E-HEALTH WORKFLOW-BASED AUTHORIZATION USING AN AGENT-ORIENTED VIRTUAL HEALTH CARE RECORD

Keywords: ehealth, agents, authorization, RBAC

Abstract: In this article a proposal to an integrated e-Health solution based on the Patient Electronic Health Record is presented. The main point is how the caregivers' role that is obtained from authentification and authorization process is enforced in a cross-organizational care workflow using multi agent systems. Interoperability between healthcare organizations and provisioning of permission for accessing the medical record are also addressed using mediation and negotiation software agents. We envision the healthcare system as an open digital ecosystem, where multi-agent systems are organized in organizations.

1 INTRODUCTION

E-Health is today a major research theme in the academic community but also a starting point for many families of commercial products. Among other aspects, e-health can change the way healthcare providers cooperate, it can improve the quality of disease diagnostics, can lower the costs for treatment of terminal and chronic diseases. Some of the areas for research in e-Health are:

- Home Care
- Pre-Hospital Emergency Care
- Hospital Care
- Health Monitoring and Surveillance

(Villar et al., 2008). In the following we describe our vision for an e-Health integrated solution based on the Virtual HealthCare Record (VHCR), an internet entity that communicates with the EHR and other systems of caregivers in order to capture and integrate relevant information on healthcare events occurred during the life of patients. (Serbanati and Vasilateanu, 2008). It is built to support a broad range of current healthcare processes while being flexible enough to work with improvements and developments in best practice. Our solution is founded on the assumption that a healthcare system is similar to a business enterprise having its own business processes that are complex activities undertaken and directed to prevent, treat, and manage of illness, and preserve of mental and physical well-being through specific services. Actually information systems are widely used to support business processes in healthcare as they do in an enterprise (Serbanati et al., 2005). This is why our approach embodies lessons learned from solutions for enterprise integration (Luzi et al., 2006) and virtual enterprise. VHCR realizes a longitudinal record, spanning over the whole life of the patient, integrating distributed and heterogeneous sources of information. We model VHCR as a multiagent system (Huhns and Stephens, 2008) following an organizational approach, where avatars of caregivers and the patient are composed of agents that cooperate to maintain a complete and authoritative virtual representation of the patient's health state and clinical history. The benefits of e-Health solutions depend on their adoption rate, both by healthcare providers and patients. The main obstacles in wide acceptance are, in our opinion, interoperability and security issues. In this paper we focus on the security aspects of our solution, namely the caregiver authorization and role provisioning in complex, cross-organizational care process workflows.

The paper organization is the following: first the VHCR concept is presented with its two main parts - the care record and the agency, then the authoriza-

tion and authentification processes, based on the e-consent principle derived from the care process workflow are detailed. Finally the VHCR's possible integration with the existing LUMIR project is presented as well as an overview of similar initiatives and future improvements.

2 INTRODUCING VIRTUAL HEALTH CARE RECORD

At the center of our solution lies the Virtual Health Care Record (VHCR). VHCR is not a simple repository; but a complex e-service provider for supporting healthcare processes. VHCR has to deal with two major functionalities: 1) maintaining the coherency and consistence of information in the VHCR in order to provide in any moment both an accurate and coherent "snapshot" of the patient's current health status as well as the history of her/his clinical events, and 2) providing services for message exchange with other applications. VHCR cohesion is accomplished by a dedicated ontology, derived from HL7 RIM v3, developed to have a consistent view on health services, healthcare provider roles and process execution language.

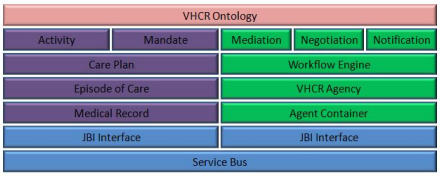


Figure 1: VHCR Architecture

The services are implemented using an agent-oriented approach; the community of agents contained in VHCR is called VHCR Agency. Analyzing the functionalities and deriving the agent roles from the roles of external systems that interact with the VHCR and the internal tasks the VHCR should carry out, we designed agents that:

- interact with the caregivers
- interact with the medical devices
- monitor the status of the patient's health as reflected in his record and issue notifications
- supervise the realization of the clinical workflow
- act as mediators between organizations
- negotiate permissions

3 VHCR AS AN ORGANIZATION OF SOFTWARE AGENTS

To design and implement such a complex system involving interraction between parties with different objectives, a multi-agent approach was seen as the optimal choice as it minimalizes the semantic gap between the analysis used to conceptualize the problem and the implementation of the actual system. (Jennings, 1999) As stated in (Wooldridge, 1997)

> an agent is an encapsulated computer system that is situated in some environment, and that is capable of flexible, autonomous action in that environment in order to meet its design objectives

In our view, the envriroment in which the agents function is the complex digital health ecosystem populated with interested parties organized in agencies, national and international regulations, business processes and models and contractual framework. An agent of the VHCR has the ability to interact in this complex envriroment, to communicate with other digital components, to enter contextual alliances and to participate in business processes.

Moreover we envision our digital ecosystem as an open system where agents can enter, live or become extinct. Since direct control or internal modifications or visualization of the agents in this open system is impossible we must provide a superior abstraction, that of agent organization. The organization provides organizational structures and also organizational rules which express global requirements for the execution of multi-agent systems. The rules can control the actions performed in a MAS defining which agents are permitted, obligated and prohibited to exectute those actions. To interract with VHCR, an external agent must assume a role in the organization, mapped to the stakeholder it is representing (Patient, Doctor, Health Researcher etc.) and be subject to the regulations of this virtual world. (Zambonelli et al., 2001)

4 CARE RECORD

VHCR functions as a longitudinal record: the record of a citizen keeps track on the progress of the patient along a lifelong period of time. Healthcare is seen as a life-long process composed from episodes of care and our solution supports elaborated, personalized health care workflows, denominated *care plans*. A care plan (see Fig. 2) is a healthcare service; a description of the planned care activities (drug administration, procedures, investigations etc). The care plan

is derived from a medical guideline, published in a national clearinghouse and available for download in a computer representation like Guideline Interchange Format(GLIF). Based on this template and on the patient‘s medical history (allergies, previous treatment response) the care provider creates a customized care plan and uploads it in the patient's medical record. Once the activities present in the care plan are performed, their completion is also added to the medical record, and the care plan execution is updated. If the execution of the planned activities varies from the medical guideline, this variance is also documented. In the case the care plan contains activities to be performed by different care providers (which is the case for chronic diseases in complex workflows), in different institutions, then it becomes a tool for cooperation and integration.

5 AGENT ASSISTED AUTHORIZATION

5.1 E-Consent in E-Health

The scenario described earlier raises many complexities from the point of view of privacy as it implies multi-role access to the patient‘s record. In a simple scenario it may involve a laboratory assistant to add a set of investigation results to the health record, supposing the investigations were a planned activity in the care plan. In a complex scenario, the patient can be sent for further investigation to another care provider, a specialist, who can change the diagnostic and/or the care plan activities in the health record. Can we mandate him that authority? The patient must give his/her “e-consent“ for access to his/her health record. The working definition for e-consent is *signification by recorded electronic means of concurrence or otherwise with an action to be taken by another party*. E-consent deals with authentification and authorization. E-consent in e-Health raises additional problems as we have to deal with two divergent requirements. The first is the degree of confidentiality involved in personal health records and, for a solution to be largely adopted, it needs to maintain this confidentiality. The second requirement is that of access to medical records in case of emergencies or when the patient is unable to give his/her e-consent and our solution must also obey this requirement.(Ruan and Yeo, 2009) Broader speaking, how does our system manage read/write permissions to the contents of the health record?

5.2 Introducing authentification and authorization in VHCR

The following quickly summarizes the main types of access control as well as the current foundation documentation in HL7 regarding security. Furthermore, by analyzing several complex healthcare processes we design our agent architecture introducing the following security-based agents in VHCR Agency:

- Mediator Agent, for inter-organizational interoperability, workflow mediation and role discovery
- Clinical Workflow Engine Agent, for directing and supervising the execution of the care workflow
- Permission Negotiator Agent, for negotiation permissions for non-default role permissions

5.3 Types of access control

The first issues we need to tackle in securing our system are authentification and authorization. Authentification is the act of verifying the identity of an entity. In our case this implies deciding between a centralized authentification protocol and a federated one. We choose the latter since authentification schemas and products are already deployed in legacy EHR systems which we want to cooperate with. By applying Security Assertion Markup Language (SAML) assertions our system can reuse the local authentification services and exchange data between security domains. Authorization, commonly referred as access control determines whether an identified user has access to the functionalities he/she is requesting.(Kanneganti and Chodavarapu, 2008) More access control techniques have been developed, ranging from discretionary as DAC (Discretionary Access Control) to non-discretionary as MAC (Mandatory Access Control) and RBAC (Role-Based Access Control). (Sandhu et al., 1996) Other models rely on Access Control Lists in which administrators associate a list of rules to each resource.

5.4 HL7 approach to security

HL7, an organization involved in the development of healthcare standards, adopts a role based access control model, consistent with OASIS eXtensible Access Control Markup Language(XACML) and ANSI INCITS RBAC in which a role definition consists of a name and a corresponding set of permissions. HL7 also defines a normative set of permissions, contained in the HL7 permission catalogue.

> Permission is an approval to perform an operation on one or more RBAC protected objects. An operation is an executable image of a program, which upon invocation executes some function for the user. An object is an entity that contains or receives information.

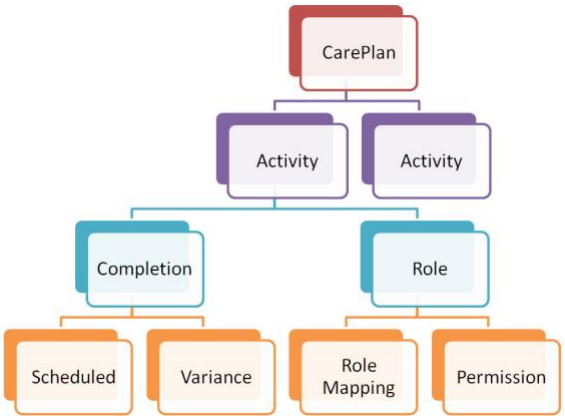


Figure 2: Care Plan used for Permission Enforcement

5.5 Organizational interoperability and role mapping

The main challenge we are faced with is that different healthcare institutions are organized in heterogeneous ways, usually opaque to the outside world. In order to be able to automate access control, based on a care plan workflow, we need roles acting as recipients of our permissions. Unfortunately these roles are not universal and even in HL 7 they are not standardized:

> Roles are not currently part of the HL7 permission catalog definition. At this time, roles are considered to be locally defined by organizations that build them using HL7 standard permissions.

A certain aspect to which we must pay atention is that institutions can implement the same norms differently as they use different ontologies to refer to the same concepts present in the norms. (Grossi et al., 2006)

In effect we need to achieve an organizational interoperability, by harmonizing the security policies of the healthcare institutions. Each institution will have an expert software agent, aware of the institution organization ontology and able to respond to queries regarding the specific domain knowledge.(Wooldridge, 2009)

Our agent in VHCR Agency, called Mediator Agent is tasked with querying the institution specific agents and mapping their ontology to ours, in order to translate the institution internal organization, extract the care provider roles and map them to our defined roles.

5.6 Workflow execution and permission negotiation

Once the care plan is uploaded in the medical record, its execution will be directed by the Clinical Workflow Engine Agent. To each active care plan a workflow agent is assigned, which monitors the realization of the care plan. The plan is divided in activities/tasks (Minsky, 1988) and the Workflow Agent advertises these tasks then acts as a manager, supervising its realization. For example it may advertise a notification activity before a scheduled procedure, to be undertaken by a Notification Agent. When deriving the care plan, the healthcare professional can mark which activity realizations are required to be acknowledged. For example it is critical for the patient to take a medication once a day. When the medication is taken the patient marks this fact on his PDA or in the patient portal and the event is sent to the VHCR where it is extracted by the workflow agent. The care plan is in fact modelled as a business process as described in (Leonardi et al., 2007)

