e-Health – For Continuity of Care
C. Lovis et al. (Eds.)

doi:10.3233/978-1-61499-432-9-413

A model for Consent-Based Privilege Management in Personal Electronic Health Records

Oliver HEINZE[a,1] and Björn BERGH[a]
[a] *University Hospital Heidelberg, Department of Information Technology and Medical Engineering, Heidelberg, Germany.*

Abstract. One of the biggest issues in the domain of standardized, regional, cross-institutional, personal, electronic health records is the privilege management. While many health information exchange projects use IHE-based architectures there are still unsolved questions regarding the restricting parameters a patient can use in the electronic consent configuring access control. This work determines these parameters, derives an information model of privilege management, introduces a set representation of the model and shows how to apply them to EHR architectures. The introduced model can serve as framework for health information exchanges using a consent-based privilege management. The set representation can help to understand the complexity of consent representations.

Keywords. PEHR, informed consent, privilege management, access control, IHE

Introduction

One of the biggest issues in the domain of cross-institutional, regional electronic health records (EHR) is the question of access rights management [1-4]. Whereas many health information exchange projects around the world selected the cross-enterprise document sharing profile (XDS.b) from the worldwide initiative Integrating the Healthcare Enterprise (IHE) and some other surrounding profiles to build those EHRs, the question which technology and which concepts to choose in order to implement a proper access rights management being within the law and matching ethical as well as privacy aspects, is still being discussed. From a technological point of view the basic patient privacy consent (BPPC) profile and solutions based on the extensible access control markup language (XACML), an OASIS standard, are in wide spread use [5-8]. Regarding the content and the scope of an informed consent together with the degree of how far it will be used to manage EHR access rights, the situation is more vague.

The health information exchange in the Rhine-Neckar region is based on a personal electronic health record (PEHR). The concept strongly focuses on the involvement of the citizens making tools available to them empowering them to keep their informational self-determination. One tool is the access control and content management component of the patient portal [9]. Using this tool the patient can decide which content will be transferred from the primary systems to the PEHR and who of

[1] Corresponding Author.

his physicians and caregivers can access it. The architecture of the PEHR is based on IHE profiles and an XACML representation of informed consents. However there are still some open issues concerning the scope, the semantics, and the restricting parameters of the informed consent a patient can use to configure access control.

Thus the objectives of this paper are to

- Determine restricting parameters
- Present a privilege management information model
- Derive a set representation of an electronic consent (eConsent)
- Describe the application in the PEHR

1. Methods

The work presented in this paper is a part of the doctoral thesis of the author. It represents an iteration of the problem-solving design and creation research strategy being used in his thesis.

To determine the restricting parameters the privilege management of the hospital information system of the University Hospital Heidelberg (UHH) has been analysed, the UHH's data privacy officer was interviewed and a literature analysis using MEDLINE was conducted. Afterwards the information model was derived from the parameters and built using entity-relationship-diagrams. Next the model was mapped to our regional setting resulting in the set representation of eConsents. Finally the model and the set representation have been applied to the PEHR architecture.

2. Results

The comprehensive privilege management as well as the content management of the Heidelberg PEHR is controlled by the patient using his electronic consent document as configuration. Integrated health information exchange settings usually use four operations manipulating data in the centralized electronic health record: Create, read, update and delete which are also known as CRUD-operations. In IHE-based setting these operations are executed through message based, standardized transactions, which are used by actors. Actors do represent a role in a software system like a document consumer and are implemented in certain software components. In the case of XDS.b the transactions are

- C: Create/Write: Provide and register document set-b (ITI-41)
- R: Read/Retrieve: Registry stored query (ITI-18) and retrieve document set (ITI-43)
- U: Update: Update document set (ITI-57)
- D: Delete: Delete document set (ITI-62)

2.1. Restricting Parameters

To restrict access to specific content of a PEHR the following question has to be answered: *Who* is allowed to execute *which operation*s on *which information objects* in *what time*?

The who is characterized by a person. A person can have a role, a specialty and it can belong to a professional group and to one or more organizations.

The operations are represented by the CRUD-operations.

The objects represent the content of the record. This can be a single document or a document type. Objects can belong to a specialty, they have an origin like an organization or a subunit and they have an author.

The time restriction can be characterized by a period, a timeframe, an expiring date or a treatment episode (life long, administrative case, medical case).

Finally, a consent document of a patient consists of one or more answers to the question above.

2.2. The privilege management information model

The next step is to derive an information model from the found restricting parameters. Figure 1 displays the entity-relation-ship-diagram of the model including the surrounding of the consent document.

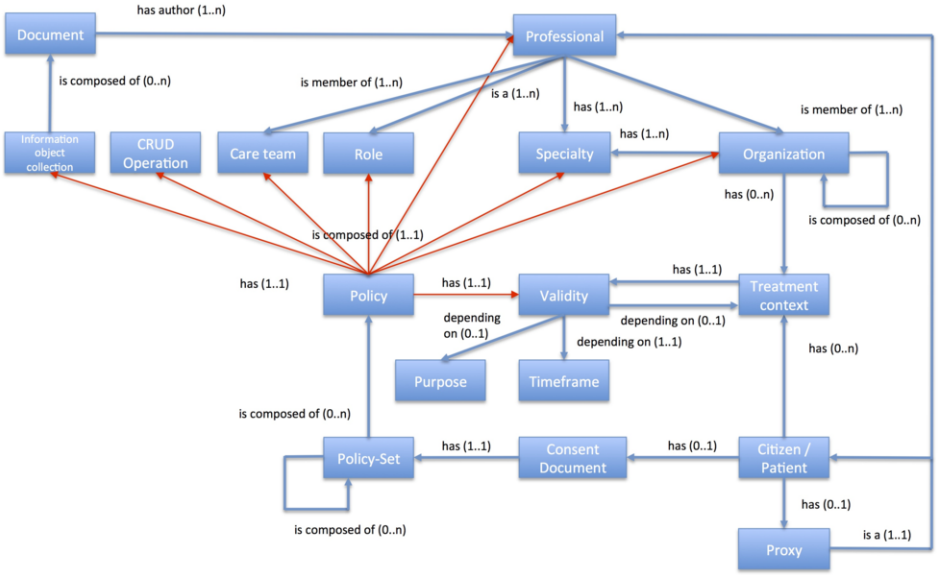

Figure 1. Privilege Management Information Model

Each answer to the question is expressed in one policy and a policy can be grouped inside a policy set, which can be transformed into the XACML syntax representing a consent document. A citizen/patient has got no more than one of them. He has one proxy, which can be another citizen or a professional. A patient has one or more treatment contexts with a validity and one or more organizations. The organization can be composed of other organizations and these can have one or more specialties. A professional has one or more specialties and he can be a member of one or more organizations. He has a role, and he is member of a care team. The red arrows mark the part of the model representing the answers to the question. A policy has a validity, which depends on a timeframe or a purpose (e.g. emergency) and a treatment context.

A policy can be composed of an organization, a specialty, a professional, a role, a care team, a CRUD-operation and an information object collection which is composed of one or more documents, which do have an author who is a professional.

2.3. The set representation of eConsent

For illustration, the information model is mapped to a part of the regional PEHR setting, which is displayed in figure 2. Each policy represents a 3-dimensional set of affected object instances. In the figure the answer to the question is: Each physician with specialty cardiology shall view documents with specialty medication and cardiology. Blue dots are physicians, yellow one's are caregivers, green one's pharmacists. Documents with c are from cardiology with r from radiology and m's do represent medications.

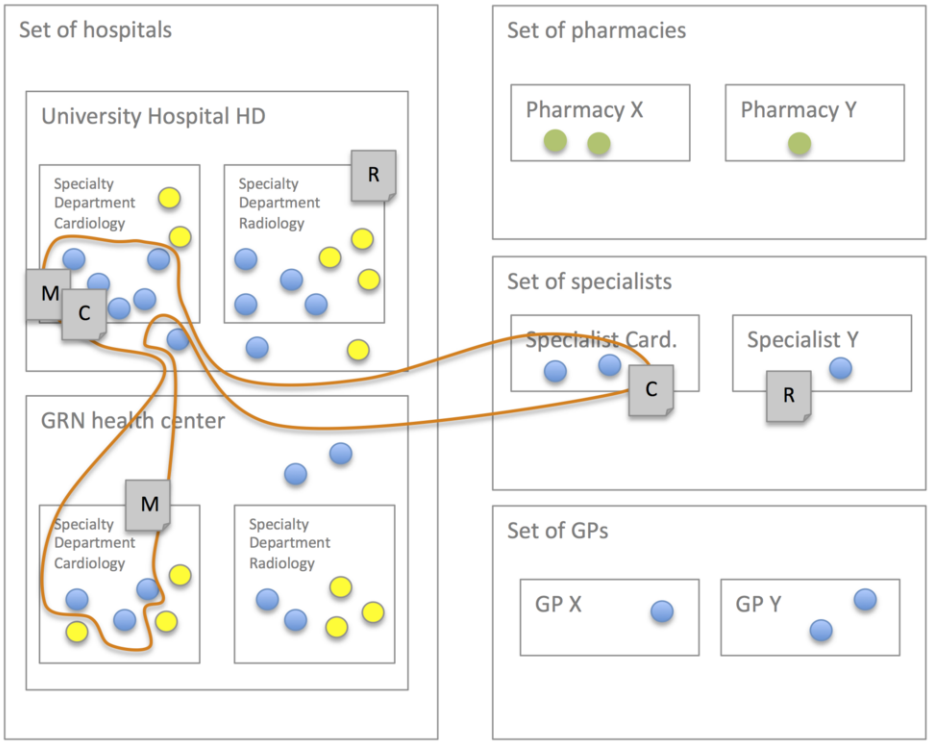

Figure 2. Set representation of eConsent

2.4. Application to the PEHR architecture

To apply the information model to the PEHR architecture it is important to know in which components the restricting parameters are managed and how they are identified and represented. The IHE Health Provider Directory stores information and identifiers of organizations and professionals including specialties and roles. The XDS-Metadata does contain information on the author, the origin, the document type, the specialty and identifiers. The XACML-based consent document has to use the right identifiers and representations of the restricting parameters. Thus the decision making component

(Policy Decision Point) can query the different services for information, compare them with the information inside the consent document and come to a decision if access is granted or not.

3. Discussion

This work describes the derivation of restricting parameters for informed consents and the generation of a comprehensive privilege management information model based on these parameters. The model can be used in any health information exchange project implementing a consent-based privilege management. The comprehensive model can serve as a framework. Not every single parameter has to be implemented. This has to be decided by those responsible. As an example this work described the application to the PEHR architecture of the Rhine-Neckar region.

The introduced set representation of the information model can help to understand the complexity of the consent issue. In the future it might be used in order to graphically configure consent documents.

As a limitation the introduced information model has not been compared to other standardized reference information models like the HL7 RIM yet. This will be one of the next steps in order to derive a standardized representation of the consent document itself as well as the representation of single parameters for example regarding data types.

References

[1] Bergh B, Bach N, Brandner A, Heinze O. *EHR access rights and the role of the patient* in *IFMBE Proceedings World Congress on Medical Physics and Biomedical Engineering*. 2009. Munich, Germany.

[2] Blobel B. *Authorisation and access control for electronic health record systems.* Int J Med Inform, 2004. **73**(3): p. 251-7.

[3] Kluge EH. *Informed consent and the security of the electronic health record (EHR): some policy considerations.* Int J Med Inform, 2004. **73**(3): p. 229-34.

[4] Win KT, Fulcher JA. *Consent mechanisms for electronic health record systems: a simple yet unresolved issue.* J Med Syst, 2007. **31**(2): p. 91-6.

[5] Heinze O, Birkle M, Köster L, Bergh B. *Architecture of a consent management suite and integration into IHE-based Regional Health Information Networks.* BMC medical informatics and decision making, 2011. **11**: p. 58.

[6] Namli T. Dogac A. *Implementation Experiences on IHE XUA and BPPC.* Technical Report Middle East Technical University Ankara, 2006.

[7] Sujansky WV, Faus SA, Stone E, Brennan PF. *A Method to Implement Fine-Grained Access Control for Personal Health Records Through Standard Relational Database Queries.* J Biomed Inform, 2010. **43**(5): p. 46-50.

[8] Idris T, Brandner R, Bergh B, Heinze O. *Eine standardisierte Sicherheitsarchitektur für den einrichtungsübergreifenden Datenaustausch*. in *e-Health2013*. 2012. Solingen: medical future verlag.

[9] Heinze O, Brandner A, Bergh B. *Establishing a personal electronic health record in the Rhine-Neckar region.* Studies in health technology and informatics, 2009. **150**: p. 119.