Digital Healthcare Empowering Europeans
R. Cornet et al. (Eds.)
© 2015 European Federation for Medical Informatics (EFMI).
This article is published online with Open Access by IOS Press and distributed under the terms of the Creative Commons Attribution Non-Commercial License.
doi:10.3233/978-1-61499-512-8-823

Privacy provision in eHealth using external services

Jaime DELGADO and Silvia LLORENTE

Distributed Multimedia Applications Group (DMAG)
Computer Architecture Department (DAC)
Universitat Politècnica de Catalunya (UPC)

Abstract. Privacy provision is a key issue for successful secure access to patients' health information. Current approaches do not always provide patients with the ability to define suitable rules to access to their information in a secure way. This paper presents an approach to give patients control over their information by means of external services. In this way, health information management and access control are kept independent and more secure.

Keywords. Medical Informatics Applications, Patient Data Privacy.

Introduction

Nowadays, most medical institutions have digitized the clinical information of their patients and many of them directly work in a digital environment. Therefore, there is a strong need of systems to manage health information, i.e. Electronic Health Records (EHR), in an efficient and secure manner. In this context, a major issue has raised: The protection of patients' privacy. Our approach consists in allowing patients (or medical organizations on their behalf) to define their own policy rules in the most granular way. Of course, there is always the possibility to simplify the granularity level definition. Then, the access control based on those rules is managed by an external independent and secure system.

1. Methods

The main objective of this paper is to describe a solution we propose to access to medical data preserving patients' privacy. Although there are several requirements to be met, we focus on the protection of patients' privacy by guaranteeing the confidentiality, integrity and availability of their data.

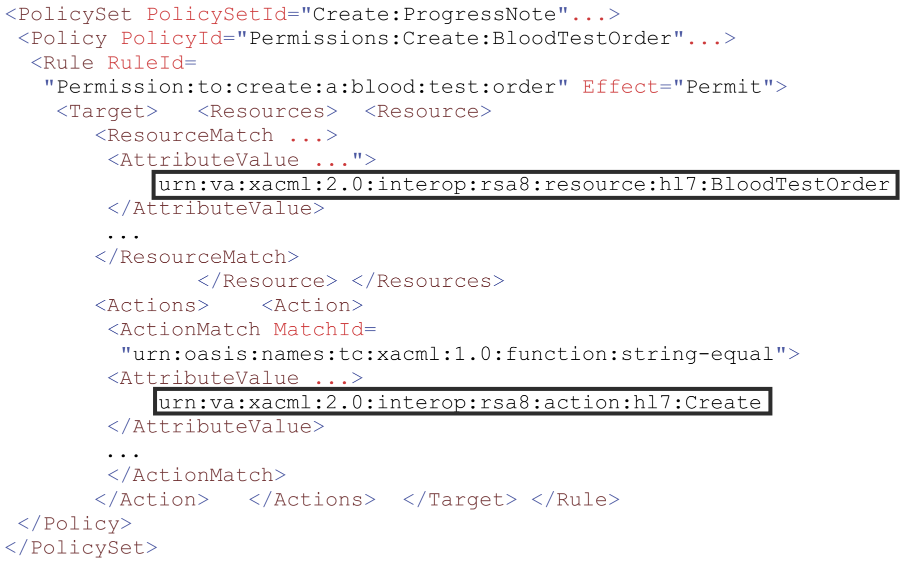
To do so, patients' must be able to state the privacy policies for their medical and personal information, which determines the access rules on the usage and disclosure of their data. In this sense, the association of policies and usage rules to the stored patients' information, together with the notification of events for the later verification of the policies enforcement, will pave the way to a better privacy preserving solution. With such a solution, patients' must be able to verify that the policies specified are enforced.

In addition, the previously mentioned CIA (confidentially, integrity and availability) requirements are met by enforcing the specified privacy rules. Information encryption enhances the security of the whole system.

Definition of privacy policies

EHRs may contain very sensible information regarding patient's health. For this reason, access to this information should be limited only to the right people. For instance, family doctor may have full access, specialist may only have access to the part related to the specific disease she treats, laboratory personnel should only have access to the tests results parts, etc. To provide protected and controlled access to this information, flexibility and granularity are required as well as extremely secure mechanisms. In order to represent the information on how to control access to patients' information, we use eXtensible Access Control Markup Language (XACML) [1], the language selected by HL7 [2] to define access policies.