In the following “continuity of care“ scenario, a patient must be administered a certain drug by intravenous injection on a regular basis. Since hospitalizing the patient is both expensive and unnecessary for his condition, a nurse comes to his house every week to provide him the medication. Acknowledging the administration is critical as the patient‘s health will degrade if the treatment is not followed. From this information the care provider designs the care plan which is uploaded to the medical record. The workflow agent analyzes the care plan and finds the predefined role “NURSE“ with the permission to acknowledge for drug administration. It must map this role to a real person, and to a certain episode of care and particular drug. The former must be done with input from the care provider or patient who inputs the ID of the particular nurse. In a more complex scenario the roles and permissions are not so clear cut and need to be mapped or negotiated as they involve an escalation of rights. Suppose the patient is sent to a specialist care provider for a routine check and this specialist operates in a large hospital with a complex organization. The workflow agent analyzes the care plan and then calls the mediator agent to map its predefined role “SPECIALIST“ to the actual role and id of the care provider in the organization of the institution. Next it assigns the default permissions for this role in the care

plan, to view the general health information as well as the information for this episode of care and to add an observation to the episode. However during the consultation, the specialist needs additional data and he/she must be allowed to consult information for different episodes of care, information he has not yet the permission to read. This demand is transferred to the software agent of the healthcare provider, responsible for interoperating with VHCR. In order to obtain the needed information the Provider Agent begins a dialogue with the VHCR Permission Negotiator. Each dialogue begins with a negotiation phase in which the Provider Agent requests the information. If the negotiation phase fails, the dialogue shifts to persuasion, where the requestor brings arguments in favour of his claim such as the potential negative impact on the diagnostic quality in case of a rejection or advertises the trust record of the healthcare provider. In its turn, the VHCR Negotiator has the goal to communicate only needed information, which will not affect the privacy of its owner. Particularly it will reason whether the claims of the opposite party are acceptable for the disclosure of confidential medical and social facts in the health record. To summarize, roles are engineered from care plans and they are mapped to the practitioners in a process of organizational interoperability. The roles provide only default permissions which can be escalated by means of negotiation.

6 PRESENT AND FUTURE IMPLEMENTATION AND DEPLOYMENT

VHCR started as a stand-alone, proof-of-concept prototype. To this date we have worked on extracting scenarios and work flows from current medical practice, national documents and regulations, published clinical pathways and also HL7 storyboards and functional requirements. We have also concentrated on designing a message ontology to support our agent-based communication. More recently we are tasked with integrating VHCR in a greater ehealth research project, namely LUMIR. LUMIR (LUcania - Medici In Rete), a project managed by the Institute for Biomedical Technologies, National Research Council in Italy, is a a region-wide infrastructure of web-services which interconnects at application level local healthcare applications (including EMRs), as well as regional healthcare information systems in use in the Basilicata Region. LUMIR has at its core an intelligent broker for routing messages. Our intention is to "plug in" VHCR in the existing Enterprise Service Bus (Rademakers and Dirksen, 2008), in order for it to reuse the existing services for security, authentification and notification (see Fig. 3). The architecture is Java Business Interface (JBI) compliant so in effect the container where VHCR agents reside will expose a JBI interface and will be deployed within the LUMIR framework. The agent messages will be wrapped in the existing messaging solution based on HTTP web services and the current public key infrastructure(PKI) based on Bouncy Castle Crypto API and Java Cryptographic Extensions (JCE). However, while this existing PKI allows us to gurantee message level security and authentification between the participants, it is not enough to authentificate individual agents within the container. In order to accomplish that we use the JADE Security Plug-in based on Java Authentication and Authorization Service. (jad, 2005) The other applications used by the healthcare providers(general practitioner, laboratory, hospital, pharmacy) connect to the esb by installing a wrapper that handles the tranformation, routing of messages and also authentification. This wrapper also holds a lightweight agent container in which the agents of the healthcare providers reside.

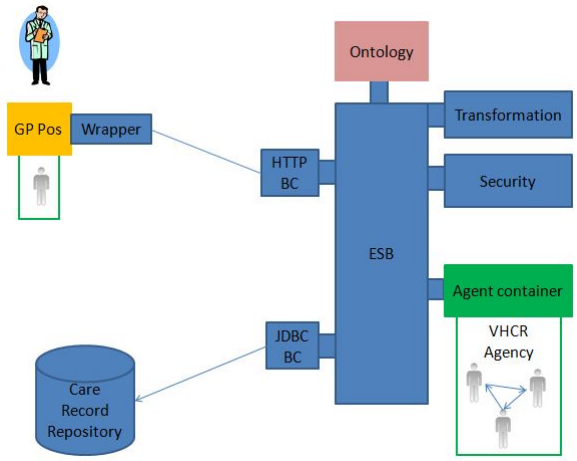


Figure 3: VHCR within LUMIR

7 CONCLUSION AND FURTHER IMPROVEMENTS

Using a multi-agent implementation for an open system involving the transport, storage and interpretation of sensitive medical data created the necessity to employ additional, superior abstractions to guarantee the privacy of the stakeholders. To construct these higher-level frameworks, we have used concepts from

Organizational Theory.

