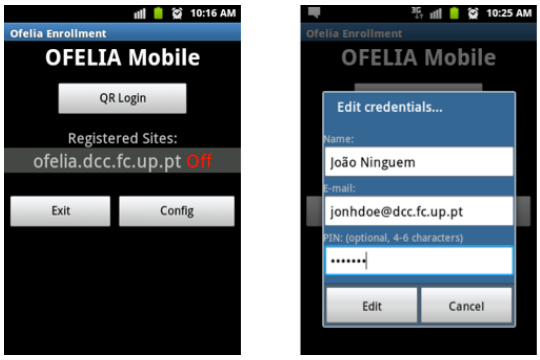

Fig. 3 – Smartphone interface of OFELIA's registration process using QR codes (prototype).

Fig. 4 shows how OFELIA integrates with PACVIM and how a patient interacts with the visual interface. The part in the bottom shows the registration with the OFELIA web service. On the top right is the visual interface showing an access control network (section IV.B) that the patient sees when browsing the EHR. Here, OFELIA client asks authorization to the OFELIA web service, awaits the data which the server gathers, and presents it on the patient's screen.

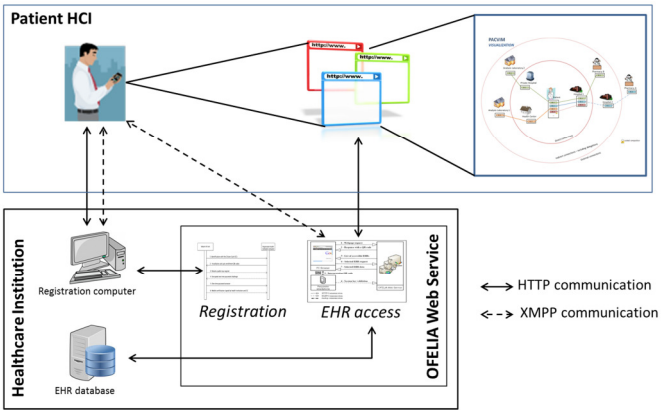

Fig. 4 – PACVIM: integration with OFELIA and visual interface.

–

IV. PACVIM

A. General Requirements

As an application responsible for ruling a patient's access and visualization to an EHR, PACVIM must satisfy specific

requirements including: (a) healthcare standards, (b) access control models together with security directives and practices and (c) usability features.

Healthcare standards: several healthcare standards regarding EHR's security requirements define, with some fine-grained detail, access control roles and sensitivity levels for healthcare professionals to access EHRs [28][29]. Moreover, the International Standard ISO/TS 13606-4 states some content structure for a specific EHR, for instance, what parts it can integrate, how information can be organized and what roles can access that information. Such directives and indications are taken into account within the proposed PACVIM.

Access control models and practices: PACVIM implements concepts already defined within the Patient's Access Model (PAM) in [30]. PAM is built upon the standard RBAC (Role-Based Access Control) and integrates other characteristics such as: *break-the-glass (BTG)*, where there is the possibility to change temporarily the access control policy in a controlled manner, for instance, in emergency or unanticipated situations (an example of how BTG can be used in a record is shown in Fig. 6); and *temporal constraints*. Temporal constraints are added to roles in order to limit the timeframe of access control permissions, for example, to healthcare professionals that work on shifts. Moreover, in order to provide contextualization for these added features, PACVIM will include the *purpose of use* that, in relation to permitting constraints, provides context to define the most adequate access control rules for requesting information resources. Examples of purpose of use can be: emergency accesses, asking for a second opinion, research usage and so on [31].

Usability: to achieve a user-friendly and captivating application for the patients, PACVIM will have a user interface where patients can monitor data, roles, people, healthcare institutions and their relations over time, simply by looking at the screen. Moreover, where possible, PACVIM should be operable by touch-screen gestures, giving feelings and feedbacks similar to those of a simple game. Such interactional features are already offered by most used and widespread mobile devices (e.g., smartphones and tablets), which nowadays promote very successfully, and on a daily basis, this type of visual usage.