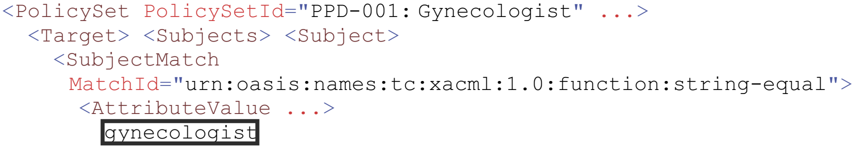
Figure 1 presents an example of an XACML policy that defines the {Create, Blood Test Order} permission and Figure 2 shows how this permission is given to the Gynecologist role.



```
<PolicySet PolicySetId="Create:ProgressNote"...>
 <Policy PolicyId="Permissions:Create:BloodTestOrder"...>
  <Rule RuleId=
   "Permission:to:create:a:blood:test:order" Effect="Permit">
    <Target>   <Resources>  <Resource>
       <ResourceMatch ...>
        <AttributeValue ...">
           urn:va:xacml:2.0:interop:rsa8:resource:hl7:BloodTestOrder
        </AttributeValue>
        ...
       </ResourceMatch>
               </Resource> </Resources>
       <Actions>    <Action>
        <ActionMatch MatchId=
         "urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue ...>
           urn:va:xacml:2.0:interop:rsa8:action:hl7:Create
        </AttributeValue>
        ...
        </ActionMatch>
       </Action>   </Actions>  </Target> </Rule>
 </Policy>
</PolicySet>
```

Figure 1. Create Progress Note XACML policy.

The roles' assignment takes place when users authenticate into the system by means of SAML [3] tokens, which determines the role for the user during the session. In order to enforce the defined rules, a XACML policy based authorizer has been implemented. The specific way in which these elements interoperate in our external system is briefly described in section 2.



```
<PolicySet PolicySetId="PPD-001:Gynecologist" ...>
  <Target> <Subjects> <Subject>
    <SubjectMatch
     MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue ...>
        gynecologist
        </AttributeValue>
        ...
      </SubjectMatch>
    </Subject> </Subjects> </Target>
    <!-- Permissions associated with the ginecologist role -->
    <PolicySetIdReference>
       Create:BloodTestOrder
    </PolicySetIdReference>
  </PolicySet>
```

Figure 2. Lab Technician Permissions Example.

2. Results

Our main result is a standards-based platform for the secure management and access to medical information. This platform allows protecting patients' privacy and guaranteeing the confidentiality, integrity and availability of the patients' data.

The architecture of the proposed framework, which takes MIPAMS (Multimedia Information Protection and Management System) [4] as a starting point, is presented in Figure 3. MIPAMS is a secure digital content management and distribution platform, whose architecture is based on the flexible web services approach. It consists of several modules and services, which provide a subset of the whole system functionality needed for governing and protecting content. The architecture presented here is an adaptation of the original one from MIPAMS, with specific modules to protect health information, which is modelled as a special case of multimedia content. The proposed framework consists of several modules described in [4,5]. The ones specific for health are:

- User Application: It presents the health information to the user. The information presented will depend on user role and XACML rules.
- Object Registration and Content Services: They register medical information, together with resources (medical images, tests results, etc.) associated to it.
- Policy and Authorization Services: They generate and authorize privacy policies expressed in XACML language.

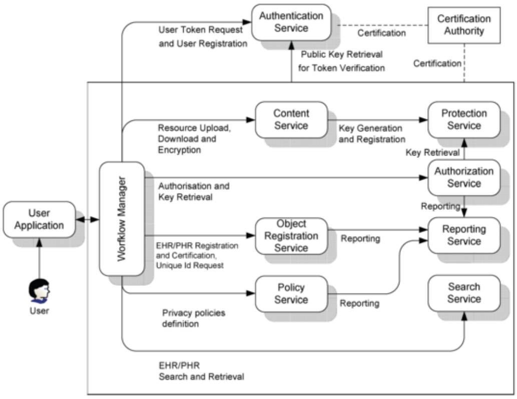

Authentication Service
Certification Authority
User Token Request and User Registration
Certification
Public Key Retrieval for Token Verification
Certification
Content Service
Protection Service
Resource Upload, Download and Encryption
Key Generation and Registration
Key Retrieval
Authorization Service
Authorisation and Key Retrieval
Reporting
Workflow Manager
User Application
Object Registration Service
Reporting Service
Reporting
EHR/PHR Registration and Certification, Unique Id Request
User
Policy Service
Search Service
Reporting
Privacy policies definition
EHR/PHR Search and Retrieval

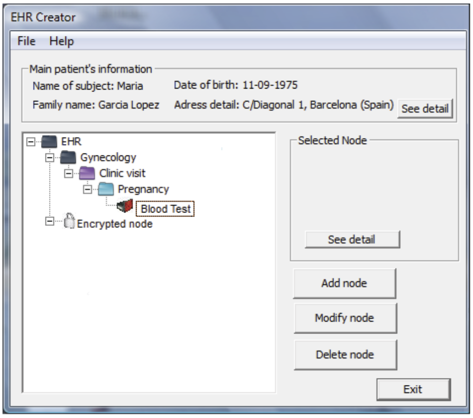
Figure 3. Platform for the management of medical information.

Based on the eHealth specialization of MIPAMS, we have defined a pilot demonstrator, whose implementation from a functionality point of view is described in the Discussion section. The pilot consists on a user application that connects with the different services provided by MIPAMS in order to manage patient clinical data. Its focus is to test if it is feasible to protect clinical data at any level of granularity, from a medical image to the complete EHR. For this purpose, we take advantage of the structure of the clinical information.

3. Discussion

It is worth noting that with the architecture presented in section 2, we can cover several different EHR management scenarios. Our final aim is to facilitate patients the possibility of controlling access over their medical data, from full control by patient, where she completely decides who can access to her medical information (for instance, her family doctor, her relatives, etc.), to give complete control to medical institutions, although patients should still have access to it. Nevertheless, there is always the possibility of medical institution defining template policies to which the patient adheres.

To test the proposed solution, we have implemented a demonstrator that allows creating and managing clinical data (EHRs). Furthermore, we are able to create, in a simple way, privacy policies.



Main patient's information

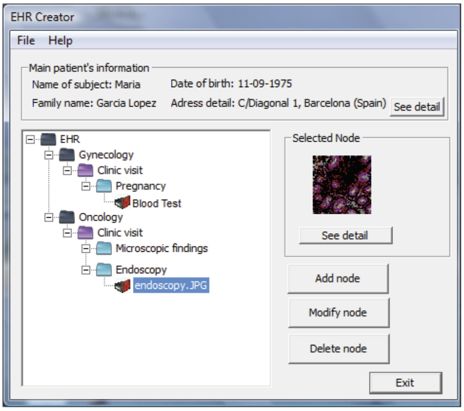
Name of subject: Maria

Date of birth: 11-09-1975

Family name: Garcia Lopez

Adress detail: C/Diagonal 1, Barcelona (Spain)

Figure 4.a. User application screen shot – lab technician view.



Main patient's information

Name of subject: Maria

Date of birth: 11-09-1975

Family name: Garcia Lopez

Adress detail: C/Diagonal 1, Barcelona (Spain)

Figure 4.b. User application screen shot – gynecologist view.

Concerning functionality, the User application module enables users to interact with the clinical data. First, when a registered user authenticates into the system, the Authentication Service generates a SAML-based token for the user, which contains the role for the user for this particular session. Once authenticated, the User application module presents the data to the patients and healthcare providers according to the permissions they have. It also enables users to add and update clinical information, such as in the blood test results example. Figure 4 shows two different views for an EHR. In the first screenshot (Figure 4.a), a lab technician accesses the EHR, and she has only permissions to add and/or edit the patient's undergoing blood test, while in the second one (Figure 4.b), the gynecologist has permissions to view all data within the patient's EHR. Note that each time an authorized user modifies the EHR, the provenance of the data is also stored.

This proposal needs a standard format providing the required level of granularity access, in order to protect only the elements defined by patient. In this way, elements can be protected at different levels, according to several privacy policies. After positive authorization, only the required element is unprotected and shown to the user. The authorization is based on the role and the privacy policies.

On the other hand, an advantage of our approach is that it integrates independent aspects such as a distributed architecture, structured medical information, and expression and governance of privacy policies. Other systems trying to provide privacy over health information do not cover all these aspects [6,7].

4. Conclusions and Future Work

In this paper, we have described a modular architecture that provides secure access control to patient's information using XACML privacy policies and an external system to enforce them. One of the innovative aspects of this approach is that the privacy policies creation and authorization processes are provided by means of secure external web services, which allows an easier integration with existing health information systems willing to provide privacy capabilities to their users, specially their patients. Another important point is the flexible granularity offered by the policies editor and XACML.

In this sense, the authors are involved in a new initiative to provide health professionals with an innovative mechanism to access to HL7 Clinical Document Architecture (CDA) [8] documents while preserving patient's privacy.

Acknowledgements

Part of this work has been co-funded by the Spanish administration: Protection, search and interoperability of multimedia content: New techniques and applications (PBInt) (TEC2011-22989).

References

1. eXtensible Access Control Markup Language (XACML) V3.0, http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf; 2013.
2. HL7 International, http://www.hl7.org/; 2015.
3. OASIS, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2; 2005.
4. Llorente S, Rodriguez E, Delgado J, Torres-Padrosa V. Standards-based architectures for content management, IEEE MultiMedia, Volume: 20, Issue: 4, 62-72; 2013.
5. Rodriguez E, Delgado J, Alcalde G., Protection of patients' privacy by means of standard technologies. Proceedings of the 9th International Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods; 2011.
6. Haas S, Wohlgemuthb S, Echizenb I, Soneharab N, Müllera G. Aspects of privacy for electronic health records. International Journal of Medical Informatics 80; 2011.
7. Fernández-Alemán JL, Carrión Señor I, Oliver Lozoya PA, Toval A. Security and privacy in electronic health records: A systematic literature review. Journal of Biomedical Informatics, Volume 46, Issue 3; 2013.
8. OpenCDA, http://clinicaldocumentengineering.com; 2015.