Work on VHCR is still in progress as we are analyzing different technology stacks and we are refining the message protocols based on healthcare ontologies. Also the seamless interoperability as process-level is being put under scrutiny to evaluate the extent at which it can be incorporated in a nation-wide deployment. The possibility of using an ebXML registry and repository is also evaluated.

8 RELATED WORK

Using agent-based solutions in e-health is not a novelty anymore and different research projects based on this paradigm have been completed or are underway (see (Leonardi et al., 2007), (Haigh et al., 2002), (Beer et al., 2003), (Nealon and Moreno,)). What the added value of the VHCR project compared to other initiatives and its research potential are, is comprised in the following:

- Hollistic approach: tackles all issues relating to e-Health: from security to interoperability and integration with medical devices and third party applications
- Realistic: developed starting from use cases and clinical pathways found in healthcare regulations
- Standards based: uses standardized messages derived from HL7 RIM v3
- Organizational view on multi agent interactions
- Institutional integration

REFERENCES

(2005). Jade security guide. `http://jade.tilab.com/doc/tutorials/`.

Beer, M., Hill, R., and Sixsmith, A. (2003). Deploying an agent-based architecture for the management of community care. In *Proceedings of the second international joint conference on Autonomous agents and multiagent systems*, page 933. ACM.

Grossi, D., Aldewereld, H., Vázquez-Salceda, J., and Dignum, F. (2006). Ontological aspects of the implementation of norms in agent-based electronic institutions. *Computational & Mathematical Organization Theory*, 12(2):251–275.

Haigh, K., Phelps, J., and Geib, C. (2002). An open agent architecture for assisting elder independence. In *Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 2*, page 586. ACM.

Huhns, M. and Stephens, L. (2008). 2 Multiagent Systems and Societies of Agents.

Jennings, N. (1999). Agent-oriented software engineering. *Multi-Agent System Engineering*, pages 1–7.

Kanneganti, R. and Chodavarapu, P. (2008). *Soa security*. Dreamtech Press.

Leonardi, G., Panzarasa, S., Quaglini, S., Stefanelli, M., and van der Aalst, W. (2007). Interacting agents through a web-based health serviceflow management system. *Journal of Biomedical Informatics*, 40(5):486–499.

Luzi, D., Ricci, F., and Serbanati, L. (2006). E-Clinical trials supported by a service-oriented architecture. *in MedNet*.

Minsky, M. (1988). *The society of mind*. Simon and Schuster.

Nealon, J. and Moreno, A. Agent-based health care systems.

Rademakers, T. and Dirksen, J. (2008). Open-source ESBs in action.

Ruan, C. and Yeo, S. (2009). Modeling of an Intelligent e-Consent System in a Healthcare Domain. *Journal of Universal Computer Science*, 15(12):2429–2444.

Sandhu, R., Coyne, E., Feinstein, H., and Youman, C. (1996). Role-based access control models. *Computer*, 29(2):38–47.

Serbanati, L., Ricci, R., Luzi, D., Fazi, P., Collada Ali, L., and Vignetti, M. (2005). Modelling medical research processes in humans to set up a standard for clinical trial management system. *Cunningham P. and Cunningham M. (Eds), Innovation and the Knowledge Economy: Issues, Applications, Case Studies*.

Serbanati, L. and Vasilateanu, A. (2008). Supporting Continuity of Care with a Virtual Electronic Health Record. pages 84–87. IHIC.

Villar, A., Federici, A., and Annicchiarico, R. (2008). Agents and Healthcare: A Glance to the Future. *Agent Technology and e-Health*, pages 141–148.

Wooldridge, M. (1997). Agent-based software engineering. *IEE Proceedings] Software Engineering. IEE Proceedings-[see also Software*, 144(1):26–37.

Wooldridge, M. (2009). *An introduction to multiagent systems*. Wiley.

Zambonelli, F., Jennings, N., and Wooldridge, M. (2001). Organisational abstractions for the analysis and design of multi-agent systems. In *Agent-Oriented Software Engineering*, pages 407–422. Springer.