A Flexible Solution for Privilege Management and Access Control in EHR Systems

G Gazzarata[1,2], B Blobel[3,4,5], M Giacomini[1,6,7]

[1] Department of Informatics, Bioengineering, Robotics and System Engineering, University of Genoa, Italy

[2] Institute of Social Medicine and Health Economy, University of Magdeburg, Germany

[3] Medical Faculty, University of Regensburg, Germany

[4] eHealth Competence Center Bavaria, Deggendorf Institute of Technology, Germany

[5] First Medical Faculty, Charles University Prague, Czech Republic

[6] Healthropy s.r.l., Savona,Italy

[7] HL7 Italy

Abstract

Background: Inter-organizational healthcare businesses are ruled by a huge set of policies: legal policies, organizational policies, medical policies, ethical policies, etc., which are quite static, patients policy and process, social and environmental conditions, which are highly dynamic. In the context of a business case, those different policies must be harmonized to enable privilege management and access control decisions.

Objectives: The authors offer a methodology to achieve interoperability through policies harmonization in a privilege management and access control solution for EHR systems, to be later on implemented in a cancer care network using HL7 specifications.

Methods: To meet the objective, the authors make use of a system-theoretical, architecture-centric, ontology-based approach to formally representing the aforementioned polices for harmonization.

Results: Because of its flexibility and generality, a policy-driven RBAC model is used to formally represent all the other access control models such as MAC, DAC, RBAC, ABAC, HL7 Data Segmentation and Labeling Services. All the policies deployed in the context of an inter-organizational collaboration for cancer care can be formalized and then harmonized.

Conclusions: The authors provide an implementation-independent methodology to enable policies harmonization in EHR systems. The methodology described in the paper is independent on the maturity of organizations' privilege management and access control system. Furthermore, it does not hamper organizations progressing to more advanced solutions over the time. Even dynamic policies can be harmonized at run time, allowing advancement towards a patient-centered care.

Keywords

Electronic Health Record (EHR); Privilege management; Access control; Policy management; Healthcare Privacy and Security Classification System (HCS)

Correspondence to:

Giorgia Gazzarata

Department of Informatics, Bioengineering, Robotics and System Engineering, University of Genoa Via All'Opera Pia 13, 16145, Genoa, Italy.

E-mail: giorgia.gazzarata@gmail.com

EJBI 2017; 13(1):59-66

received: June 18, 2017

accepted: July 01, 2017

published: October 10, 2017

1 Introduction

The University of Genoa – supported by the Institute of Social Medicine and Health Economy at the University of Magdeburg, Germany – currently engages in the establishment of a cancer care network combining regional healthcare establishments at primary, secondary and tertiary care level. Breast cancer is the most frequent type of cancer, establishing 30% of the cancers females in Italy are suffering from [1]. In females, it is the first cause of death [2]. Breast cancer care is a multi-disciplinary challenge involving different specialties and units in a hospital, but can also cross-organizationally include different hospitals, clinics, practices and laboratories.

For improving quality and efficiency of care delivery, health systems around the globe are evolving towards

inter-organizational, inter-regional and even international communication and cooperation, increasingly based on Electronic Health Record (EHR) systems.

Two of the most important prerequisites to inter-organizational collaboration are security and privacy for establishing trust between the actors involved in the business case including the patient. Security aims at guaranteeing information availability, confidentiality, integrity, authenticity and accountability. Privacy is a human right for self-determination, respecting legal requirements, ethical principles, personal preferences and expectations regarding collection, processing, communication and use of personal data, thereby preventing harm from disclosure of that personal information [3]. One of the key elements to provide security and privacy is privilege management and access control to information and functionalities. Figure 1 illustrates the schema of a general access control system [4].

The business case deals with access to clinical objects stored in the EHR, which is not a banal information sharing. Permissions have to be managed in a way that only the medical staff involved in the patient care can access a patient's clinic information according to the 'need to know' principle. It is important to underline that both communication security and application security are relevant. Using an EHR system, the authors will focus on application security, considering communication security as a prerequisite and not healthcare specific.

