TOWARDS AN EHR ARCHITECTURE FOR MOBILE CITIZENS

Tiago Pedrosa, Rui Pedro Lopes
Polytechnic Institute of Bragança, Portugal
pedrosa@ipb.pt, rlopes@ipb.pt

João C. Santos
Coimbra Institute of Engineering, DEE, Portugal
jcandido@isec.pt

Carlos Costa, José Luís Oliveira
University of Aveiro - IEETA, Portugal
carlos.costa@ua.pt, jlo@ua.pt

Keywords: EHR, PHR, Integrated access, Security.

Abstract: Electronic Health Records are typically created and stored in different places, by different healthcare providers, using different formats and technology. This poses an obstacle to patient mobility and contributes to scatter personal health related information. Patients constantly move between healthcare providers, searching for a better service, lower prices or specialists. It is important that healthcare professionals, regardless of technology and location, have access to the complete patient health record. The access to this personal health record can be granted through a network (web-based, for example) or can be carried by the patient, in a usb drive, for example. Either approach has to enforce the patient consent to access his information, cope with different types of EHR systems and formats. This paper is an ongoing research, part of a PhD on Electronic Health Records for Mobile Citizens.

1 INTRODUCTION

The typical medical procedure aims at recognizing a disease or a health problem based on a set of symptoms and signs. To facilitate the process, the physician will try to build the diagnostic based on physical signs and medical tests. The result of the tests, such as blood pressure, medical imaging, electrocardiogram, and others is information that will contribute to the patient's medical history, or health record, a valuable insight for future diagnostics. In the past, this information was paper-based, which suffered from problems such as of illegibility, unavailability, volume of the health record during patient life, difficulty of sharing information between the different healthcare providers (which frequently implies duplication of information) (Román et al., 2006; Coiera, 2003; Pories, 1990). Moreover, the paper-based record demands a huge number of resources to do the routing, archiving and maintenance of the records, for all the presented reasons and others it can be said that the paper-based patient record is reaching it's limits (Uslu and Stausberg, 2008).

In the natural evolution of the paper-based health record appeared the Electronic Health Record (EHR), as an alternative to paper-based records. Different types of EHRs exist but the most promising is the Integrated Care EHR (ICEHR), that acts as a repository of all the health information of a patient, responsible for storing, manage access to the information in a secure away. The repository should maintain information about the clinic history of the patient, as well current produced information and prospective information (Technical Committee ISO/TC 215, 2005).

The paper-based record also affects the mobility of the citizens, increasing the problems of medical information sharing and access. The health record is typically stored in a specific health provider, which may cause difficulties if the patient is mobile. Mobility is inevitable and proportional to the mobility of persons, either for professional, personal or medical reasons. Mobility exists at local, regional, national and international scope, between public and private healthcare providers. For creating a useful ICEHR it is necessary to create an unique view of the scattered health information across different providers. Hence,

it is unavoidable that the different systems need to address such challenges as a standardized logical information model, persistence of information, and aspects such as security and privacy of the records. At a lower level, functional interoperability is needed for sharing information, but a semantic interoperability would increase the value of the solution. For achieving the semantic interoperability, the option is the standardization of clinical concepts using terminologies, archetypes and templates. A logical information model is being developed by organizations such as ISO (International Organization for Standardization), CEN (European Committee for Standardization), HL7(Health Level Seven) and the OpenEHR project.

Despite these efforts, many systems are already in use with different or without communication mechanisms, they have different identification codes for the same patient, using divergent terminology and coding schemas.

This paper presents an access control solution that creates an unified view of disperse patient health-care information, allowing the achievement of the goals of an IEHR. The developed model is supported by a centralized access control mechanism that implements the intent consent policy when the patient can control the access to his/her personal information. Moreover, to attain the IEHR, several services gather disperse health information, create an unified view of the health record and enforce the access policy to health professionals.

2 RELATED WORK

Different approaches on the creation of the EHRs exists and are already being used. First, it should be differentiated the two main streams: the Electronic Health Records (EHR) and the Personal Health Record (PHR). They can have the same record architecture but they differ in the data custody ownership, which has also the responsibility of manage it. The PHR can be a self-contained registry, maintained and controlled by the subject of care. It can be based on a specific portable data storage, some entry in a web service provider or even a component of an IEHR. In the EHR case healthcare providers are responsible for its maintenance (Technical Committee ISO/TC 215, 2005).

In this interoperability context, standardization is the solution to enable the communication between different systems. Several European and American committees, country initiatives and also the World Health Organization, are putting efforts into this goal. These attempts pushed forward the research, but they also brought results that evidence standards interoperability barriers. These efforts can be divided in two main areas: the communication standard and the document standard (Sunyaev et al., 2008). The former refers how systems can communicate with each other and the later describes how information is stored to ensure a correct interpretation by other systems.

Several standardization results were already obtained concerning health care information, some dealing with data integration approach, others with data transfer. HL7/CDA proposal copes with the communication and document needs by the different functions in healthcare, from hospital information systems (HIS), radiology information systems (RIS), picture archiving and communication systems (PACS), to EHR. It supports prescriptions, emergency and administrative data. Others such as DICOM, xDT and EDIFACT support fewer healthcare functions but have also played important roles in specific domains (Sunyaev et al., 2008). The standardization approaches are necessary for enabling communication capability between the different institutions' systems, but the problem remains, i.e. the unique view of the disperse EHR will persist. The mobility factor poses challenges as information dispersion between different healthcare providers' systems increases. Even a solution where the health records are centralized in one place, cannot cope with mobility constraints. It can be accepted that a national centralization of medical data, at most, could exist , but a world-wide centralization is not feasible (Hasselbring, 1997). So the information will continue to be stored in different systems bringing the need to create interoperability solutions between those systems and data.

In the last decade, the use of smart-cards in healthcare information systems has been consensual, as they provide a secure way for storing information and authentication credentials for remote authentication (Chien et al., 2002). The Electronic Health Card (EHC) is basically a smart-card that is used to support information related with administrative tasks, emergency medical data, security certificates and, in some cases, e-prescriptions. This type of tokens is used in some countries like, for instance, Germany and Austria to achieve a national IEHR solution.

As discussed, the IEHR implementations need to provide an integrated access mechanism to disperse information. So, the integrator system must know the data location and, more precisely, the query engine service to extract information of a specific patient. This linkage information can be stored in the integrator database, however some projects decided to extend electronic health card to support that ser-

vice. Hence, the Virtual Unique Electronic Patient Card (VU-EPR) appears as a possible solution. Costa et al (Costa et al., 2003; Ferreira Polónia et al., 2005; Carlos Costa, 2003; Carlos Costa,) developed a VU-EPR solution named Multi-Service Patient Data Card (MS-PDC).

The MS-PDC is based on a token that contains card-owner resident clinic-admin information, as well as structured references to its distributed electronic records. The smart card securely contains this reference, a structured data set. The association of Public Keys Cryptography and Crypto Smart Cards, provides a way to securely store, transport and access the card-owner information. Moreover, it also grants the owner full control over the access to its data, through a PIN and/or biometric registration.

This MS-PDC model empowers patients, enabling the discretionary access to remote data, when crossed VU-EPR card with health professional card, and also allows an open access to the medical emergency data stored in the card. It also allows the card-owner to entitle information access levels to other users such as the clinical professionals. The main benefits associated to this solution can be characterized by highly scattered geographical storage requirements.

The MS-PDC uses URLs to fetch the information on the disperse systems and present them to the user as a unique view. This model copes well with mobility issues, such as the gathering of disperse data and controlling the access to it. Nevertheless, in a wider concept of mobility it's not feasible that all patients will hold the same type of card world-wide. Another discussable aspect is the physical dependency of the card whenever exists the need to access the patient IEHR. Many other questions can be associated with this model like, for instance: How to retrieve data from systems with different communication and data standards? How can the references be dynamically updated when new information is created, if the card is not present? In this approach the new information is created in EHR systems, what to do when such system is not available?

The model, on Section 3,appears as a solution to the problems of previous approaches in patient mobility environment.

3 RESULTS

As a result of the drop-backs identified in previous approach, this paper proposes a model, based on the MS-PDC concept, for coping with the special needs of citizens' mobility.

Since many health providers already use EHR systems, it is proposed that those systems would continue to be used for producing new patient information. Our novelty is in the information search and display mechanism that uses a different solution to promote the integrated access to disperse health information. The approach is compliant with the freedom of choice of an EHR system by each healthcare provider. With institutions where an information system is not available in mind, this model enables the use of a web-based PHR (Figure 1). Hence, the proposed integrated access mechanism will enable the users to have a unique unified health record that dynamically concatenates all available information in the network, i.e. EHR and web-based PHR data elements.

The display of disperse patient information in a unique view is issued by a proxy component that will be used for querying the remote EHR systems and the web-based PHR (Figure 1). The proxy will implement mechanisms for understanding the remote coding, terminology and communication protocol. It will also translate the results to a common terminology and coding for creating the read-only unique EHR. This proxy mechanism will be modular and will be developed as an interface module to talk with each type of remote EHR system. Moreover, for systems that don't have the ability to be queried remotely, a broker should be deployed to enable the proxy communication with that remote system. To query all the desired information, the proxy must establish a trust relation with every remote EHR and web-based PHR. The authorization control responsibility will be delegate to a trusted agent component (Figure 1), respecting the privileges of the requesting user.

Resuming, the proxy and the trusted agent component need to know where is the information of a specific patient, how to retrieve it and which information should be available for the requesting user. All those important issues are the responsibility of a Virtual Health Card System (VHCS). The VHCS is a key component that will be explained later on this document. The remote access to the distributed patient information must be authorized by the patient and the local EHR system access will continue to be managed by the local policies of each healthcare provider.

The proposed model (Figure 1) for achieving an Integrated Electronic Health Record (IEHR) copes with the needs of mobile citizens. Basically the model was developed with the goal of providing an integrated access to the disperse health information systems that are already stored in Electronic Health Records, providing a read-only, unique view of patients' IEHR.

The model will just create a new way for viewing the information and will not create more workload for

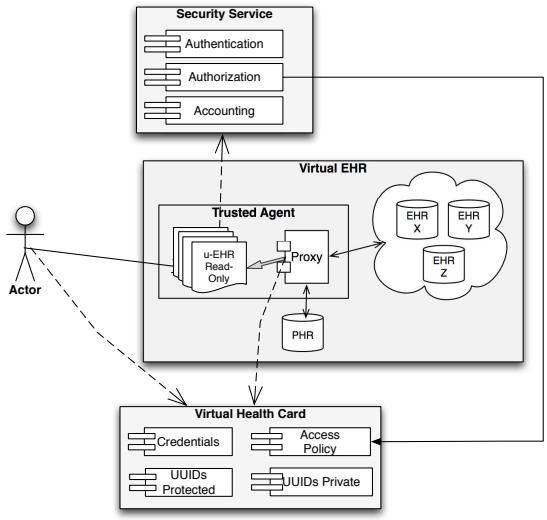

Figure 1: EHR Architecture for Mobile Citizens.

the practitioner since he will continue to work with his usual tools. He will only need to use a different solution for navigation on the IEHR.

In the model, the component VHCS - Virtual Health Card System (Tiago Pedrosa, 2009) is responsible for associating the scattered EHR information of a patient and also for providing the access control mechanisms to the patient information. As information resides in different organizations systems, private and public, even in different countries, the Virtual Health Card System implements the intent consent of the patient to enable the access to his information. The VHCS allows the disassociation between the credentials used by users in system authentication and the credentials used inside the system. For accessing his Electronic Health Card, the user will authenticate himself using a token. The system is sufficiently flexible to support different tokens including the new Portuguese Citizen Card, an electronic identification card (eID card) that contains a certificate for authentication. Moreover, if the user token or eID is lost or stolen, the system can temporary block the access to the Virtual Health Card until the new token is available and associated to a patient Virtual Health Card.

The “intent consent” consists of the patient express permission to grant the health professional access to some part or all of his EHR. This consent enables the patient to manage aspects like who can access and what kind of information a specific health professional can access. Basically, the patient in the first contact with the practitioner creates an access policy rule, including the access privileges. After this consent the practitioner can access the patient EHR while the access rule exists, enabling time limit to the access period that is granted.

The model has also a ”break-the-glass” mechanism that enables the bypass of the access policy, whenever the patient is not able to provide his intent consent. This mechanism will only give access to information that is not protected in a private area. The use of ”break-the-glass” mechanism will generate auditing records for future analysis and detection of misconduct access.

Each patient will have his virtual health card, this component has the patient digital credentials, the EHR access policy and an universal unique identifiers (UUIDs), that will act as links to the disperse information. Each link has also complementary information about access mechanisms (or services).

There are two types of UUIDs (Figure 1). The UUID Private is used to handle references of very sensible and discriminatory information. On this component, the patient can manage the information that he does not want accessible to any health professionals, in any occasion. To enforce this behavior, the system will cypher the references with the users correspondent public-key forcing that only with the user’ private-key this information can be read. The access to this private information demands always the explicit patient consent.

The Protected UUID is the place where other system components (or external services) can update the UUIDs, as new information is being produced in several health systems. Components that, on behalf of an authenticated and authorized user, want to access the patient’s information, query this component to get information about remote patient data location and how access to it.

The credential component is responsible for securely storing the private and public key of the user (Figure 1). The access to the private-key container is only available to the authenticated user (the actor), by the way of a secret (a password or other method (Basney et al., 2005)). The private-key inside the container is the credential that will be used internally for authentication, signing, cypher and de-cypher the information. This modus operandi separates the credentials for authentication in the system from the credentials that the user uses to logon in other system or components in the model.

The Security Service component (Figure 1) is responsible by the practitioner’s authentication, the authorization and the accounting of requests. Hence, each request made to the trusted agent is accounted on this service, this will enable to audit the requests and the creation of a report each time the ”break-the-glass” mechanism is used. This component has also

the critical mission to interact with the access policy on the patient's virtual health card in order to grant access to the EHR to the requesting user.

After this description of model components and functions, we will explain in detail the procedure steps to create a patient unique EHRs, in Figure 2 (for simplicity, the accounting is not represented in the figure). A practitioner, after obtaining patient intent

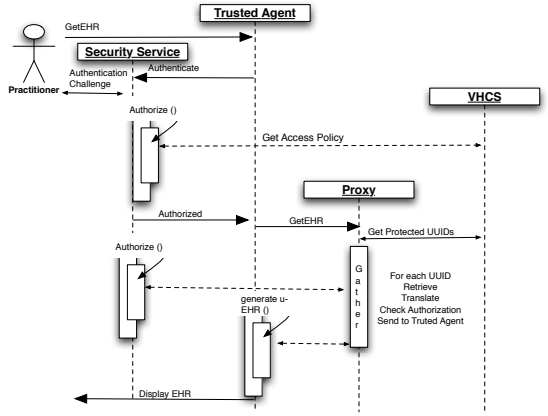

Figure 2: Practitioner getting an EHR.

consent, requests the u-EHR to the trusted agent. The Security Service will do the accounting of this request and will also do the practitioner's authentication in the system. Another important feature is the authorization, so the service will consult the access policy on the patient virtual health card to create the EHR view according to the practitioner privileges. However, in emergency scenarios, the authorization process can be bypassed using the "break-the-glass" mechanism. This will enable the practitioner access to all the information available in the protected UUIDS.

The next step is to gather the information stored in dispersed EHR systems and eventually on the web-based PHR. As previously stated in the Virtual Health Card System exists a component -the protected UUIDs -that works as links to the disperse information and also informs how information should by queried and translated to the u-EHR. This linkage information is passed to the Proxy component. Hence, for each link the proxy will use the correspondent module to communicate with the remote system, retrieve and translate the information to the u-EHR. The retrieved information is filtered according to practitioner privileges. The proxy will do this procedure for all protected UUIDs available on the patient Virtual Health Card. At the end, the trusted agent would have available the u-EHR view corresponding to the practitioner's privileges. With this behaviour, only the information in the protected UUID component is gathered, the information that the patient considered private is not contemplated. To enable the access to private UUID data, the patient must explicitly request the access to the trusted agent, i.e. given his express consent.

