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

doi:10.3233/978-1-61499-432-9-463

Policy-Driven Management of Personal Health Information for Enhancing Interoperability

Bernd BLOBEL[a,b,1], Pekka RUOTSALAINEN[c], Carolina GONZÁLEZ[b,d], Diego LÓPEZ[b,e]
[a]*Medical Faculty, University of Regensburg, Germany*
[b]*eHealth Competence Center Bavaria, Deggendorf Institute of Technology, Germany*
[c]*University of Tampere, Finland*
[d]*Computational Intelligence Research Group, University of Cauca, Colombia*
[e]*Telematics Engineering Research Group, University of Cauca, Colombia*

Abstract. Based on a system-theoretical approach, aspects of real world systems have been introduced. In this context, the relations between a system's architecture, i.e. its components, their functions and relations, formally represented by domain-specific ontologies considering all domains relevant in the system's use case on the one hand and the system's behaviour ruled by the applied policies on the other hand have been described. A refinement of policies ruling a clinical setting has been exemplified. It could be shown that ubiquitous health systems must be designed and managed following a thoroughly systems-oriented, architecture-centric, ontology-based and policy-driven approach. The feasibility of the approach has been practically demonstrated.

Keywords. Ubiquitous health, system architecture, system behaviour, policy, Generic Component Model

Introduction

Health and social systems around the globe are on the move towards personalized and ubiquitous health, which includes prevention, predictive, proactive care as well as lifestyle and wellbeing. The aforementioned paradigm shift requires a multi-disciplinary, integrative approach, combined with the challenge to manage the resulting complexity and methodological diversity of the resulting eco-system on a trustworthy basis [1]. On the one hand, many different specialties represented by experts using their own terminology based on domain-specific ontologies must be mapped. This requires a formal representation of the domain structure and function as well as underlying natural rules and relationships between the domain elements in consideration. On the other hand, many different and sovereign stakeholders bound to different regulations and representing different interests must cooperate in an efficient, safe and quality-assured way to benefit citizens and patients, health organizations and the society. Also

[1] Corresponding Author. Bernd Blobel, PhD, FACMI, FACHI, FHL7, Professor; University of Regensburg, Medical Faculty, Regensburg, Bavaria, Germany; Email: bernd.blobel@klinik.uni-regensburg.de; URL: www.ehealth-cc.de

those actors' knowledge and skills, impacted by experiences and culture, must be explicitly and formally represented. To meet all those challenges, the ubiquitous health approach has to be as detailed and as general as needed, reducing the complexity on the necessary level for a specific business case/use case, providing any functional flexibility through re-usability of the systems components by appropriate system aggregation and management. Only the formal, abstract, flexible and extendable methodology of system theory meets the aforementioned requirements [2].

1. Methods

A system is a (frequently ordered) composition of interrelated elements. Possible system categories are: System, Element, Structure, and Function [3]. The architecture of a natural system in the sense of a system's structural and functional aspects, i.e., its components, their functions (operations) and possible interrelations including the underlying rules controlling that system and its survival are frequently defined and represented through the ontologies of the domains the system covers. In contrast, humanly designed or managed systems realize intended structures und functions regarding the constituents as well as their interrelations by selecting components as well as constraining their operations and relations administratively and so ruling the behavioral aspect of a system by humans. Sloman has named "rules governing the choices in behavior of a system" a policy [4]. Another policy definition was provided in Bell Labs' Policy Description Language as "collection of general principles specifying the desired behavior of a system" [5]. In ISO 22600, policies have been defined as "set of legal, political, organisational, functional and technical obligations for communication and cooperation" [6]. According to Damianou et al., policies "are often used as a means of implementing flexible and adaptive systems for management of internet services, distributed systems, and security systems" [7]. Boutaba and Aib described policy-based management of systems as being in the "heart of a multitude of management architectures and paradigms including SLA-driven, business-driven, autonomous, adaptive, and self-management". It "separates the rules governing the behavior of a system from its functionality" [8]. "Policies define choices in behavior in terms of the conditions under which predefined operations or actions can be invoked rather than changing the functionality of the actual operations themselves" [7]. In summary, the rules defined for system components and relations according to their ontologies are amended by policies defined according to the business process. It has to be mentioned however that the leeway of humanly administering systems has been continuously widened in the humans' history, also intervening in natural processes.

A meanwhile widely used approach to semi-formally represent systems is the Generic Component Model, as it allows modeling their structure, functions and interrelations, at the same time also enabling the separate representation and management of aspects of that system. Ways to present the GCM formally are given in [9]. In the GCM, the structural and functional aspects of different perspectives on the system are represented by subject-specific GCM domains. The behavioral aspect of that system, i.e., the relations and constraints according to business process, contextual and environmental conditions are summarized in policy domains (see Figure 1a). Following, this approach will be demonstrated for policy-driven design and management [10] of health systems, also such complex ones like ubiquitous health systems.