In healthcare context, policies that have to be respected are a complex mix of legal, organizational, functional, medical, social, ethical and technical aspects [3]. In addition, also personal wishes, local, timely, contextual and environmental constraints have to be considered [5]. We can distinguish at least legal and domain-specific policies, organizational policies, process-related policies as well as personal policies. Domain-specific policies are, e.g., the Hippocratic Oath, the medical code of conduct and ethical principles. The patient consent is frequently mistakenly called a personal policy. However, it is just the agreement or disagreement with an organizational policy [6]. For distributed business cases, also security and privacy management must be realized

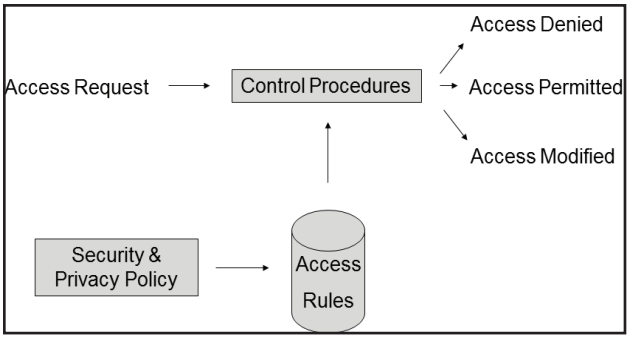

Figure 1: Access control system [4].

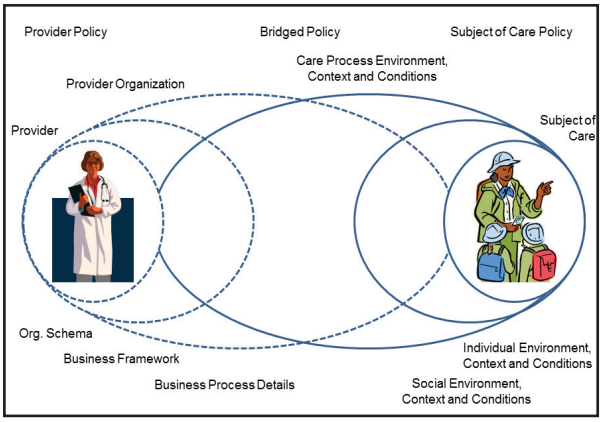

Figure 2: pHealth interoperability schema [7].

in a distributed way. Figure 2 presents the policies and the conditions defining the relation between a physician and a patient [7]. This is the most complex relation, because it involves a large number of policies: legal policies, organizational policies, ethical policies, etc., which are quite static, the subject of care policy and process, social and environment conditions, which are highly dynamic. In the context of a business case, those different policies must be harmonized to enable privilege management and access control decisions. In general, the more the subjects, their knowledge, experiences and skills are close and implicitly sharable, the easier is policy harmonization.

In this paper, the authors want to offer a system-theoretical, architecture-centric, ontology-based, policy-driven approach to achieve interoperability through policies harmonization in a privilege management and access control solution for EHR systems, to be implemented using HL7 specifications.

2 Principles and Methodologies

In order to realize appropriate privilege management and access control, it is fundamental to find a thorough model, which is an abstract representation of that part of the reality the business case deals with. The authors will deploy system theory for that purpose.

A system is group/composition of elements separated from the environment according to properties or needs in the context of a business process. A system could be a part of a super-system, or it can be split in subsystems. A system could be analyzed in two different ways, resulting in the black box approach and the white box approach. The black box approach assesses the system's input-output functional relationship. With this approach, we can describe the overall function of the system without understanding the internal processes and the reasons behind. To carry out greater control, it is necessary to move from the black box to the

white box approach. With the white box analysis, a system is conceived as a collection of interrelated elements. That way, a system is more than just the sum of its components. A system can be represented through its architecture, describing the elements that compose the system, their functions and relationships. The complete understanding of structure, function and relationships of the system elements allows controlling the system itself. The set of rules that controls the behavior of the system is named policy. For managing a quite complex business case, the authors have to use the white box approach.

An ontology is a formal "explicit specification of a conceptualization" [8] of the domain of interest. An ontology defines a controlled vocabulary and represents domain knowledge in a formal and structured form. It consists of concepts, concept definitions and relations between those concepts. A formal description decreases language ambiguity. It allows to make domain assumption explicit, to share knowledge between agents, to re-use and to analyze knowledge [9, 10].

3 Results

In a business process, an entity requests access to some information objects. The purpose of privilege management is to provide the permissions, if any, the entity has, deciding on when, where, why, for which purpose, how, under which conditions. Then, according to the assigned permissions, the request of access to the resource has to be permitted, denied or modified (as instance veiling some information).