In short, PACVIM must include characteristics reminding human-centric, visual and context-aware access control systems. Besides, it should be centred on to be usable by the patients, commonly less familiar with EHR technology than the medical staff and healthcare professionals.

B. Design Features

PACVIM's access control *visual* model represents pictorially healthcare institutions, medical records and/or their parts. It shows where those elements are located and which roles are allowed to access them. PACVIM adopts visual tools, such as the Transparent Enhancing Tools (TETs) [32], to generate a network that graphically shows privacy policies and data rights, as well as the extent of disclosure of personal data to third parties. TETs give better understanding of both trust and security that are involved in its design and are therefore able to provide, not only more user-friendliness, but also a stronger access control usable security.

An example of an access control network is drawn in Fig. 5. Each node is an instance of a patient's medical record accessible to the patient, regardless where the record is physically located and stored. Usually records are available at specific sites, for example hospitals, laboratories, and pharmacies, which in Fig. 5 are represented by icons. Inside the rectangles are the various *compositions* of the records that are available and/or shared to the healthcare professionals who work at that specific institution. This "sharing" relation is represented with a straight full line. One or more compositions can be shared among several institutions.

This compact representation gives patients an immediate overview of the EHR's *direct*, *indirect* and *external* connections, as well as *delegations*. Direct connections are those that in Fig. 5 lay within the inner circle. They show the patient records accessible by the healthcare institutions where the patient has registered to access his/her EHR. Indirect connections are those lying within the outer circle. This usually indicates that a composition has been generated by another healthcare institution, following a request made by the directly connected institution. For example, the main institution, say a hospital, may request a laboratory exam that cannot be performed at site; the results of that exam, despite generated at the laboratory, need also to be available to the hospital that requested it. External connections are the ones laying outside the bigger circle in Fig. 5, and are initiated from any indirect connection. These are usually located three or more links from the patient. Delegations, in Fig. 5 drawn by dotted lines, show the entities that have been temporarily allowed to access a record, with the patient's consent. Section V discusses delegation in more detail. A logging/monitoring feature will also be available to check role, time and date of last accesses to a composition.

PACVIM's access control *visual* model assumes that users have touch-screen devices. Thanks to this technology, patients can select different monitoring and searching functionalities of the parts comprising the EHR by applying hand gestures. Patients need only to touch the respective node or rectangle to zoom in/out and access any content they want. The graph is normally centred on the patient's record - in Fig. 5 that is the human icon from where all the connections start - but patients can re-centre the network according to his/her needs or taste, by dragging nodes around.

Fig. 6 shows an example of the content of three different compositions of an EHR when a patient magnifies a rectangle in the network. These are chronologically ordered. Colours are purely indicative here and just help to represent different compositions and facilitate the identification of the same composition shared at different sites throughout the network.