2. Modeling Policy-Driven Systems

According to good modeling practice and the design principles of the GCM, systems can be decomposed into subsystems, as domains can be refined into subdomains. Ignoring medical subdomains such as clinical care, primary care, or home care, the representation of a clinical care system used by different resources is presented in Figure 1a.

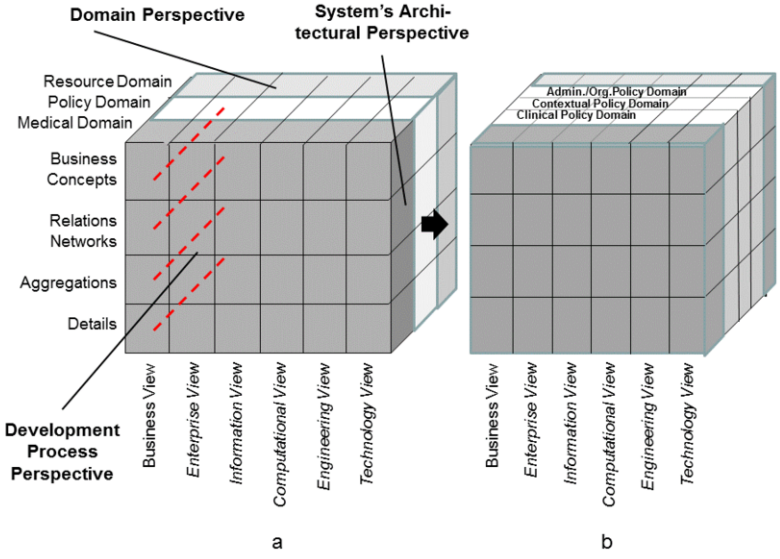

Figure 1. a) GCM representation of a policy-driven system, b) Refinement of the policy domain

Policies can be defined for managing resources, for managing the clinical process (e.g. by Best Practice Clinical Guidelines), but also to rule the relations between resources and targets legally, regulatory and ethically, summarized as context. In Figure 1b, the system presented in Figure 1a has been refined accordingly.

The separately analyzed different system elements (components) aggregated in one domain and represented based on the domain's ontology as well as the different aspects of the system established through the different domains to be considered, must be integrated, by that way realizing the business process. The GCM principles allow only relations at the same level of granularity. Interrelated ontologies are harmonized using their top level ontology. Others are managed as process steps or control the business process. The different aforementioned policies must be harmonized at the corresponding granularity level to define the final behavior of the system. Policy harmonization includes matching, mapping, alignment, and merging [11]. While the first two mechanisms are used at runtime, the others must be performed a priori.

The policy representation works best when using the policy ontology defined in ISO 22600 and deployed in a series of HL7 specifications such as the HL7 Security and Privacy Domain Analysis Model [12], the HL7 Healthcare Classification System [13], the HL7 Security Labeling Services specification [14] or the HL7 Patient Consent spec [15]. Base classes of that policy ontology are BasicPolicy, specialized into AuthorizationPolicy, RefrainPolicy, ObligationPolicy, and DelegationPolicy. For creating policies and for harmonizing policies, a MetaPolicy and a CompositePolicy

have been defined, respectively. When constraining the consideration on implementable ICT solutions instead of covering the entirety of the real world of human cooperation, XCAML, a policy language based on the SOA ontology can be practically deployed [16].

The practicality of the approach has been demonstrated, e.g., at HIMSS 2013, where more than 50 vendors' solutions have provided intelligent policy-based interoperability in real clinical settings [17] using the HL7 Security Labeling Services specification [14]. Those services are based on the HL7 Healthcare Classification System [13], which has defined security labels and related vocabularies for binding them to objects or constraining processes. In detail, following security labels have been specified: Confidentiality, Sensitivity, Integrity, Compartment to characterize security and privacy rules for specific information objects and Handling Caveats for constraining activities, i.e. processes of using information objects. Confidentiality labels are used to classify an information object 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 labels categorize the value, importance, and vulnerability of an information object perceived as undesirable to share. Integrity labels convey the completeness, veracity, reliability, trustworthiness, and provenance of an information object. Compartment labels indicate that access and use is restricted to members of a defined community or project. Handling caveat labels convey dissemination controls and information handling caveats such as obligations and refrain policies to which an IT resource custodian or receiver must comply. Confidentiality and Handling Caveats labels are part of the Clinical Policy Domain. Sensitivity and Integrity labels belong to the Contextual Policy Domain, while Compartment labels refer to the Admin/Org Policy Domain. When resolving the selections and constraints regarding the resources, objects and processes according to the defined policies, the architectural schema of Figure 1b has to be reflected.