In order to guarantee an appropriate privilege management and access control, a prior observation of the business is fundamental. Through observation, interpretation and understanding of the system, its relationships and its rules can be derived and represented as knowledge. Accepted ontologies enable creation, representation and management of the knowledge about the domain of interest in a consistent, reasonably expressive and formalized way that properly reflects the reality.

For realizing interoperability, i.e. advanced communication and cooperation, the different policies must be harmonized. If policies are static and can therefore be predefined, policy harmonization can be performed in advance by coordinating or aligning policies relevant for the predefined business case in the design and definition phase already. This is, e.g., the case when defining, negotiating and contracting disease management programs (DMPs). We must have in mind however the impossibility of predefining any thinkable policy harmonization, e.g. in open care settings and personalized health, as some of the policies to be applied are not known at that time. Furthermore and even more relevant, the consideration of any thinkable policy would make the system too complex, and therefore undefined and not computable. In consequence, we should only consider policies relevant for the corresponding business case. If the harmonization of business case related policies cannot be performed in advance, it has to be performed at run time, using decision intelligence systems for security and privacy services, especially for a specific privilege management. Dynamic policy harmonization can be performed by a system-theoretical, architecture-centric, ontology-based, policy-driven approach.

Figure 3 shows the policy-driven RBAC schema, which is provided by ISO 22600 [6].

In this schema, the principal is the user who wants to access a resource (an information object as target or a service). The structural role is the role assigned to the user by the organization, such as head physician, medical doctor, nurse, etc., but also specific qualifications or competences. The structural roles policy represents the relationships within the organization and is quite static. The process policy is the set of rules that control the business process. In the healthcare context, a process policy can be established through clinic guidelines or best practice guidelines. The functional role is the role that the user has related to the process, which is connected to the actions he/she can perform on resources in a certain process act, e.g. ordering an observation, justifying a statement by signature, or prescribing a medication, so becoming a requester, signer, prescriber. In the business case described, the target policy is strongly influenced by the fact that information objects are clinic information stored in the EHR. Thanks to its flexibility, this model is able to formally represent all the other access control models. This means that in the context of an inter-organizational collaboration all the policies can be formalized and then harmonized without touching them. So, cross-organizational interoperability can be provided irrespective of the access control level and the underlying access control model of the single organization. The model in Figure 3 can be extended by top level policies any business is bound to such as legislation, ethical rules, etc. In order to harmonize policies, it is necessary to obtain a consistent formalization of the policies themselves.

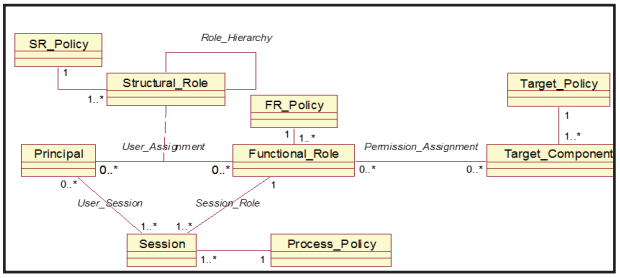

Figure 3: Policy-driven RBAC schema [6].

Following the policies, rules can be applied to assign privileges to actors or to roles played by actors. While the first case allows binding static policies to individual actors, the second enables an easier manageable rather coarse-grained binding of policies to roles, which in the worst case are structural roles and therefore static. When considering functional (predefined) roles, the business process defines the roles and privileges assignment to an entity. As an outcome, we implement statically Access Control Lists (ACLs), Mandatory Access Control (MAC), Discretionary Access Control (DAC), or Role Based Access Control (RBAC).

HL7 provides a special policy-driven solution for managing security and privacy in a business case and an individual context, and for deciding on that basic on privileges at runtime. Within the US national project of data segmentation for advancing communication and cooperation between healthcare establishments, HL7 has specified the HL7 Healthcare Privacy and Security Classification System (HCS) – Release 1 [11]. This specification defines security labels as markers bound to a resource, which connect an information object, but also process steps or actions, to a set of security and privacy attributes. This solution has already been demonstrated at different HIMSS events [5, 12].

The HL7 Healthcare Privacy and Security Classification System consists of two parts:

- A context-sensitive segmentation of health information;
- Security and privacy labeling of data segments, enabling machine processing of privilege management and access control.