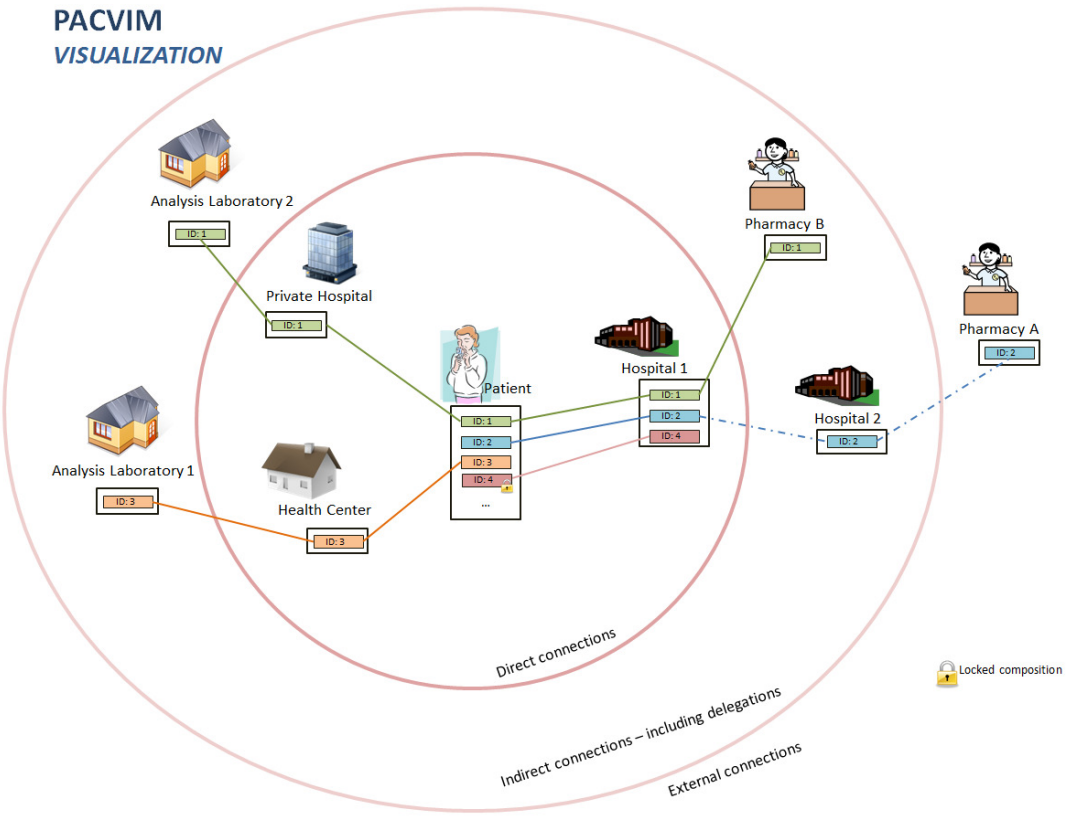

Fig. 5 - PACVIM: visual access control network of a patient's EHR. A dotted line represents a delegation between two institutions and a lock represents a private composition.

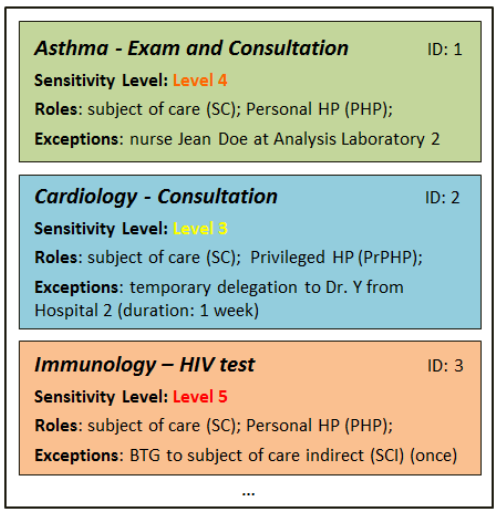

Fig. 6 - Example of an EHR's content with three chronologically ordered compositions.

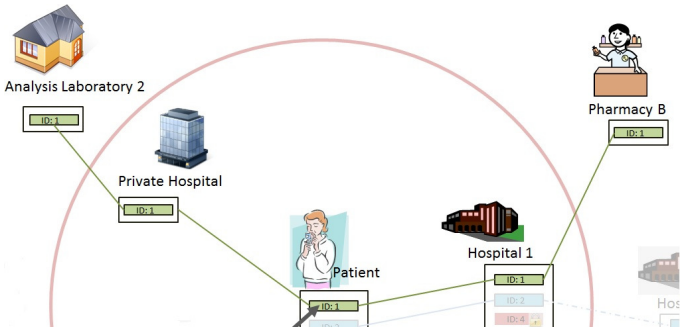

Fig. 7 - View of the Asthma - ID1 composition over the visual access control network.