That way security attributes and coarse-grained privacy policies are used for access control decisions and their enforcement. The labels refer to policies ruling in detail how to perform in the business case for meeting the security and privacy requirements. A detailed description of both HL7 specifications will be published in [18]. One weakness of existing implementations to be overcome is the involvement of citizens/patients regarding appropriate trust models, transparency and understandability of policies, as discussed in more detail in [19].

3. Discussion and Conclusion

Ubiquitous health systems can be best formally and abstractly modelled by the deployment of a system-theoretical approach. Thereby, the different aspects of systems have been highlighted. A system's architecture describes the systems elements (components), their functions and interrelations. The representation of aspects (domains) of real world systems has to be based on the corresponding domain ontologies. Rules for selecting components and functions as well as constraints of the relations according to a business case are called policies. Policies define the intended behavior of systems.

Therefore, flexible, scalable, business-controlled, adaptive, knowledge-based, intelligent ubiquitous health systems must follow a systems-oriented, architecture-centric, ontology-based and policy-driven approach.

Acknowledgment

The authors are indebted to thank their friends and colleagues at HL7 International, ISO TC 215 "Health informatics", CEN TC 251 "Health informatics" and IHTSDO for the excellent cooperation and support. Special thanks are dedicated to Mike Davis, U.S. Department of Veterans Affairs, San Diego, John Moerke, General Electric Company, Menomonee Falls, Ioana Singureanu, Eversolve LLC, Windham, and Kathleen Corner, U.S. Department of Veterans Affairs, San Diego.

References

[1] Blobel B. Translational Medicine Meets New Technologies for Enabling Personalized Care. Stud Health Technol Inform 2013; 189:8-23.
[2] Blobel B. Architectural approach to eHealth for enabling paradigm changes in health. Methods Inf Med 2010; 49,2:123-134.
[3] Völz H. Information. Berlin: Akademie-Verlag; 1982.
[4] Sloman, MS. Policy Driven Management for Distributed Systems. Journal of Network and Systems Management 1994; 2(4):333-360.
[5] Lobo J, Bhatia R, and Naqvi S. A policy description language. In AAAI '99/IAAI '99: Proceedings of the 16th National Conference on Artificial Intelligence and the 11th Conference on Innovative Applications of Artificial Intelligence, p. 291-298. American Association for Artificial Intelligence: Menlo Park, CA, USA; 1999.
[6] International Organization for Standardization. ISO 22600 Health informatics – Privilege management and access control. Geneva: ISO; 2006.
[7] Damianou NC, Bandara AK, Sloman MS, Lupu EC. A Survey of Policy Specification Approaches. CiteSeerxβ, 2002 – available at www.doc.ic.ac.uk.
[8] Boutaba R and Aib I. Policy-Based Management: A Historical perspective. J Netw Syst Manage 2007; 15;447-480.
[9] Blobel B, Pharow P. Analysis and Evaluation of EHR Approaches. Methods Inf Med 2009; 48,2:162-169.
[10] Blobel B, Nordberg R, Davis JM, Pharow P. Modelling privilege management and access control. Int J Med Inform 2006; 75(8):597-623.
[11] M. Rebstock, J. Fengel, H. Paulheim. Ontologies-Based Business Integration. Berlin: Springer; 2008.
[12] HL7 International Inc. HL7 V3 DAM: Composite Security and Privacy – Release 1. Ann Arbor: HL7 International; May 2014.
[13] HL7 International Inc. HL7 Healthcare Privacy and Security Classification System (HCS) – Release 3. Ann Arbor: HL7 International; May 2013.
[14] HL7 International Inc. HL7 Version 3 Standard: Privacy, Access and Security Services; Security Labeling Service, Release 1. Ann Arbor: HL7 International; January 2014.
[15] Health Level 7 International, Inc., Ann Arbor, USA. www.hl7.org
[16] Blobel B. Ontology driven health information systems architectures enable pHealth for empowered patients. Int J Med Inform 2011; 80(2):e17-e25.
[17] Data Segmentation for Privacy VA/SAMHSA RI/Pilot at HIMSS 2013. http://wiki.siframework.org/Data+Segmentation+for+Privacy+Homepage
[18] Blobel B, Davis MJ, Ruotsalainen P. Policy Management Standards Enabling Trustworthy pHealth. Stud Health Technol Inform 2014; 200 (in print).
[19] Routsalainen P and Blobel B. Trust Information and Privacy Policies – enablers for pHealth and Ubiquitous Health. Stud Health Technol Inform 2014; 200 (in print).