In HCS specification, security labels are defined as meta-data bound to resources that transmit constraints on the use of the resources. Security labels are applied based on risk assessment of harm resulting from unauthorized disclosure. "This assessment may reflect personal perceptions or legal requirements, which may involve inherently emotional characterization of clinical information as prejudicial to a party's "interests" when exposed in unauthorized ways or to those who lack authority and responsibility for its care and use" [11]. With the implicit knowledge stored in security labels as "mini policy", privilege management and access control decisions can be performed without accessing the target information. The label refers to the explicit policy stored in a policy repository to be accessed when needed for interpretation as explained in some more detail as follows.

NIST FIPS PUB 188 specification defines a security label as a set of specified fields. Each field consists of globally unique Tag Set Name and a set of semantically interoperable security tag or field values. These labels define the classification of each item. HL7 HCS specifies a Security Classification Tag Set (Confidentiality), a Security Categorization Tag Set (Sensitivity, Integrity, Compartment, Privacy Law), and Handling Caveat Tag Set (Purpose of Use, Obligations, Refrain Policies). In the following, the label fields will be introduced in some details [13]:

- Confidentiality: classifies an IT resource (clinical fact, data, information object, service, or system capability) according to its level of sensitivity, which is based on an analysis of applicable privacy policies and the risk of financial, reputational, or other harm to an individual that could result from unauthorized disclosure;
- Sensitivity: categorizes the value, importance and vulnerability of an IT resource perceived as undesirable to share;
- Integrity: conveys the completeness, veracity, reliability, trustworthiness and provenance of an IT resource;
- Compartment: "segments" an IT resource by indicating that access and use is restricted to members of a defined community or project. An example for compartment labels is "for pharmacy only";
- Privacy Law: refers to the corresponding legislation;
- Handling Caveat: conveys dissemination controls and information handling caveats, such as constraining the purpose of use, defining concrete refrain policies and obligations to which an IT resource custodian or receiver must comply.

Confidentiality, Sensitivity, Integrity and Compartment fields characterize security and privacy rules ("mini policies") for specific health information. Instead, handling caveat fields are characteristics of activities, such as processes of using that information. The valid security labels and how they have to be compared with the users' clearances have to be expressed as explicit policies specified in the Security Policy Information Files (SPIF). The SPIF are usually XML based [5].

The newest project established at HL7 for privilege management and access control is the draft specification "Privacy and Security Architecture Framework – Trust Framework for Federated Authorization, Release 1. Being more consistent with the prosed methodology than older specifications, also this model can be represented and harmonized with others following the presented approach [14].

For managing and harmonizing the different privilege management and access control models, Figure 3 is used as Reference Architecture Model of the privilege management and access control system. For that purpose, all those models have to be architecturally represented in that schema.

All the different policies provided by the different solutions presented have to be considered for the specific privilege assignment and access control decisions. For concluding on all those policies, the concepts have to be provided at a level of expressivity and formalization allowing that all concepts established by domain experts or laymen from different domains in different context with different education, experiences and skills can be appropriately and consistently taken into consideration. For that purpose, the concepts of the policy domain have been ordered and interrelated in the policy domain ontology as described in ISO 22600 [6]. Additionally to the definition of the base classes of that ontology and their structural relations, the latter must be quantified using a proper logic representation. The knowledge (concept) processing in the decision making process is based on an ontology harmonization process. An extended study of relevant tools to perform this task is underway as well.

More details related to access control models and their policies formalization will be presented in [15].

For implementing the policy decision process, existing standards and related services can be used as shortly discussed in the following.

Within the scope of the HCS and its use in an access control system, there are two principal services: the Security Labeling Service (SLS) and the Privacy and Protective Services (PPS) [16]. The SLS evaluates the submitted clinical information objects, including clinical tagging and provenance, to determine the appropriate security labels to assign to information objects for access control based on rules. Access Decision Services can then use the labeled clinical objects as classified resource Access Control Decision Information (ADI) to check clearances. Access decision policy can be dynamic, particularly in the case of patient preferences. For this reason, labels should be applied at runtime, rather than being permanently stored with information objects. In this way, classified resource ADI could be current with the most current policy. The SLS is supported by a Security Label Management System. The latter establishes, provisions, and manages the security tagging vocabularies and security labeling rules needed to support jurisdictional, organizational privacy and security policies, including patient consent directives. Once an access control decision is made, also obligations should be met before releasing the resources. Then, the Policy Decision Point (PDP) decision and obligations are provided to a Policy