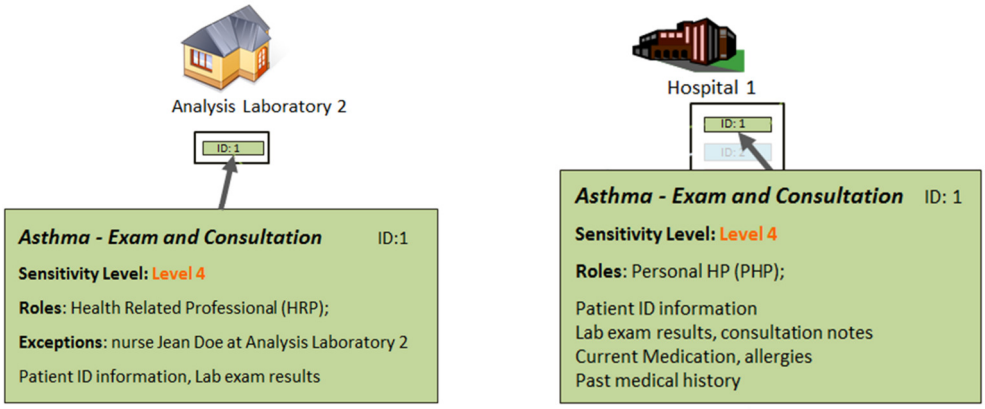

Fig. 8 - Different views of the Asthma Composition - ID1, at two healthcare institutions (e.g. Analysis Laboratory 2 (left) and Hospital 1 (right)).

A composition may include information regarding: (a) the clinical episode (clinical content is not shown here); (b) which roles – corresponding to types of healthcare professionals and associated permissions - can access a composition (e.g., the patient as subject of care; the patient's GP as Personal HP; as defined in [28]); (c) exceptions to those roles, which can be applied directly to a role or a specific user (e.g., a role or a user from a group of professionals can perform *Break-the-glass* on a composition); (d) sensitivity levels and any other information that may be relevant to both patients and healthcare professionals. The sensitivity level of a composition, expresses which groups of roles can access it and these can be set by default depending on the type of episode, specialty and healthcare professional creating that composition. It can also be customized later by that same healthcare professional or perhaps another with, at least, the same access control permissions. The higher the sensitivity level, the more sensitive is the information and only more privileged and restricted roles can access it.

Healthcare professionals can be allowed to have their private EHR's compositions. These pieces of information can be directly or indirectly related to the patient, but should be accessed only by its owner, i.e., the professional who created them. In Fig. 5, a lock (🔒) indicates the presence of private compositions and in this example, the patient can see a locked composition, where it was created, and by whom, but cannot access its content.

PACVIM permits different views. For instance, if the patient only wants to view the Asthma – ID1 composition of his/her EHR (Fig. 7), these would be highlighted over the other components, showing a subset of the full graph. The same composition could have different contents and access roles depending on the healthcare institution where it is available or shared. Fig. 8 shows two views and content of the same composition (in this case the Asthma composition ID 1) in two different healthcare institutions. Although the sensitivity level is the same, the roles for each institution are different and therefore, relate to also different access control permissions and composition's content. In the example shown for asthma consultation, the information needed in an analysis laboratory to perform the required exams, is not the same as in a hospital where the healthcare professional accesses these exams and, together with other patient information, has to perform a more accurate diagnostic.

All colors and graphics presented here are just for reference and will most likely change/evolve as research studies with patients and healthcare professionals will provide more adequate visual, usability and security requirements.

V. Discussion & Future Work

To implement PACVIM is challenging because of the socio-technical nature of the healthcare domain and the non-expertise of patients who are going to use it. PACVIM must provide socio-technical security, because even if security mechanisms may be proven robust they may still rely on users' decisions and the context where they are set, to reliably work. Further, all this needs to be applied without compromising usability.

Such issues need to be addressed accordingly. This section discusses the visionary design proposed so far, and present what needs to be done so that it can be realized and used by the patients, on a daily basis.

Concerning its visualization features, PACVIM offers patients a visual way to access and browse their EHR. The authors believe that the proposed graphical interface is simple, because it is inspired by state-of-the-art user-friendly strategies like Transparent Enhancing Tools. Of course this claim should be validated by experiments with real users. When running on interactive mobile devices, PACVIM offers patients gestures to interact with the EHR. This feature should appear familiar to the majority of patients which are accustomed to carry on several everyday interactive activities such as browsing, playing and shopping, in touch screen devices.

