Compliance Aware Cross-Organization Medical Record Sharing

Jovan Stevovic, Fabio Casati and Bilal Farraj
DISI - University of Trento,
Via Sommarive, 5, 38123,Trento, Italy
{stevovic, casati}@disi.unitn.it,
bilal.farraj@studenti.unitn.it

Jun Li and Hamid R. Motahari-Nezhad
Hewlett-Packard Laboratories
1501 Page Mill Road,
Palo Alto, CA 94304, USA
{jun.li, hamid.motahari}@hp.com

Giampaolo Armellin
CRG - Centro Ricerche GPI,
Via Ragazzi del '99, 13,
38123, Trento, Italy
giampaolo.armellin@cr-gpi.it

***Abstract* — Data sharing about Electronic Health Records (EHRs) across healthcare organizations is still a challenging task due to compliance requirements with regulatory policies that can vary across states and countries, and organizations' internal business requirements. Even when adopting the same regulatory policies, each organization can interpret and implement these policies and requirements differently in its internal IT environments. This paper proposes a compliance-aware data management solution for EHR systems. It allows healthcare organizations to define their own security and regulatory compliance requirements for accessing and sharing healthcare data, and enables policy enforcement while sharing data with other organizations. The policy requirements are expressed in form of business processes that govern the access and sharing of data between people and systems. The business process operations are mapped into low-level operations on internal and remote record stores and policy enforcement points. We have implemented the prototype system that supports the proposed approach and integrated it with an open source electronic medical record system called OpenMRS, using which we have defined and enforced some real-world regulations and organizations' policies for data sharing.**

Keywords: regulatory compliance, cross-organization data sharing, business process modeling and execution.

I. INTRODUCTION

Regulations such as Italian Personal Data Protection Code [11] define rules on healthcare data management at different levels, starting from unions/federations and then by individual countries and regions. Furthermore, organizations have their own business requirements and needs. For these organizations exchanging medical records and being compliant to regulatory policies is a complex and challenging task. In particular, some of the challenges consist of mapping regulatory policies described in natural language into business-level specifications and then defining data sharing mechanisms to exchange medical records while protecting data privacy. Such data sharing mechanisms and privacy policies also need to respect organization specific business requirements and thus facilitate organization participation to the EHR sharing network.

Our goal is to design a common data sharing solution that can be offered as a service to healthcare organizations to exchange healthcare data. In this service environment, many organizations that come from different states and jurisdictions should be able to exchange data while conforming to their own regulatory policies and business requirements.

To meet the challenges and design goals, we have designed and developed a compliance-aware data management system called CHINO, and a methodology for establishing explicit links between high-level regulatory policies and detailed data management processes and privacy policies. The methodology starts with the collection of business and compliance requirements that are later used in the definition of executable data management processes and privacy policies. CHINO provides a modeling framework through which organization can define their own security and privacy policies, and data sharing processes to conform to high-level regulatory compliance requirements. Each process step defined in the business process is mapped into low-level operations on data and rules managed by the internal IT infrastructure components. The processes and policies are then executed in a shared processes and policies execution environment.

To evaluate the CHINO methodology and prototype, we examined regulatory and architectural differences among EHR systems in Italy and UK through the analysis of some common cross-organizational data sharing scenarios. We defined data sharing processes in compliance to Italian and UK regulations and executed them inside CHINO. To test the data sharing scenarios we integrated CHINO with a popular open source medical record system called OpenMRS (openmrs.org). In the integrated system, the data sharing processes are used to mediate two OpenMRS instances belonging to the two regulatory contexts and having their own data management processes and policies. This integrated system demonstrated that with CHINO, organizations are able to share medical records while being compliant with regulations and satisfying their internal business requirements.

II. REQUREMENTS AND CASE STUDY

To understand requirements and policy differences among regulations and EHR standards, we analyzed some common cross-organization data sharing scenarios in Italy and UK. Such scenarios are important given the EU plans for offering integrated services across EU countries with projects such as epSOS (epsos.eu). Our focus is on the operating processes that cover policies and interaction protocols between different actors. We paid particular attention on differences with respect

978-3-901882-50-0

to policy enforcement points or the so-called data controllers, which are the entities responsible for applying privacy policies.

The scenario we describe here is called doctor-consultation. It starts with the patient requesting a visit to her personal doctor regarding a medical problem. In case the problem needs further evaluation, the doctor may request a consultation from another physician (specialist). While doctors and specialists may belong to different healthcare organizations, both need to access the patients' medical records.

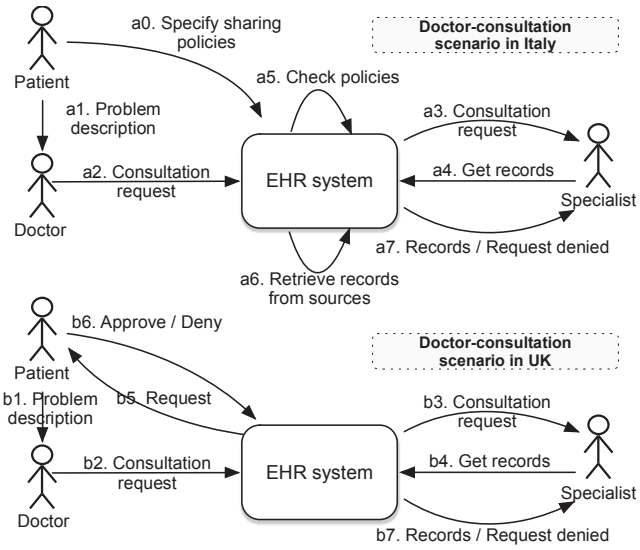

Figure 1. The doctor-consultation scenario as it is performed according to Italy (above) and UK (below) regulatory contexts and EHR systems.

Figure 1 shows a high-level interaction diagram that summarizes how information sharing and interactions are carried out among actors according to compliance policies and EHR systems in Italy [5] and UK [4]. Beyond the obvious differences with respect to the interaction patterns, other key differences include:

- **Privacy policies**, which define who can access which data under which conditions and for which purpose. Conditions and purposes are usually defined by regulations [4, 11] while data owners (usually patients) define data access policies. In Italy the policies are defined at record creation phase (i.e. when patients accept to create their EHRs at step *a0* in Figure 1) and then applied by the EHR system on data requests (*a5*) [11]. In UK the data owners create and apply the policies at runtime (*b6*) deciding to allow or deny the access to their data [4].
- **Security policies**, which define access control mechanisms, data encryption strategies and locations where the records should reside. In Italy the records are stored in decentralized record stores while in UK they are stored at a backbone centralized record store. This implies the need for different data retrieval processes (*a6*) to retrieve the record from the record stores.
- **Policy Enforcement Points** are responsible for applying the policies on data requests. In Italy, the shared EHR systems act as the enforcement points and take decisions (*a5*) on data requests based on patients' policies [5]. In UK patients grant explicitly the access rights to other actors (*b6*) [4]. These policy enforcement differences result in different interaction protocols among patients, doctors and systems.
- **Business specific requirements** can be any organization-specific privacy, security, or other technological related requirements. Such requirements can represent obstacles for organizations in participating to EHR programs [12]. For example, organizations are required to adopt specific audit strategies and as a result the EHR should be able to interact with the external organizations' audit system.

Similar differences can be identified in other data exchange scenarios such as emergency room case or legally motivated cases in which public authority requests override patients' policies. In such exceptional cases specific audit strategies need to be applied and records disclosed to requestor without restrictions [4, 11]. Consequently, the special conditions and auditing strategies have to be implemented and made transparent to auditors and privacy experts.

III. CHINO Methodology for Compliance Aware Data Sharing

We cope with the problems identified above by first defining a methodology to support compliance-aware data sharing processes with organization-level customizations to manage (store, retrieve, and share) the data. Although similar methodologies have been applied to solve compliance issues in business contracts and finance reporting [10], to the best of our knowledge, none of them has solved the regulatory compliance issues in the domain of EHR related data management.

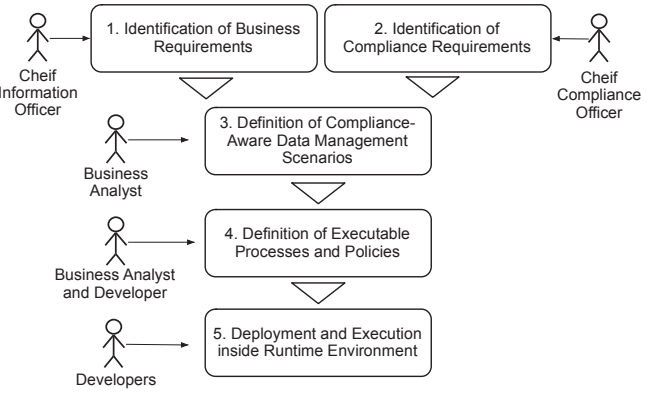

Figure 2. The CHINO methodology and approach to define, translate, deploy and execute the data management operations.

The proposed methodology, as shown in Figure 2, consists of a sequence of steps performed by different actors:

1. First, the Chief Information Officer of the organization identifies the business requirements describing, for example, the flow of interactions, business specific requirements, and assigning flow steps to be fulfilled by different departments or organizations. Such requirements are often described in natural language with operational models describing how actors interact with the EHR systems [4, 5].
2. Second, the Chief Compliance Officer of the organization reviews the business requirements, and follows the com-

pliance checklists to identify the necessary compliance requirements, and security and privacy policies that need to be incorporated. For example, to define at which step which security and privacy policies need to be applied, and to identify exceptional cases in which data can be disclosed without patients' authorizations [11]. Examples of such checklists extracted from UK regulations can be found at Appendix B of [4].

3. Third, a Business Analyst combines the business requirements and the compliance requirements to devise a high-level representation that describes the steps that the involved parties should follow [12]. Figure 1 reveals an example of such representation (with many details omitted). The Business Analyst can also annotate the interaction diagram with the corresponding security and privacy policies identified at *Step 2*.
4. Fourth, the Business Analyst and System Developers translate the high-level representations into executable business processes and rules. The business processes implement the business logic of granular data management operations such as *PushRecord*, *GetRecord* and so on. The operations reflect the identified compliance-aware data exchange interaction requirements and policies. Security and privacy rules are also incorporated into the business process steps and enforced through operations on internal CHINO components.
5. Finally, the resulting executable business processes and rules are deployed and executed into the shared execution environment. The processes orchestrate multi-party human and system interactions including patients, doctors and EHR systems. Business process steps define the data access through a set of operations that are executed on internal IT system components such as medical record store and metadata registry. Business process steps perform also the operations in terms of enforcing the defined security and privacy rules at policy enforcement points.

In summary, the CHINO methodology defines the sequence of steps carried out by multiple stakeholders, from high-level business requirement collection to the low-level process and policy enforcement that results in meeting the high-level compliance requirements.

IV. CHINO Policy Modeling and Execution Framework

Following our proposed methodology, once the business analysts define high-level compliance requirements (*Step 3*), the analysts and developers translate them into executable business processes and privacy and security rules (*Step 4*). To support these steps, the CHINO platform offers the following set of modeling features:

- It defines **Data Management Interfaces (*DMI*)** that represent granular operations over data and rules. Each *DMI* needs to be implemented and customized by data owners using *modeling element*s, *data, operations* and *rules*. *DMIs* include for example, *PushRecord* that stores a data record to the record store and *GetRecord* that serves for requesting a data record. *GetRecord* returns the requested record if the requester is authorized, or a denied status otherwise, or the wait status to signal pending-approval. Another DMI interface, *SearchMetadata*, returns metadata that matches the searching query and that the requestor is authorized to access. Our framework also supports the DMI interfaces of *GrantRecordAccessRights* and *GrantMetadataAccessRights* that grant access rights respectively to data records and metadata records for a specified period of time.
- It borrows the standard BPMN 2.0 [3] elements as **modeling elements** for the definition of processes. The access to *operations*, *data* and *rules* is performed through a set of *Low-Level Operations* (*LLO)* that are invoked inside BPMN *Service Tasks* elements [3].
- It identifies **operations on data** and **rules** that are used within modeling elements and executed by the internal CHINO components. Operations can also involve the calls to external entities such as audit systems, record stores or policy enforcement points. Rules are used for expressing policies identified at *Step 3*.

The *Step 4* of the CHINO methodology starts with the identification of the right sequence of calls to the *DMI* interfaces that respect the high-level interaction requirements and policies identified at *Step 3*. Namely, each step in Figure 1 can be seen as one or many calls to *DMI*. For example the step *a2* is performed first calling the *PushRecord* to save the *Consultation Request* on CHINO *Record Store*. Then *PushMetadata* saves the corresponding instance of metadata on the *Metadata Registry* component. Then *GrantRecordAccessRigths* grants the access rights to the specialist for the *Consultation Request* and other patient's records. When the specialist receives the notification about *Consultation Request* she will ask for patient's metadata records and then request the corresponding data records. The calls to the *GetRecord* DMI will trigger the record owners' processes and privacy policies. The *GetRecord* process has its elements mapped on *LLO* operations. An example of *GetRecord* process could initially check the access rights through a call to the *Access Right Policy Enforcement Point* internal component. Then it will retrieve the data records from the internal or an external *Record Store* and then it will send the retrieved data records to the requestor. Furthermore, it could have additional calls to external audit systems or filter the record content according to declared purpose of use of data. In that case it will call the *Data Filtering Policy Enforcement Point* that will filter unnecessary data [1]. All those configurations are supported in our process-based approach.

Overall the combination of *DMI* calls implements a two-phase data exchange protocol that relies on the metadata records to signal record availability and then sharing the corresponding data records with authorized data consumers. This protocol is based on IHE – Cross-Enterprise Document Sharing (XDS) profile [6]. This protocol has been proved to be effective to exchange medical records while preserving privacy in Trentino region in Italy (for more details see [1]). Records can be stored encrypted on the CHINO record store or kept on external record stores [8]. Our process-based methodology supports both data storage settings and can implement different interaction protocols to retrieve data from sources.

To validate our methodology we developed the CHINO prototype that is able to support process and policy definition

and execution. We used Activiti (activiti.org), an open source BPMN 2.0 process engine, as the process repository and execution engine. The Activiti plugin for the Eclipse IDE (eclipse.org) is used as the collaborative process-modeling tool. In terms of runtime support, Activiti provides long-term persistence of processes and concurrent process execution. The calls to *LLO* are done through the developed Java libraries and APIs offered by the Mule Enterprise Service Bus (ESB). The ESB provides message persistence, transaction management, and many other technical features. It allows also the creation of the *LLO* and *DMI* APIs and integration with Activiti runtime through a set of REST APIs.

V. The OpenMRS Integration

To demonstrate and validate the CHINO system prototype we integrated it with an open source electronic medical records system called OpenMRS (openmrs.org). To test the interaction we developed an OpenMRS module for the doctor-consultation scenario called *ChinoOpenMRSModule*. Then we developed two different sets of processes and policies to simulate the configuration in which one organization operates under Italian legislation while the other organization is under UK legislation. Both OpenMRS instances rely on a common CHINO policy execution environment deployed separately from these two OpenMRS instances. As a result, we can show that one organization on an OpenMRS instance can perform data sharing with the organization on a different OpenMRS instance having different data management requirements and policies.

VI. Related Work

Extracting requirements and constraints from government regulations and business contracts has been widely studied [10]. Our methodology can support the choice of any of these proposed methods. The GEODAC framework [7] provides a modeling language for the service provider and the service customer to communicate their data assurance policies but it does not provide policy enforcement points orchestration and processes visibility. The importance of process visibility aspect is emphasized by work [2], which demonstrates that with visual representation of business processes, systems could improve the trust, compliance and understandability of data management processes. The work reported by [10] focuses on process design in the context of business contract. In contrast, our focus is on designing processes that implement data management operations. A methodology for compliance-aware process design is proposed in [9] while [12] proposes an argumentation-based framework for the definitions of goals. However, these process design techniques can be certainly leveraged in our methodology to support developers and business analysts when developing compliant processes.

Protecting data in untrusted environments represents a key challenges in systems such as CHINO [8]. In [1] we defined a purpose-based access control mechanism for data sharing to satisfy the data sources needs. This work takes advantage of the previously developed mechanisms and incorporates them into the business process execution in order to achieve privacy-aware data sharing. To address data representation, data storage and data exchange interoperability, we take advantage of standards that have been proposed by institutions such as the Integrating the Health care Enterprise - IHE consortium [6]. IHE proposes a set of profiles such as data sharing XDS profile that has been applied in projects such as Italian National Health Record [5], EU cross-country epSOS project (epsos.eu) and many others. XDS is based on a central registry that contains searchable metadata while records are stored on decentralized record stores. In this paper, we extend the XDS profile to support data and rule management.

VII. Conclusions

Regulatory compliance is a complex task to achieve for every organization that deals with sensitive data. In healthcare, this is even more difficult since regulations and best practices vary from one regime to the other regime, and from one organization to the other organization. To help organization exchanging healthcare data, we proposed a new methodology and an execution environment to:

- capture the sequence of steps that need to be carried out by organizations to define their own security and privacy policies and data sharing processes to conform to high-level regulatory compliance requirements.
- identify a set of elements, IT components and actors that can be orchestrated by data sharing processes to achieve regulatory compliant data sharing.
- provide an environment for the definition and execution of shared processes and policies to support data, process and policy management.

References

[1] G. Armellin, D. Betti, F. Casati, A. Chiasera, G. Martinez and J. Stevovic. Privacy preserving event driven integration for interoperating social and health systems. SDM'10.

[2] R. K. E. Bellamy et al. Seeing is believing: designing visualizations for managing risk and compliance. IBM Syst. J,'07.

[3] Business Process Model and Notation (BPMN) version 2.0, OMG. 2011.

[4] Department of Health (UK). Confidentiality, NHS Code of Practice. '03.

[5] InFSE: Technical Infrastructure for Electronical Health Record Systems. Italian Ministry of Innovation and Technology, v1.0. 2010.

[6] IHE - Integrating the Healthcare Enterprise, IHE IT Infrastructure (ITI) Technical Framework, Vol 1 – Integration Profiles, v.8 Aug 2011.

[7] J. Li, B. Stephenson, H. R. Motahari-Nezhad and S. Singhal. GEODAC: A data assurance policy specification and enforcement framework for outsourced services. IEEE TSC, 2011.

[8] J. Li, S. Singhal, R. Swaminathan, and A. H. Karp. Managing Data Retention Policies at Scale. IEEE Transactions on Network and Service Management (TNSM), Vol 9, No 4, December 2012.

[9] R. Lu, S. Sadiq and G. Governatori. Compliance aware business process design, BPM 2007.

[10] Z. Milosevic, S. Sadiq and M. Orlowska. Translating business contract constraints into compliant business processes, EDOC, 2006.

[11] Personal Data Protection Code. Italian Privacy guarantor, Legislative Decree no. 166 dated 30 June 2003 (2003).

[12] A. Siena, G. Armellin, G. Mameli, J. Mylopoulos, A. Perini and A. Susi. Establishing Regulatory Compliance for IS Requirements: An Experience Report from the Health Care Domain, ER, 2010.