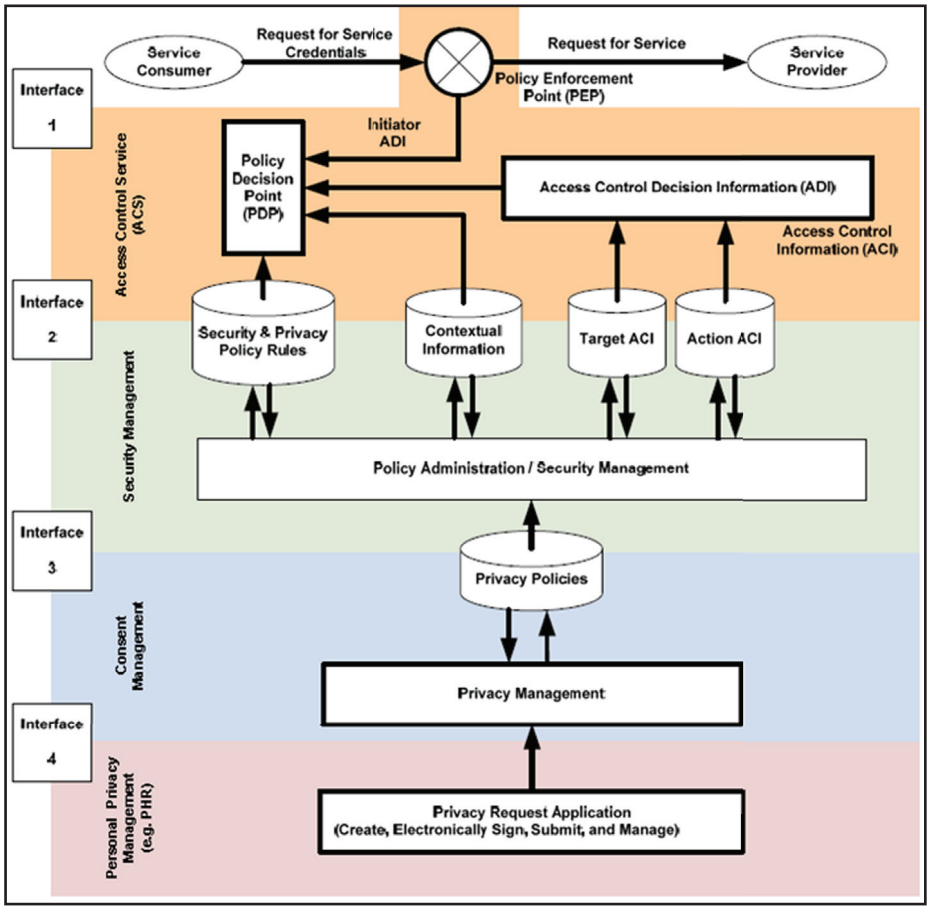

Figure 4: Authorization Reference Model [18].

Enforcement Point (PEP), which tasks appropriate obligation services, such as PPS, to impose the obligations. Basing upon rules, the PPS can apply various transforms to the security labeled resources: masking, redaction, shedding, shifting, annotations, anonymization, pseudo-anonymization, etc. The PPS is supported by its own Protective Services Management Sub-System, which establishes the type of transformations to be applied based upon rules. The latter can be determined in advance or dynamically at runtime. The transformed resource is finally sent to the recipient [5].

Once users' clearances, resources security labels and SPIF are defined, privilege and access control management in health information systems can be automated [5].

For implementing the aforementioned advanced service, the HL7 Implementation Guide: Data Segmentation for Privacy (DS4P) as well as HL7 Version 3 Standard: Privacy, Access and Security Services; Security Labeling Service [16, 17] have been specified. This Implementation Guide, including the value definitions and references, must be localized for the Italian environment. Figure 4 presents the Access Control logical architecture model [18].

4 Deployment of the Developed Methodology

The aforementioned privilege management and access control models refer to predefined policies in their informational representation. As the informational representation is usually defined by informaticians, the consistency with real world policies cannot be guaranteed. The solution offered by the paper is overcoming those limitations by:

- The definition of all policies relevant for a specific business case using the domain specific terminologies;
- The formal representation of those policies using the domain specific ontologies;
- The harmonization of real world policies at runtime.