Concerning security, PACVIM comprises access control policies and enforces the necessary security mechanisms since it integrates with a secure and transparent infrastructure (i.e.,

OFELIA) that is located within a healthcare institution's security perimeter and policies. In general, OFELIA's technical security has been tested elsewhere [16], but it is necessary to evaluate how its integration in PACVIM is going to be reliable and robust when PACVIM is used daily by non-experts. The authors intend to apply techniques of socio-technical analysis, such as those proposed in [15], to estimate PACVIM's usable security.

Regarding *registration* and *authentication/authorisation*, PACVIM uses QR codes. It has been proved that the use of QR codes for accessing resources is efficient, easy to understand and secure (at least from certain types of attacks, like shoulder surfing) [16][26]. Surely, the patient's device and the EHR server can exchange information without the patient's manually entering complex data strings. However, to be able to register, patients need to be instructed about the process and be physically present at each health institution hosting the EHR whose access is being requested. This could discourage some patients. However, registration is requested only once and after patients have registered, they can take advantage of the PACVIM's interface and have a seamless and transparent visual access to all the medical records. Patients should have Internet connectivity, which they commonly have, and use their preferred browser to authenticate, connect and browse the EHR shown on the PACVIM's visual interface.

Preliminary studies indicate that patients understand registration and authentication implemented in this way, but there is the need to test it further and in real health scenarios with a bigger and more diversified sample of patients. Qualitative and quantitative studies need to be performed in order to define what types of visualization are adequate to the different communities of patients, together with their main goals regarding healthcare diagnosis and treatments. These studies can also be applied to devise what is the most useful and required information inside an EHR composition. The composition's content is compliant with current ISO directives, but this needs also to be defined by both patients and healthcare professionals. Moreover, a definition of the different views for each type of end-users' community, goals and characteristics, is still required to make PACVIM usable widely. For instance, as already mentioned, healthcare professionals could prefer creating private compositions, inaccessible to patients. Such features, if required, raise further questions: should locked compositions be visible to patients or should they be completely transparent to them? Such interrogatives can also be answered within the preliminary studies and experiments to design and implement PACVIM.

At present, the proposed PACVIM design gives patients read-only access. But there is already a scenario, delegation, where would be reasonable to let patients intervene and decide upon who can access their EHR. In fact, delegation is granting temporary access permissions to subjects outside the defined access control policy network. It would not be difficult to extend the current design to realize this feature: healthcare professionals would have to invoice a delegation request to the patient's mobile device using OFELIA. After the patient successfully identifies and authenticates those professionals, s/he can decide to allow that request or designate a responsible to handle it, likely a trustee acting on the patient's behalf. PACVIM sets up a delegation connection by attributing a temporary role to the healthcare professional that needs to access his/her composition(s). The status of the delegation can be monitored and audited at any time: delegations appear as dotted lines in the EHR network (Fig. 5).

Other future work is about including advanced features in PACVIM. The first is allowing *compositions* for alternative medical encounters or patients' notes – e.g., acupuncture, physiotherapy or even a patient's health diary. A second feature is to add *advanced search tools* able to index with fine-grained detail the pieces of information contained within the compositions. Searching may be a must, when an EHR network becomes too big to be represented in one screenshot, or when it has too many healthcare institutions that share a patient's EHR and turns out to be highly confusing. There may be the need to adapt different views according to this and other factors. A third and last feature is about permitting *to edit/change roles*. A patient's control could be extended with the right to manage roles attributed to the healthcare professionals in healthcare institutions, of course in limited, well-defined situations. For example, access can be granted to substitute general practitioners or, for example, to allow doctors that happen to be around and help the patient in some urgent, first-aid situation [33].

To conclude this discussion, is important to mention the current status of EHR implementations. Although some of those databases are up and running, there is little or no standard solutions to integrate the EHRs from different healthcare institutions. Data integration in healthcare is still a very big and unresolved challenge. The overall technical security, workflow and access policies enforced by those institutions are likely bound to be different. The various systems are probably running on different infrastructures, and are implemented from different designs. A step towards this integration is to have an OFELIA web service acting as an integrator layer and running in every EHR. There are plans to test OFELIA in two different healthcare institutions but this is a long term future work for it involves coping with different administrations, regulations and other constraints. However, this does not impede to build a PACVIM prototype, and test it, at first within one hospital where different EHR compositions are created and shared within various medical departments.

VI. CONCLUSION

This paper presents and discusses a preliminary design of PACVIM, an access control visual application that allows patients to access their EHR. No such application is available yet. The proposed visionary design addresses socio-technical security and usability features, but further research studies are needed to put into practice the vision presented in this paper. These include: (a) a survey applied to patients and healthcare professionals to know more about their opinions regarding

PACVIM, its possible uses and expectations; (b) designing and building a PACVIM prototype, which integrates the results obtained in (a); and (c) applying this prototype in one or various healthcare practices to learn more in terms of its security and usability aspects, in order to enhance PACVIM.

ACKNOWLEDGMENT

This research is supported by CORE-FNR Luxembourg "Socio-Technical Analysis of Security and Trust" [I2R-APS-PFN-11STAST] and project I-CITY "ICT for Future Health" [NORTE-07-0124-FEDER- 000068].

REFERENCES

[1] Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data. Council of Europe – Committee of Ministers, 1997.

[2] U.S. Department of Health & Human Services, Health insurance portability and accountability act, 1996.

[3] Lei Acesso aos Documentos da Administração, Artigos 5º e 7º. Diário da República 46/2007.

[4] F. Falcão-Reis, M. E. Correia, L. Sousa, "Towards patient empowerment – can the patient really decide?", in 11th World Congress on Medical Physics and Biomedical Engineering, vol. 25, pp. 345-348, 2009.

[5] R. P. Burke, A. F. Rossi, B. R. Wilner, R. L. Hannan, J. A. Zabinsky, J. A. White, "Transforming patient and family access to medical information: utilisation patterns of a patient-accessible electronic health record" in Cardiol Youngm, vol. 20, pp. 477–84, 2010.

[6] R. Van der Vaart, C. Drossaert, E. Taal, M. Laar, "Giving patients online home access to their electronic medical record (EMR): advantages, drawback and preconditions according to care providers" in Rheumatol Int, vol. 33, pp. 20405-10, 2013.

[7] C. Bartlett, K. Simpson, A. N. Turner, "Patient access to complex chronic disease records on the Internet" in BMC Medical Informatics and Decision Making, vol. 12, 2012.

[8] C. Pyper, J. Amery, M. Watson, C. Crook, "Access to electronic health records in primary care - a survey of patients' view" in Med Sci Monit, vol. 10, pp. 17-22, 2004.

[9] M. Peleg, D. Beimel, D. Dori, Y. Denekamp,"Situation-based access control: privacy management via modeling of patient data access scenarios" in J Biomed Inform, vol. 41, pp. 1028–40, 2008.

[10] D. W. Roblin, T. K. Houston, J. J. Allison, P. J. Joski, E. R. Becker, "Disparities in use of a personal health record in a managed care organization" in JAMIA, vol. 16, pp. 683-689, 2009.

[11] A. Ferreira, A. Correia, A. Silva, A. Corte, A. Pinto, A. L. Saavedra, A. F. Pereira, R. Cruz-Correia, L. F. Antunes. "Why facilitate patient access to medical records" in Medical and Care Compunetics, vol. 127, pp. 77-90, 2007.

[12] K. Hayrinen, K. Saranto, P. Nykanen, "Definition, structure, content, use and impacts of electronic healthrecords: A review of the research literature" in Int J Med Inform, vol. 77, pp. 291-304, 2008.

[13] K. D. Mandl, P. Szolovitz, I. S. Kohan, "Public standards and patients' control: keep electronic medical records accessible but private" in BMJ, vol. 322, pp. 1368-9, 2001.

[14] A. Bakker "Access to EHR and access control at a moment in the past: a discussion of the need and an exploration of the consequences" in Int J Med Inform, vol. 73, pp. 267-70, 2004.

[15] A. Ferreira, R. Giustolisi, J-L. Huynen, V. Koenig, G. Lenzini, "Studies in socio-technical security analysis: authentication of identities with TLS certificates" in 3rd IEEE International Symposium on Trust and Identity in Mobile Internet, Computing and Communications (TrustID), 2013.

[16] A. B. Augusto, M. E. Correia. "OFELIA – a secure mobile attribute aggregation infrastructure for user-centric identity management" in Proceedings of the IFIP - Information Security and Privacy Research - Advances in Information and Communication Technology, vol. 376, pp. 61-74, 2012.

[17] D. W. Roblin, T. K. Houston, J. J. Allison, P. J. Joski, E. R. Becker, "Disparities in use of a personal health record in a managed care organization" in JAMIA, vol. 16, pp. 683-689, 2009.

[18] Google Health: http://www.google.com/intl/en_us/health/about/ http://googleblog.blogspot.com/2011/06/update-on-google-health-and-google.html. Accessed in November 2013.

[19] I. Carrión, JL. Fernández-Alemán, A. Toval, "Are personal health records safe? A review of free web-accessible personal health record privacy policies", J Med Internet Res, vol. 14, 2012.

[20] A. Kharrazi, R.Chisholm, D. VanNasdale, B. Thompson, "Mobile personal health records: an evaluation of features and functionality" in Int J Med Inform, vol. 81, pp. 579-593, 2012.

[21] M. Anwar, W. L. Philip, A. Fong, "A visualization tool for evaluating access control policies in facebook-style social network systems" in Proceedings of the 27th Annual ACM Symposium on Applied Computing, pp. 1443-1450, 2012.

[22] P. Díaz, I. Aedo, D. Sanz, A. Malizia, " A model-driven approach for the visual specification of Role-Based Access Control policies in web systems" in IEEE Symposium on Visual Languages and Human-Centric Computing, 2008.

[23] M. Harbach, M. Smith, "Visual access control for research ecosystems" in 5th IEEE International Conference on Digital Ecosystems and Technologies, 2011.

[24] S. Fahl, M. Harbach, M. Smith, "Towards human-centric visual access control for clinical data management" in Stud Health Technol Inform, vol. 180, pp. 756-60, 2012.

[25] C. Santos-Pereira, A. B. Augusto, M. E. Correia, A. Ferreira, R. Cruz-Correia, "A mobile based authorisation mechanism for patient managed tole based access control" in Information Technology in Bio- and Medical Informatics, Lecture Notes in Computer Science, vol. 7451, pp. 54-68, 2012.

[26] H. C. Huang, F. C. Chang, W. C. Fang, "Reversible data hiding with histogram-based difference expansion for QR code applications" in IEEE Transactions on Consumer Electronics, vol. 57, pp. 779-787, 2011.

[27] University of Maryland at College Park, "Questionnaire for User Interaction Satisfaction-QUIS", vol. QUIS 7.0 ed.

[28] ISO/TS 13606-4, "Health informatics - electronic health record communication – Part 4: Security", 2009.

[29] HL7 Security Technical Committee, Role Based Access Control (RBAC) Healthcare Permission Catalog, in *Release 2*, ed: HL7, 2010.

[30] C. Santos-Pereira, L. Antunes, R. Cruz-Correia, A. Ferreira, "One way to patient empowerment - a proposal for an authorization model" in Proceedings of the International Conference on Health Informatics, pp. 249–255, 2012.

[31] HL7 Security Technical Committee, Role Based Access Control (RBAC) Healthcare Constraint Catalog, ed: HL7 2010.

[32] M. Janic, P. Wijbenga, T. Veugen, "Transparency enhancihng tools (TETs): an overview", STAST workshop, 2013.

[33] O. Garcia-Morchon, K. Wehrle, "Efficient and context-aware access control for pervasive medical sensor networks" in Pervasive Computing and Communications Workshops, pp.322-327, 2010.