Concluding, the intent consent is done by the patient directly to the VHCS. He defines, for each health professional, the access level to his information. The model is generic enough to allow the patient's definition of access policy or it can use a service that defines the privileges that each category of professionals should have to the EHR. In the former, the patient would have to create the complete access policy, defining which type of information of his EHR the health professional could access. In the later approach, a system that maps each category of health professionals to the type of information it should access can be used, the patient only needs to choose the health professional that he wants to grant access and the category of the professional. The model can even cope with an external service that could create the access rules in the policy of each patient.

4 CONCLUSIONS

The proposed VHCS is an integrated access model to disperse healthcare information. The main achievement is the implementation of a unique EHR that copes well with requirements of mobile citizens. This model implements the patient intent consent to enable the sharing of sensible information between different healthcare actors. It promotes the transparent use of existent EHR systems in the healthcare providers. Moreover, where a local system is not available, it provides a web-based PHR solution to save the new information.

The model separates the credentials used in authentication from the credentials used in the indexing system. It enables the creation of a dynamic mechanism to update references of remote patient information. It also copes with the existence of different identifiers for the same patient, along different healthcare systems. Moreover, it empowers patients with the capability to decide what information is absolutely private. Finally, the use of the informed consent mechanism respects the regulatory framework for sharing healthcare records between distinct professionals (or institutions) in different regions or countries.

Supplementary work should be done in researching how each component should specified and developed, considering the need of high-availability and of security. It will be also necessary to define the structure, coding and terminology used in the u-EHR.

REFERENCES

Basney, J., Humphrey, M., and Welch, V. (2005). The MyProxy online credential repository. *Software: Practice and Experience*, 35(9):801–816.

Carlos Costa, José Luís Oliveira, A. S. "um sistema de integração e acesso seguro a informação clínica distribuída suportada num cartão de utente de saúde." (a secure and integrated access system for distributed clinical data based on a patient card). Patent Reference PT20040103114 20040429.

Carlos Costa, José Luís Oliveira, A. S. V. G. R. (2003). A new concept for an integrated Healthcare Access Model. *Studies in health technology and informatics*, 95:101.

Chien, H., Jan, J., and Tseng, Y. (2002). An Efficient and Practical Solution to Remote Authentication: Smart Card. *Computers & Security*, 21(4):372–375.

Coiera, E. (2003). *Guide to health informatics*. Arnold London.

Costa, C., Oliveira, J., Silva, A., et al. (2003). A new concept for an integrated healthcare access model. *The new navigators: from professionals to patients: proceedings of MIE2003*, page 101.

Ferreira Polónia, D., Costa, C., and Oliveira, J. (2005). Architecture evaluation for the implementation of a regional integrated electronic health record. Connecting Medical Informatics and Bio-Informatics—Proceedings of MIE2005—The XIXth International Congress of the European Federation for Medical Informatics. Geneva: IOS Press.

Hasselbring, W. (1997). Federated integration of replicated information within hospitals. *International Journal on Digital Libraries*, 1(3):192–208.

Pories, W. (1990). Is the medical record dangerous to our health? *NC Med J*, 51(1):47–55.

Román, I., Roa, L., Reina-Tosina, J., and Madinabeitia, G. (2006). Demographic management in a federated healthcare environment. *International Journal of Medical Informatics*.

Sunyaev, A., Leimeister, J., Schweiger, A., and Krcmar, H. (2008). It-standards and standardization approaches in healthcare. *Encyclopedia of Healthcare Information Systems. Editors: Wickramasinghe, N.; Geisler, Publisher: Idea Group*.

Technical Committee ISO/TC 215 (2005). Health informatics — electronic health record — definition, scope, and context - iso/tr 20514:2005(e). Technical report, International Organization for Standardization.

Tiago Pedrosa, Carlos Costa, J. L. O. R. P. L. (2009). Virtual health card system. *Inforum 2009*.

Uslu, A. M. and Stausberg, J. (2008). Value of the electronic patient record: An analysis of the literature. *Journal of Biomedical Informatics*, 41(4):675 – 682.