Then, it is intuitive that static and rigid policies are not suitable. Instead, policies coming from different domains have to be mapped dynamically and in an adaptive and automated way. In order to allow this, it is essential to provide a formal description of the policies that can be used by the authorization services to obtain the security and privacy rules to apply to the resources [19]. Furthermore, the environment conditions have to be evaluated in the same moment in which the user makes the access request. To implement an access control

- To service functionalities: it is necessary to make a functional description of the service, specifying security and privacy minimum requirements for each functionality through security labels, or at the next level by dynamically representing the related explicit policy;
- To the resources: the resources have to be classified through security labels, or at the next level by dynamically representing the related explicit policy.

Through the description of the security and privacy labels (or the explicit policies) of processes and resources, the authorization service is able to obtain the policy to be applied and to check the resulting constraints at runtime. As mentioned above, the policies that have to be mapped come from different domains. So, policies must be formally expressed for allowing their integration in advanced e-health environments. Since different expression means will be used to formally modelling policies, measures and tools for expressing and mapping them have to be developed. Interoperability between different domains requires ontology management by harmonizing common ontology domains' sub-ontologies (e.g. harmonizing concepts of medical sub-ontologies such as SNOMED and LOINC) or by linking different domains' ontologies (e.g. linking policy and medical concepts or linking legal policy and medical policy). Harmonizing ontologies can be performed a-priori by merging, aligning, integrating, or at runtime by matching or mapping. Matching addresses the management of equivalent concepts, while mapping addresses the management of similar concepts. As ontologies are used to represent architectural components of the Generic Component Model (GCM) at appropriate level of generalization/specialization, the GCM process principles also apply to the ontology management (e.g., only interrelating concepts at the same level of granularity).

5 Discussion

In this paper, the authors offer a solution for policy harmonization for privilege management and access control in healthcare context to be implemented using HL7 specifications. Personal health information and related process information will be managed using the Italian Fascicolo Sanitario Elettronico (FSE). The FSE is a regional EHR approach to collect clinical data and documents produced by present or past clinical events and constitutes the patient clinical history. The FSE can be accessed through the Internet with appropriate security and privacy measures in place. The patient can have access to his/her FSE through personal credentials or a smartcard [20].

In order to guarantee adequate privilege management and access control, it is necessary to identify the subjects who request to access to the resources. For this reason, the solution must include an authentication service. The authors focused on authorization services, supposing that an adequate system for identification and authentication already exists. This

assumption is justified by the current Italian governmental effort to set up a national identity system called Sistema Pubblico di Identità Digitale (SPID), Public System of Digital Identity [21]. As its name suggests, the SPID is a national service that provides a digital identity for Italian citizens. The latter are identified through the fiscal code (Codice Fiscale), which is an alphanumeric code of sixteen characters that is associated to Italian individuals at birth and to foreigners when having contacts with Italian institutions. The fiscal code depends on the subject's name, surname, sex, place and date of birth and is unique and tailored for the person. Up to now, the SPID supplies two levels of authentication [22]. At the first level, one factor authentication is provided by a password. At the second level, two factor authentication is provided by a password and a One Time Password. During 2017, a more secure two factor authentication, provided through a password and a physical medium (such as a smart card) should be available for first services. Efforts similar to the SPID are also performed in other European countries with the opportunity of cross-border use, see the Electronic identification and electronic Trust Services (eIDAS) regulation [23, 24]. However, a strong and secure three factor authentication is fundamental for activities as awkward as healthcare.

In Italy, healthcare organizations have different access control models: in some organizations access control is static, rigid and strongly hierarchy dependent (MAC); in others authorized subjects can delegate permissions to other users (DAC); in rare cases, it is possible to find a role based privilege management (RBAC). All of these solutions have been the result of past investments of money and in many cases organizations have not the possibility to make progress towards more advanced access control. The methodology provided by the authors enables at run time the harmonization of all the policies irrespective of the access control model used in the organizations. This offers the opportunity to consider also patient policies, which are strongly dynamic, that way enabling the move from an organization-centered care to a patient-centered care. In addition, since all the access control models can be formally represented with the schema in Figure 3, the methodology does not hamper organizations progressing to more advanced privilege management and access control solutions. These are the advantages of the authors' approach over other solutions that enable harmonization only by static pre-coordination or even require the use of identical or at least equivalent solutions. As a consequence of such pre-coordination, only organizations with the stated access control model can join the intra-organizational collaboration. In addition, since policies are not harmonized at run time, a predefined solution can fit only organization centered healthcare.

6 Conclusion

The authors provide a methodology to enable policies harmonization in EHR systems by deploying a system-theoretical, architecture-centric, ontology-based, policy-driven approach, which:

- Is irrespective of the maturity of organizations privilege management and access control system;
- Does not hamper organizations progressing to more advanced privilege management and access control system over the time;
- Accepts also dynamic policies;
- Allows to advance towards a patient-centered care;
- Is implementation-independent.

References

[1] http://www.airc.it/cancro/cos-e/statistiche-tumori-italia

[2] http://www.airc.it/tumori/tumore-al-seno.asp

[3] Blobel B. Security and privacy services in pathology for enabling trustworthy personal health. Stud Health Technol Inform. 2012; 179: 203-217.

[4] Blobel B, Koeppe D. Handbook of Data Protection and Data Security in Health and Social Care, 4th ed. Frechen: Datakontext – Fachverlag; 2016 (in German).

[5] Blobel B, Davis M, Ruotsalainen P. Policy management standards enabling trustworthy pHealth. Stud Health Technol Inform. 2014; 200: 8-21.

[6] International Organization for Standardization. ISO 22600 Health informatics – Privilege management and access control. Geneva: ISO; 2014.

[7] Blobel B, Ruotsalainen P, Lopez DM, Oemig F. Requirements and Solutions for Personalized Health Systems. Stud Health Technol Inform. 2017; 237: 3-21.

[8] Gruber TR. Toward principles for the design of ontologies used for knowledge sharing. Int J Human – Computer Studies. 1995; 43: 907-928.

[9] Blobel B. Knowledge Representation and Management Enabling Intelligent Interoperability – Principles and Standard. Stud Health Technol Inform. 2013; 186: 3-21.

[10] Blanco C, Lasheras J, Valencia-García R, Fernández-Medina E, Toval A, Piattini M. A Systematic Review and Comparison of Security Ontologies. Proceedings of The Third International Conference on Availability, Reliability and Security. Barcelona, Spain, 4-7 March 2008.

[11] HL7 International Inc. HL7 Informative Guidance: Guide to the HL7 Healthcare Privacy and Security Classification System (HCS). Ann Arbor: HL7 International; May 2013.

[12] Data Segmentation for Privacy VA/SAMSA RI/ Pilot at HIMSS 2013: http://wiki.siframework.org/ Data+Segmentation+for+Privacy+Homepage.

[13] HL7 International Inc. HL7 Healthcare Privacy and Security Classification System (HCS) – Release 1. Ann Arbor: HL7 International; May 2013.

[14] HL7 International Inc. HL7 Version 3 Standard: Privacy and Security Architecture Framework – Trust Framework

for Federated Authorization, Release 1. Ann Arbor: HL7 International; January 2017.

[15] Gazzarata G, Blobel B, Giacomini M. A system-oriented, policy-driven approach to harmonize existing privilege management and access control models. In preparation.

[16] HL7 International Inc. HL7 Version 3 Standard : Privacy, Access and Security Services; Security Labeling Service, Release 1. Ann Arbor: HL7 International; January 2014.

[17] HL7 International Inc. HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1. Ann Arbor: HL7 International; September 2013.

[18] HL7 International Inc. HL7 Version 3 Standard: Privacy, Access and Security Services (PASS) – Access Control Services Conceptual Model, Release 1. Ann Arbor: HL7 International; September 2015.

[19] Blobel B. Ontology driven health information systems architectures enable pHealth for empowered patients. Int J Med Inform. 2011; 80: e17-e25.

[20] Fascicolo Sanitario Elettronico (FSE): http://support.fascicolo-sanitario.it/faq

[21] SPID (Sistema Pubblico di Identità Digitale): https://www.spid.gov.it/.

[22] SPID (Sistema Pubblico di Identità Digitale): http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/spid/percorso-attuazione.

[23] Trust Services and eIdentification: https://ec.europa.eu/digital-single-market/en/policies/trust-services-and-eidentification.

[24] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG