Metadata of the chapter that will be visualized online

Chapter Title	Enabling Privacy by Design in Medical Records Sharing	
Copyright Year	2015	
Copyright Holder	Springer Science+Business Media Dordrecht	
Corresponding Author	Family Name	**Stevovic**
	Particle	
	Given Name	**Jovan**
	Suffix	
	Organization	Centro Ricerche GPI
	Address	Trento, Italy
	Email	jovan.stevovic@cr-gpi.it
Author	Family Name	**Bassi**
	Particle	
	Given Name	**Eleonora**
	Suffix	
	Division	Department of Information Engineering and Computer Science
	Organization	University of Trento
	Address	Trento, Italy
	Division	Nexa Center for Internet and Society
	Organization	Polytechnic University of Torino
	Address	Trento, Italy
	Email	bassi@disi.unitn.it
Author	Family Name	**Giori**
	Particle	
	Given Name	**Alessio**
	Suffix	
	Organization	Fondazione Graphitech
	Address	Trento, Italy
	Email	alessio.giori@studenti.unitn.it
Author	Family Name	**Casati**
	Particle	
	Given Name	**Fabio**
	Suffix	
	Division	Department of Computer Science
	Organization	University of Trento
	Address	Trento, Italy

	Email	casati@disi.unitn.it
Author	Family Name	**Armellin**
	Particle	
	Given Name	**Giampaolo**
	Suffix	
	Organization	Centro Ricerche GPI
	Address	Trento, Italy
	Email	giampaolo.armellin@cr-gpi.it

Abstract

In healthcare a multiplicity of actors needs to access and share patients' data while being compliant with policies defined by data protection legislation. Building frameworks to enable stakeholders to design and develop data-sharing mechanisms in compliance with legislations is a challenging task.

In this work, we propose a methodology and a platform called CHINO, inspired by Privacy by Design principles, to guide the involved stakeholders during the definition of data-sharing processes by using visual representations such as Business Process Modelling (BPM). BPM enables the stakeholders to reason and share their understanding about privacy aspects from early analysis phases, while CHINO platform provides the execution framework for the defined BPM processes and privacy policies.

To prove the CHINO efficacy, we show how policies extracted from legislations can be modelled and executed and we report our studies with end-users with whom we validated the system usability. We analyse also CHINO from a legal point of view and its compliance with data protection legislations.

Chapter 16
Enabling Privacy by Design in Medical Records Sharing

Jovan Stevovic, Eleonora Bassi, Alessio Giori, Fabio Casati, and Giampaolo Armellin

Abstract In healthcare a multiplicity of actors needs to access and share patients' data while being compliant with policies defined by data protection legislation. Building frameworks to enable stakeholders to design and develop data-sharing mechanisms in compliance with legislations is a challenging task.

In this work, we propose a methodology and a platform called CHINO, inspired by Privacy by Design principles, to guide the involved stakeholders during the definition of data-sharing processes by using visual representations such as Business Process Modelling (BPM). BPM enables the stakeholders to reason and share their understanding about privacy aspects from early analysis phases, while CHINO platform provides the execution framework for the defined BPM processes and privacy policies.

To prove the CHINO efficacy, we show how policies extracted from legislations can be modelled and executed and we report our studies with end-users with whom we validated the system usability. We analyse also CHINO from a legal point of view and its compliance with data protection legislations.

AQ1

J. Stevovic (✉) • G. Armellin
Centro Ricerche GPI, Trento, Italy
e-mail: jovan.stevovic@cr-gpi.it; giampaolo.armellin@cr-gpi.it

E. Bassi
Department of Information Engineering and Computer Science, University of Trento, Trento, Italy

Nexa Center for Internet and Society, Polytechnic University of Torino, Trento, Italy
e-mail: bassi@disi.unitn.it

A. Giori
Fondazione Graphitech, Trento, Italy
e-mail: alessio.giori@studenti.unitn.it

F. Casati
Department of Computer Science, University of Trento, Trento, Italy
e-mail: casati@disi.unitn.it

S. Gutwirth et al. (eds.), *Reforming European Data Protection Law*,
Law, Governance and Technology Series 20, DOI 10.1007/978-94-017-9385-8_16

16.1 Introduction

Data sharing and interoperability among healthcare applications is fundamental to improve healthcare assistance.[1] Many projects such as the Italian Electronic Health Record (EHR) reference architecture,[2] UK NHS system, or the European epSOS project[3] have been proposed with the aim of interconnecting different applications. However, the development of such systems is challenging, and one reason is that they need to comply with strict privacy and compliance rules defined by Data Protection legislation.[4] While the projects mentioned above have considered the legislation during their development, to the best of our knowledge none of them have considered the privacy related aspects through all stages of project development as proposed by the Privacy by Design approach.[5] As a consequence, in some cases this led to critical privacy breaches[6] and limitations in their functionalities. For example, none of them gave to the data subjects (i.e. patients) the possibility to have full control over their data or transparency about data management aspects. Instead, considering privacy during the entire lifecycle of software development leads to multiple benefits such as providing more efficient security and privacy strategies, patient-centred privacy mechanisms and therefore improved customer satisfaction, trust, and more efficient operations.[7]

With the CHINO project we aim at creating a framework, inspired by Privacy by Design principles, to enable a multidisciplinary collaboration of various stakeholders involved in the design and development of data sharing mechanisms

[1] Richard Hillestad et al., "Can electronic medical record systems transform health care? Potential health benefits, savings, and costs," *Health Affairs* (2005): 24.

[2] Italian Data Protection Authority, *Guidelines on the Electronic Health Record. and the Health File*, [doc. Web 1634116] July 16, 2009, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1634116.

[3] epSOS European eHealth project, http://www.epsos.eu/; *Article 29 Data Protection Working Party, Working Document 01/2012 on epSOS*, Adopted on 25 January 2012, wp 189.

[4] *European Parliament and Council: Directive 95/46/EC: Directive on protection of individuals with regard to the processing of personal data and on the free movement of such data*; *Italian Data Protection Code: Legislative Decree No. 196/2003*. See also, *European Parliament and Council: Proposal for a regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*,2012; *European Parliament and Council: Directive 2011/24/EU: Directive on the application of patients' rights in cross-border healthcare*; See also Italian Ministry of Innovation and Technology, *InFSE: Technical Infrastructure for Electronical Health Record Systems, v1.2.*, 2012.

[5] Ann Cavoukian, "Privacy by Design," Information & Privacy Commissioner, Ontario, Canada. http://www.ipc.on.ca/images/Resources/privacybydesign.pdf. (2009).

[6] The Guardian, *NHS staff breach personal data 806 times in three years*, 2011. Available at: http://www.theguardian.com/healthcare-network/2011/oct/28/nhs-staff-breach-personal-data-806-times. Accessed on January 2014.

[7] Ann Cavoukian, "Privacy in the Clouds," *Identity in the Information Society* (2009): 1.

and to consider privacy, business and organisational requirements during all stages of software development; from analysis to deployment and execution. We aim at creating a data protection environment by moving privacy issues directly into the technology and the marketplace.[8] We envision that, by exploiting the advantages of visual representations such as Business Process Modelling (BPM) technology,[9] we can give to the stakeholders the necessary tools to reason and share their understanding about compliance aspects. Such representations should facilitate also the phases of project validations performed before going into production, and inspections by Compliance Officers at runtime.

In this direction, CHINO proposes a methodology that starts with the extraction of compliance requirements from legislations and with the gathering of business requirements from the involved stakeholders, and ends with the definition of executable processes that are able to enforce the collected requirements. At each step, the methodology guides the involved actors by giving them tools and guidelines on how to define processes and rules that are later executed into the CHINO execution environment.

The paper presents the CHINO methodology by considering a healthcare case study and privacy requirements extracted from Italian,[10] European[11] and HIPAA[12] legislations. We show examples of defined processes and report a user study with a group of developers that have tested the system usability by using notions from Human Computer Interaction discipline. We conclude by analysing the methodology with main focus on the steps in which compliance officers are involved in the definition of processes and validation of compliance against data protection laws.

The paper is organised as follows. Section 2 gives an overview of research effort in related areas. Section 3 presents the use case scenario and a first example set of extracted policies from legislations. The CHINO methodology, technology and its validation including the usability study are presented in Section 4. In section 5 we analyse CHINO from a legal point of view while in Section 6 we discuss the results and conclusions.

[8] Ann Cavoukian, "Personal Data Ecosystem (PDE) – A Privacy by Design Approach to an Individual's Pursuit of Radical Control," in *Digital Enlightenments Yearbook 2013. The Value of Personal Data*, ed. Mireille Hildebrandt et al. (IOS Press, 2013), 89–101.

[9] Activiti BPM Platform, Available at http://activiti.org/.; Richard Lenz and Manfred Reichert, "It support for healthcare processes premises, challenges, perspectives". *Data Knowledge Engineering* (2007): 61.

[10] *Legislative Decree No. 196/2003*.

[11] *Directive 95/46/EC*. See also, *European Parliament and Council: Proposal for a regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*.

[12] Office for Civil Rights. *HIPAA, medical privacy national standards to protect the privacy of personal health information*. 2000.

16.2 Related Work

Data sharing in healthcare is fundamental to improve the assistance services and many projects tried to address related challenges.[13] Commercial solutions such as PracticeFusion,[14] national projects such as the Italian EHR reference system,[15] the European project epSOS or the electronic social and health record developed for the Trentino region in Italy[16] are just some examples.

In such context process based technologies such as BPM have been demonstrated to be efficient in modelling and executing the assistance processes and activities that involve multiple users. The work by Richard Lenz and Manfred Reichert[17] analyses the impacts of process-based technologies on healthcare demonstrating their potential benefits on assistance services. The authors identify two kinds of processes: organisational processes and medical processes. In this work we analyse both types to define compliant data management processes to manage single medical records.

deletion--> The work by Ottensooser et al.[18] shows that once defined and executed, ~~the~~ BPM processes can also facilitate the verification activities by compliance officers. It analyses the understandability of a language for BPM called Business Process Model and Notation (BPMN), versus text notation for representing the design of information systems showing positive results. In another work by Recker and Dreiling[19] it is claimed that people, who know a business process notation, can switch to a new notation quite easily. We focus on enabling developers to create deletion--> ~~the~~ processes in an easy way and study their level of confidence following the methodologies and best practices in interaction design.[20]

[13] Richard Hillestad et al., "Can electronic medical record systems transform health care? Potential health benefits, savings, and costs," *Health Affairs* (2005): 24.

[14] Practice Fusion, *Free Web-based Electronic Health Record*, www.practicefusion.com.

[15] Italian Ministry of Innovation and Technology, *InFSE: Technical Infrastructure for Electronical Health Record Systems, v1.2*. (2012).

[16] Giampaolo Armellin et al., "Privacy preserving event driven integration for interoperating social and health systems," *Secure Data Management 7th VLDB workshop* (2010): 63–68.

[17] Richard Lenz and Manfred Reichert, "It support for healthcare processes premises, challenges, perspectives," *Data Knowledge Engineering* (2007): 61.

[18] Avner Ottensooser et al., "Making sense of business process descriptions: An experimental comparison of graphical and textual notations," *Journal of Systems and Software* (2012): 85.

[19] Jan C. Recker and Alexander Dreiling, "Does it matter which process modelling language we teach or use? An experimental study on understanding process modelling languages without formal education," in *18th Australasian Conference on Information Systems* (University of Southern Queensland, 2007.

[20] See for instance Helen Sharp, "Interaction design," (Wiley.com., 2003).

Some works uses BPM to tackle challenges related to privacy-aware data sharing.[21] The extracted and formally defined requirements and obligations from legislations can be synthesised as business processes[22] and work such as the one done by Bellamy et al.[23] demonstrates that with visual representations there could be benefits in understanding and improving them. The work by Lu et al.[24] shows an approach for compliance aware business process design while the work by Milosevic et al.[25] translates constrains and contracts into business processes. We chose to approach compliance related challenges proactively following the Privacy by Design[26] that has emerged as one of most promising approaches in tackling privacy related issues. Although it is only a set of high level principles and it has been criticised by some researchers due to its sometimes vague and high expectations,[27] it has been successfully applied in some projects and case studies.[28] Privacy by Design considers the privacy related aspects from early stages of systems design and has been introduced in the regulation framework by the Art. 29 Data Protection Working Party in the document *The Future of Privacy*[29] and in the *Proposal for the new European General Data Protection Regulation*. Therefore we aim at studying how the healthcare scenario proposed by the CHINO project can support and embed Privacy by Design principles, and if it can provide a reference implementation in this domain.

required "." --> instead of ","

[21] Trevor Breaux et al., "Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations," in *Requirements Engineering, 14th IEEE International Conference* (2006), 49–58.

[22] Ahmed Awad et al., "An iterative approach for business process template synthesis from compliance rules," *Advanced Information Systems Engineering* (2011): 6741.

[23] Rachel K. E. Bellamy et al., "Seeing is believing: designing visualizations for managing risk and compliance," *IBM System Journal* (2007): 46.

[24] Ruopeng Lu et al., "Compliance-aware business process design," *BPM Workshops* (2008): 4928.

[25] Zoran Milosevic et al., "Translating business contract into compliant business processes," in *EDOC'06* (IEEE Computer Society, 2006), 211–220.

[26] Ann Cavoukian, "Privacy by Design,", Information & Privacy Commissioner, Ontario, Canada. http://www.ipc.on.ca/images/Resources/privacybydesign.pdf. (2009); Ann Cavoukian, "Privacy in the Clouds," *Identity in the Information Society* (2009): 1; Peter Schaar "Privacy by Design," *Identity in the Information Society* (2010): 3.

[27] Bert-Jaap Koops and Ronald Leenes. "Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law." International Review of Law, Computers & Technology ahead-of-print (2013): 1–13. See also, Ugo Pagallo. "On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law". European Data Protection 2012: 331–346.

[28] Paolo Balboni and Milda Macenaite, "Privacy by Design and anonymisation techniques in action: Case study of Ma3tch technology," *Computer Law and Security Review* (2013): 29; Antonio Kung et al., "Privacy-by-design in its applications," in *2nd Int. Workshop on Data Security and Privacy in Wireless Networks* (D-SPAN, 2011), 1–6.

[29] Article 29 Data Protection Working Party, *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, WP 168, (2009).

16.3 Use Case Scenario and Identified Policies

To test CHINO efficacy we started by analysing data-sharing scenarios and extracting privacy and compliance requirements from legislations. During the first CHINO testing,[30] sets of requirements were extracted from Italian and UK legislations and have been applied in a use case scenario called "doctor consultation". In this work, to further validate the framework, we consider European[31] and HIPAA legislations[32] and apply ~~the~~ extracted requirements to a different use case called "immunisation scenario". The scenario involves different actors that need to share medical records about a patient:

deletion -->

Added an "s"-->

> Mr Brown wants to spend his holidays in Mozambique and to be prepared for that environment, he asks to Dr Kelly, his family doctor, some advices. Dr Kelly alerts him that in Mozambique it is possible to get the typhus disease and she prescribes him a vaccine injection to administer before leaving. Dr Kelly creates an ePrescription using her medical record system, which uploads automatically the created record containing the ePrescription to CHINO. Then Mr Brown goes to the nearest hospital to get administered the vaccine. At the hospital, Dr Smith accesses Brown's medical data using his own medical record system that gets data from CHINO and administer the vaccine.

deletion -->

Next subsection describes ~~the~~ privacy and compliance policies that have been extracted and that apply to this use case scenario.

16.3.1 Identified Policies

put "a" instead of "the" -->

"citizens' " instead of "citizen's" -->

Extracting requirements and policies from legislations embeds some pitfalls starting from collecting the complete set of legislations and guidelines that are relevant to ~~the~~ considered project scenario. Moreover, these legal requirements and organizational policies should be compared and combined in order to identify their exact hierarchy and terms of applicability.[33] For example, the Italian context is characterized by many levels of authorities and rules which protect ~~citizen's~~ privacy rights: starting from the EU level legislations[34] transposed in Italy with the Data Protection Code,[35] to the Guidelines and recommendations provided by the Italian Data Protection Authority in collaboration with the Ministry of Health on Electronic

[30] Jovan Stevovic et al., "Business process management enabled compliance-aware medical record sharing," *Int. J. Business Process Integration and Management* (2013):6.

[31] *Directive 95/46/EC.*

[32] Office for Civil Rights, *HIPAA, medical privacy national standards to protect the privacy of personal health information.*

[33] David G. Gordon, and Travis D. Breaux. "Reconciling multi-jurisdictional legal requirements: A case study in requirements water marking." *Requirements Engineering Conference*, IEEE, 2012.

[34] *Directive 95/46/EC.*

[35] *Legislative Decree No. 196/2003.*

Health Records.[36] Moreover each region has its own competences on applying healthcare legislation, which is done by many local healthcare providers called "ASL: Azienda Sanitaria Locale" that deliver assistance services to patients.[37] This context shows clearly that in Italy, like in other countries, there exist many bodies having different competences that define privacy legislations on different aspects.

Here we report a subset of privacy policies we extracted from legislation and that are relevant to the Immunisation scenario described before:

P1 a Data Controller (DC) must provide policies and procedures for the creation, maintenance, and revocation of access for both doctors and users.

P2 a DC must ensure that personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

P3 a DC must implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use PHI.

P4 a DC needs to ensure secure data management by implementing mechanisms for data encryption of Personal Health Information (PHI).

P5 a DC has the ability to disclose data for Research, Marketing, Fundraising only if appropriately de-identified by removing Personal Identifiable Information.

deletion -->

The identified requirements apply on the Immunisation scenario at different steps. During the doctors' access to patients' data, the P1, P2 and P3 policies need to be satisfied. The doctors need to have the required access rights (P1), access only to the information that is required to fulfil the tasks (P2) and their accesses need to be logged through audit mechanisms (P3). Patients' data needs also to be kept secure on the systems used by the personal doctors, CHINO and the hospital systems (P4).

Next section describes the CHINO framework i.e., the methodology, the modelling framework and how BPM processes and rules are defined and executed based on the requirements and policies extracted insofar.

16.4 CHINO Framework

added "S" --> The main goal of CHINO is to provide a framework to involve different stakeholderS (project managers, compliance and data protection officers, analysts and developers) through the lifecycle of development of compliant data sharing processes and

[36] Italian Data Protection Authority, *Guidelines on the Electronic Health Record*; Italian Ministry of Innovation and Technology, *InFSE: Technical Infrastructure for Electronical Health Record Systems, v1.2*. (2012).

[37] Giampaolo Armellin et al., "Privacy preserving event driven integration for interoperating social and health systems," *Secure Data Management 7th VLDB workshop* (2010): 6368; Municipality of Trento. *Regulations for the protection of personal data of the municipality of Trento*. http://www.comune.trento.it/, 2007; Municipality of Trento. *Operational guidelines to privacy*. http://www.comune.trento.it/, 2009.

privacy policies. The key idea sits in using BPM technology to define data management operations (e.g. storing, sharing) according to the data owners' requirements and policies extracted from laws and organizational rules. By doing so, CHINO executes the data owners' business processes and policies while replying to data requests and interacting with external applications and actors. In such way, CHINO enables a cross-organisation and even cross-border[38] compliance-aware medical record sharing since the processes and policies, for each of the participant organization, can be defined according to their own data protection legislation and set of requirements.

Next subsection shows how the CHINO methodology and how privacy law compliant data sharing can be achieved.

16.4.1 CHINO Methodology

To identify actors and a set of steps to define privacy law compliant processes and policies that are later executed into the CHINO platform, we propose the CHINO methodology (sketched in Fig. 16.1). It identifies main steps, the actors and artefacts that are produced and consumed at each step. It does not refer to any software development methodology (e.g. Waterfall, or Agile) since the steps could be also executed iteratively and it is not tied to any specific privacy law or legislation; therefore it should be applicable to any regulatory context.

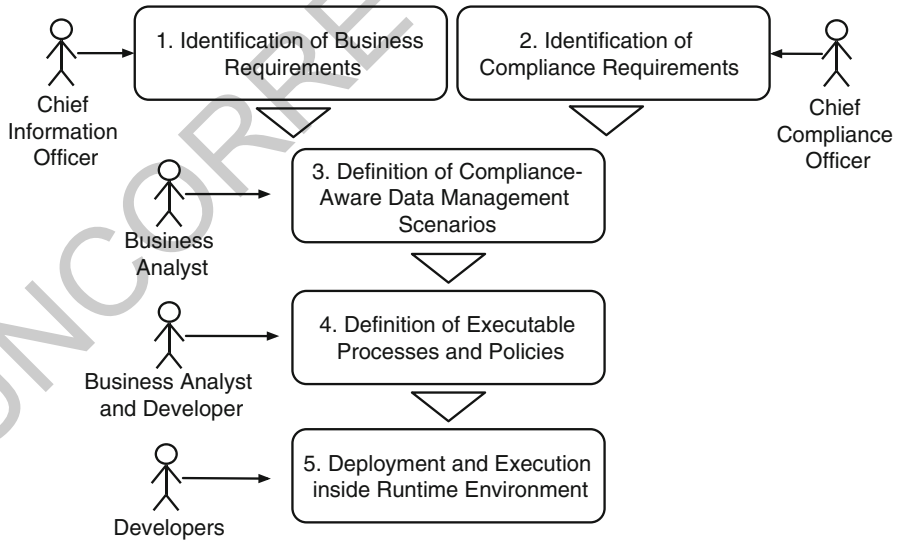

Fig. 16.1 The CHINO methodology

[38] *Directive 95/46/EC* and in particular *Directive 2011/24/EU*.

The steps, as shown in Fig. 16.1 are:

1. Chief Information Officer identifies business requirements describing, for example, the flow of interactions, and tasks to be fulfilled by different actors or organisations. Such requirements, like in the Immunisation scenario, are often described in natural language with operational models describing how actors interact among them and with the medical record systems. At this step also domain experts such as doctors and nurses could be involved in defining the assistance processes and the data that need to be managed and shared.[39]
2. Chief Compliance Officer of the organisation identifies the legislation and extracts the compliance requirements including the security and privacy policies that need to be satisfied. For example, as shown by the use case, it could define at each step which security and privacy policies need to be applied, according to the applicable law (national, European, and international), and identifies exceptional cases in which data can be disclosed without patients' authorisations (policy P5 in Section 3.1). Due to legislation intrinsic complexity, the Compliance Officer could rely on collaborations and consultations with actors having a legal background to extract all requirements. This step could consist of various interactions also among compliance and information officers to devise the set of information that will be managed, the operations and the set of norms that will apply to such operations.
3. Business Analyst combines business requirements and compliance requirements to devise a high-level representation that describes the steps the involved parties should follow.[40] The business analyst can also annotate such representations with the corresponding security and privacy policies identified at Step 2.[41] If necessary, the step 2 and 3 can be performed more times iteratively to refine the policies to be enforced.[42]
4. Business Analyst and System Developer translate high-level representations into executable business processes and rules. Business processes implement the business logic of data management operations such as *Push Record* and *Get*

[39]Giampaolo Armellin et al., "Privacy preserving event driven integration for interoperating social and health systems," *Secure Data Management 7th VLDB Workshop* (2010): 6368.

[40]Alberto Siena et al., "Establishing regulatory compliance for IS requirements: an experience report from the health care domain," *29th Int. Conf. on Conceptual Modelling* (2010): 6412.

[41]Richard Lenz and Manfred Reichert, "It support for healthcare processes premises, challenges, perspectives," *Data Knowledge Engineering* (2007): 61.

[42]We give examples of such representations in Jovan Stevovic et al., "Business process management enabled compliance-aware medical record sharing," *Int. J. Business Process Integration and Management* (2013):6; but also leave to the users the freedom to choose the most appropriate representation according to the recommendations by Article 29 Data Protection Working Party, *Working Document on the processing of personal data relating to health in Electronic Health Records (EHR)*, Adopted on 15/02/2007, wp 131.; Ruopeng Lu et al., "Compliance-aware business process design" *BPM Workshops* (2008): 4928; Alberto Siena et al., "Establishing regulatory compliance for IS requirements: an experience report from the health care domain," *29th Int. Conf. on Conceptual Modelling* (2010): 6412.

Record. The defined security and privacy rules that are incorporated into business process steps are executed through operations on internal CHINO components.

5. Finally, the resulting executable business processes and rules are deployed and executed into the shared execution environment.

In summary, the CHINO methodology identifies the sequence of steps carried out by multiple stakeholders, from high-level business requirement collection to the low-level process execution and policy enforcement. Next subsection shows the technology to support the process modelling.

16.4.2 CHINO Modelling Framework

The process and policy Modelling Framework, as described by the methodology, involves the collaboration of Business Analysts and Developers. Figure 16.2 shows the framework at work.

Developers can model processes in Section A by using a set of Business Process Model and Notation (BPMN)[43] modelling elements that can be dragged and

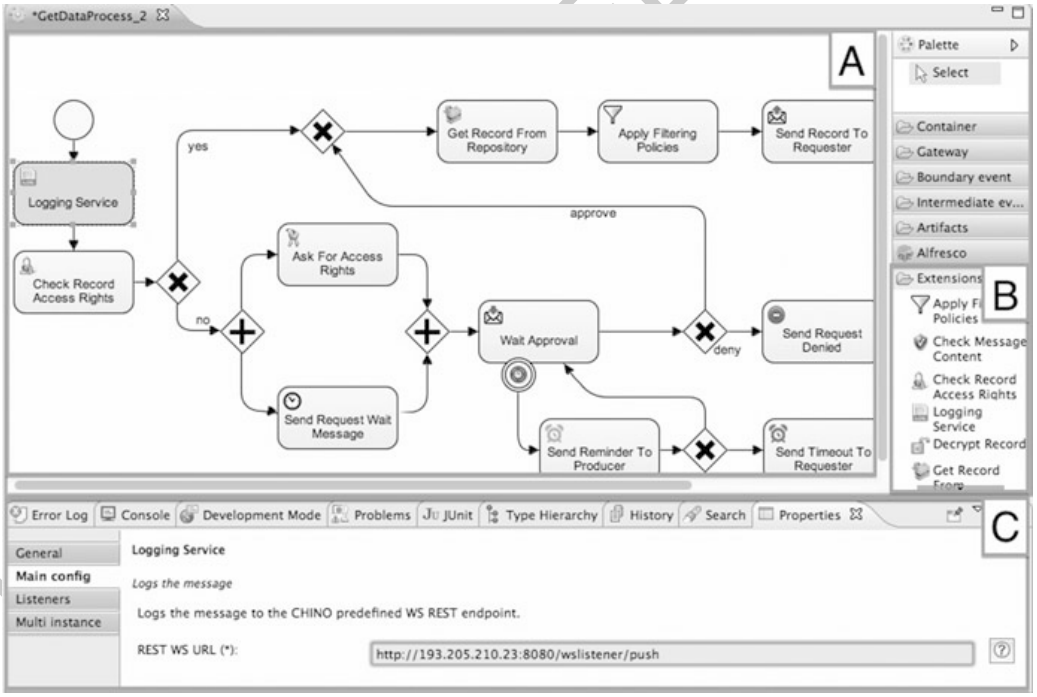

Fig. 16.2 A screenshot of the CHINO Modelling Framework based on the (Activiti Designer Activiti BPM Platform, Available at http://activiti.org/)

[43]OMG, *BPMN–Business Process Model and Notation v2.0 Specification*, 2011, Available at http://www.omg.org/spec/BPMN/2.0/.

Fig. 16.3 A subset of the CHINO Custom Tasks

dropped from Section B. They will need to input some configuration parameters in the *Properties* tab shown in Section C to make it executable. Once deployed, the processes become automatically executable to manage organisations' data. The Modelling Framework is implemented by extending the Activiti Designer[44] with a set of new constructs called *Custom Tasks* to provide a comprehensive set of elements and to facilitate the process modelling. Custom tasks are extensions to the standard BPMN 2.0 elements and a subset of them is shown in Fig. 16.3.

Each of the introduced custom tasks has a specific name, icon and behaviour. The set of custom modelling elements has been introduced to simplify the development of specific CHINO processes that implement data management operations. Namely, each of the custom tasks can be used either to reply to the requester with a specific and predefined message or to interact with the platform internal components.[45] They are used to define how patients' personal information is disclosed to, and managed by CHINO and how it is disclosed to other institutions and users. A subset of custom elements is described below:

- C1 – *Logging Service* is a customisable logging task that logs process status on internal Logging component or an external auditing system. It takes in input a customizable set of information that can be specified by the developers.
- C2 – *Get Record From Repository* restores the requested record from record store. The record store can be also external.[46]
- C3 – *Push Record* saves a record on the internal record store component.

[44] Activiti BPM Platform, Available at http://activiti.org/.

[45] For a more exhaustive technical description see Jovan Stevovic et al., "Business process management enabled compliance-aware medical record sharing," *Int. J. Business Process Integration and Management* (2013):6.

[46] According to new rules proposed by *European Parliament and Council: Proposal for a regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).*

- C4 – *Apply Filtering Rules* applies purpose-based filtering rules to records to eliminate the unnecessary data based on the specified purpose of use.[47] This is fundamental to achieve the proportionality principle and satisfy the policy P2.

The following subsection shows how these elements were used within a process example to implement an operation according to identified requirements.

16.4.3 A Process Example

Here we show an example of a process that is executed inside the CHINO platform to implement an operation over data. We analyse in particular the *Get Record* operation that is invoked when a medical record is requested by an organisation. The process model in Fig. 16.4 (simplified for readability reason) has been implemented according to policies extracted from HIPAA legislation and listed in section 3.1.

It starts by checking the request message content to ensure that the request contains all the mandatory data. According to policies P1, P2 and P3 from Section 3.1, the request needs to be authorised, it needs to access only to the data the requester is entitled to access for that specific task and, all actions need to be logged. If the requester does not have the required access rights, the process will ask for approval to the record owner. Under HIPAA, usually personal doctors approve requests to data on behalf of the patients. Therefore, the process will wait for approval soliciting the doctor periodically. In case of approved request, the process retrieves the requested record from a local record store. The record store could be also remote in case this is mandated by guidelines for EHR creation or laws.[48] Once retrieved the record, the process needs to satisfy the proportionality principle

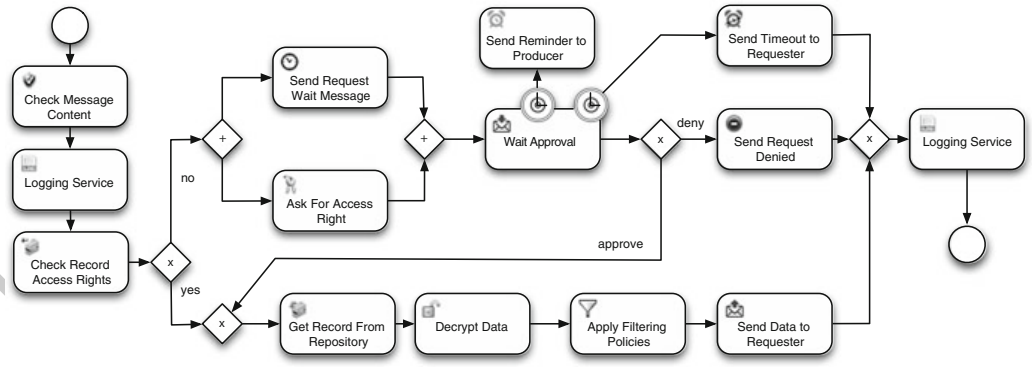

Fig. 16.4 The CHINO "*Get Record*" Process

[47]Giampaolo Armellin et al., "Privacy preserving event driven integration for interoperating social and health systems," *Secure Data Management 7th VLDB Workshop* (2010): 6368.

[48]This is the case of Italian law: Italian Ministry of Innovation and Technology, *InFSE: Technical Infrastructure for Electronical Health Record Systems, v1.2*. (2012).

that is one of the most important principles identified by Data Protection legislations and that needs to be tackled in combination with the principles of necessity and purpose limitation.[49] To satisfy those requirements, the process invokes the *Apply Filtering Policies* element that filters the data that is not necessary for that requestor for that specific purpose of access. The filtering policies are defined by record owners or entities responsible for record management (e.g. Data Controllers).[50] The record is then returned to the requestor replying to *Get Record* request. In case of request denied, a negative response is returned to the requester, while in case of timeout (neither positive nor negative response) a timeout message is returned. Finally in case something went wrong, an error message is returned.

The proposed process based approach is able also to manage easily the exceptional cases in which data subjects are under a certain age threshold or the records are about mental problems and should not be disclosed to the subjects. The defined processes are then deployed and executed in the CHINO Platform.

16.4.4 CHINO Platform

Following the CHINO methodology, once processes are defined (Step 4), they are deployed and executed inside the shared execution environment (Step 5). CHINO platform provides the execution environment and a set of internal components to manage data and rules. The platform is also responsible for technical aspects such as reliability, scalability, and secure communication with external systems.[51]

The platform prototype has been developed and tested by integrating it with a popular medical record system called OpenMRS (www.openmrs.org) and by developing the doctor consultation use case according to Italian and UK legislations. We defined data sharing processes in compliance to Italian and UK legislations and executed them inside CHINO to demonstrate that with CHINO, organisations are able to share medical records while being compliant with privacy legislations and while satisfying their internal business requirements.[52] This scenario demonstrated also how CHINO can enable cross-border and cross-legislation medical data sharing, according to Directive 2011/24/UE.

Next subsection shows how we analysed legislations in this work and how we tested process modelling with developers.

[49]Office for Civil Rights. *HIPAA, medical privacy national standards to protect the privacy of personal health information*.

[50]Giampaolo Armellin et al., "Privacy preserving event driven integration for interoperating social and health systems," *Secure Data Management 7th VLDB Workshop* (2010): 6368.

[51]Jovan Stevovic et al., "Business process management enabled compliance-aware medical record sharing," *Int. J. Business Process Integration and Management* (2013):6.

[52]Jovan Stevovic et al. "Business process management enabled compliance-aware medical record sharing," *Int. J. Business Process Integration and Management* (2013):6.

16.4.5 The Usability Validation

According to the CHINO methodology, Business Analysts and Developers should be able to define the processes in compliance to the identified requirements by using the Modelling Framework. To test these assumptions and the Modelling Framework usability, we performed a user study with a group of nine developers that had preliminary knowledge about process modelling with the standard BPMN Activiti Designer.[53] With the user study we tried to understand if the requirements identified at Steps 1, 2 and 3 can be mapped into business processes at Step 4. The users where chosen among master students and employees of the University of Trento. The analysis was based on notions from the Interaction Design (ID) studied in Human Computer Interaction (HCI) discipline and applying the usability testing methodology called Think Aloud.[54] According to it, the standard usability test is performed recording users' performance on an assigned task. In our test we showed to users a document explaining the CHINO framework, the Immunisation scenario and a list of identified requirements. We monitored and stimulated them to speak while performing the assigned tasks to analyse their behaviour.

Added " ' " -->

At the end of the test we asked them to fill a questionnaire about overall satisfaction about the assigned tasks which had two types of responses. The first one in a scale from 1 to 7 points where 1 correspond to negative opinion such as *Strongly Disagree* and 7 to a positive judgement such as *Strongly Agree*. The second type was in form of open questions. All the numeric questions were mandatory while the open ones were optional. We report some questions while the complete questionnaire including a detailed analysis of results can be found here[55]:

Q1 "Overall, I am satisfied with the ease of completing the exercise in this scenario."
Q10 "I was able to complete the exercise quickly using this system."
Q21 "This system has all the functions and capabilities I needed."
Q23 "It was easy to understand the concepts introduced by this framework."
Q25 "How do you rate the overall experience with the CHINO Modelling?"

16.4.5.1 Study Results

To evaluate the responses for each question we calculated the mean (μ_n) and variance ($\sigma_n{}^2$) where the first coefficient expresses the positive or negative opinion of the users, while the second represent the level of disagreement among users.

[53] Activiti BPM Platform, Available at http://activiti.org/.

[54] Helen Sharp, "Interaction design," (Wiley.com., 2003).

[55] Alessio Giori, "Design, development and validation of a methodology and platform for compliance-aware medical record management", Master's degree thesis at University of Trento, 2013.

Test showed a positive impression about the Modeller usage after a few times it has been used. However, when users used it for the first time some differences among opinions emerged. Only two users expressed an overall negative feedback about their performance, however, since they were able to perform their tasks, this does not represent an important limitation, although it suggests us to take into consideration developing a strategy to train new users.

Note: depending on the template, probably 350 and 351 should be quoted.

An example of a positive feedback within open questions is:

--> I am comfortable with the diagrams because it really represents the information which is held on hospitals.

And also some negative ones:

And also 353, 354, 355 -->

The framework as I said is easy to use but anyway I had some problems of stability during the usage, so for this reason, relatively to the question if I would recommend this tool to others the real answer is yes, but . . .

The stability issues are related to the Activiti Designer and not to our specific extension and it is just a matter of software maturity since Activiti project is being frequently updated with newer versions.

Overall, the study gave us important feedback about custom task usability and suggested some improvements especially regarding the explanation of their usage. Other suggestions include also the need for better explanation of usage of combinations of different tasks to achieve a specific goal. In conclusion, tests showed a satisfactory usability level of the Modelling Framework and demonstrated that users were able to transpose requirements into processes while underlining the need for smaller improvements of the CHINO platform.

Tests validated the technical usability and feasibility of the CHINO approach, while the next section analyses how CHINO achieves privacy law compliance.

16.5 Privacy Law Compliance with CHINO

Here we analyse CHINO from the legal point of view and reason about its ability to preserve privacy and data protection rights and to support compliant process definition. We show how CHINO can help in achieving the identified goals by answering in particular to the following two macro-questions:

1. If CHINO provides technological elements (modeller, modelling elements, internal components) to support the development of privacy law compliant healthcare data management processes and policies.
2. If CHINO process based approach could facilitate the tasks (emphasised in Fig. 16.5) of process and policy approvals or verifications. These activities are typically done before going into production phase or in case of legally motivated inspections by Compliance Officers at runtime.

In order to answer to the first question we summarize here how CHINO technology and, more in general, the process based approach it proposes, can satisfy

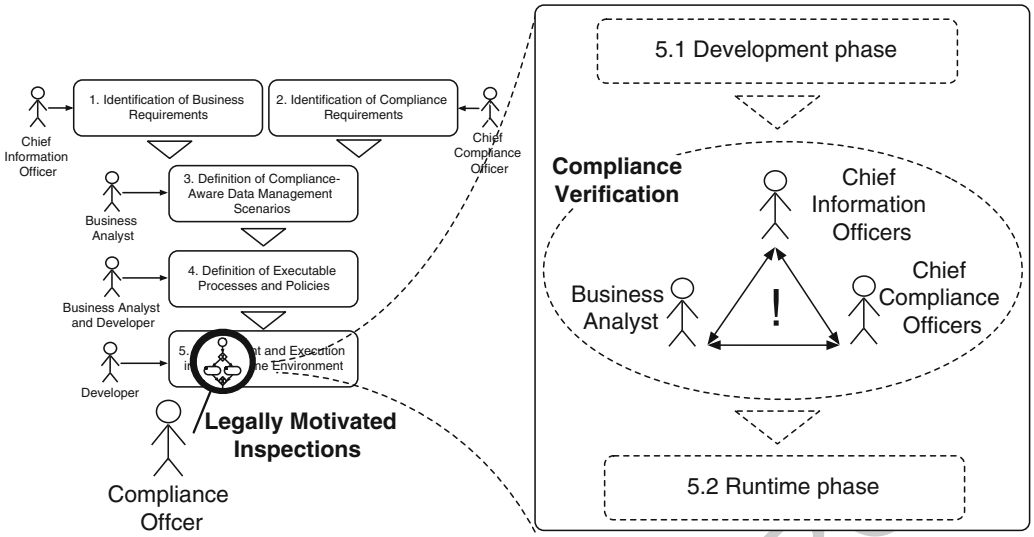

Fig. 16.5 CHINO Methodology with the focus on compliance inspections and verifications

the set of requirements extracted from the Italian legislation, directives and set of guidelines for the creation of Electronic Health Record (EHR) systems. We start by analysing the set of recommendations of the Art. 29 Data Protection Working Party in *Working Document 01/2012 on epSOS,*[56] and in *Working Document on the processing of personal data relating to health in Electronic Health Records (EHR).*[57] Art. 29 Working Party provides recommendations on several topics emphasising the need for special safeguards in order to guarantee the data protection rights of patients and individuals. Some recommendations include the respect for data subjects' self-determination and authorisation procedures, security measures, transparency, liability issues and finally, the availability of mechanisms to control the data processing.

As described in the paper, CHINO aims at providing a framework to support the privacy by design approach while providing tools and mechanisms to define data management processes and policies. In such way, CHINO proposes a proactive approach in accordance to the privacy by design principles by providing effective technical and organisational tools for healthcare institutions to consider privacy related aspects during the whole project lifecycle.[58]

[56] Article 29 Data Protection Working Party, *Working Document 01/2012 on epSOS*, Adapted on 25 January 2012, wp 189.

[57] Article 29 Data Protection Working Party, *Working Document on the processing of personal data relating to health in Electronic Health Records (EHR),* Adopted on 15 February 2007, wp 131.

[58] Ann Cavoukian, "Personal Data Ecosystem (PDE) – A Privacy by Design Approach to an Individual's Pursuit of Radical Control," In *Digital Enlightenments Yearbook 2013. The Value of Personal Data*, ed. Mireille Hildebrandt et al. (IOS Press, 2013), 89–101.

Analysing more deeply CHINO with the focus on data protection requirements, it appears to be an appropriate platform for sharing personal and healthcare data also among organizations that belong to different regulatory contexts.[59] The flexibility provided by business process technology enables users to customize data management processes and data protection strategy according to their requirements.

From the data security point of view, CHINO technology provides the necessary mechanisms to satisfy the security requirements related to healthcare data management in the Italian scenario. In particular, the architectural features and capabilities have been built following the national level guidelines for EHR creation[60] and international standards such as IHE.[61] Therefore CHINO satisfies the requirements according to Articles 31 and 33ff of the Italian Data Protection Code,[62] and the release of a Privacy Impact Assessment.[63] It implements technical and organisational features to avoid loss or unauthorised alteration, processing and access to data. Furthermore it respects data protection general principles from the Directive 95/46/EC, and in particular the principles of purpose limitation, proportionality, data quality, necessity and the data subject's rights.

CHINO is able to enforce the *explicit consent* policy that is defined as the data subjects' explicit consent on the processing of their data and it is an exemption to the general prohibition to personal data processing, according to European legislation (Art. 8, Directive 95/46/EC).[64] CHINO access right policies and the assurance mechanism enable data subjects to freely express explicit, specific and informed consent about data sharing. According to the legislation, in special cases data can be processed without consent (e.g. compliance with legal obligations, protect vital interest of data subject, public interests). This is possible in CHINO by defining special conditions on the *Check Access Right* modelling element. Processes can be also defined to delegate the disclosure of data to data subjects' personal doctors. Data subjects could also delete and block data sharing (as required for instance by Art. 7, Italian Data Protection Code). Moreover the involved actors are able to receive notifications about the process status, including the requests of access. The updates of wrong data to assure data quality policy according to Italian, European and HIPAA legislations, are done through the *Push Record* task.

[59] *Directive 2011/24/EU*.

[60] Italian Ministry of Innovation and Technology, *InFSE: Technical Infrastructure for Electronical Health Record Systems, v1.2*. (2012).

[61] Integrating the Healthcare Enterprise (IHE), "IHE IT infrastructure (ITI) technical framework", Integration Profiles, v. 8, (2011).

[62] *Legislative Decree No. 196/2003*.

[63] *European Parliament and Council: Proposal for a regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. (2012).

[64] Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, Adopted on 13 July 2011, wp 187.

According to European legislation (Art. 6 of Directive 95/46/EC) and to the Italian Data Protection Code (Art. 11), personal data can only be processed for specified explicit and legitimate purposes and may not be processed further in a way incompatible with those purposes. CHINO provides technical tools for enabling data controllers to check step-by-step the lawfulness of the personal data process following the purpose principle[65]; the legitimate purposes of the process are recorded and all the access requests are filtered according to them. CHINO provides mechanisms to release data only according to the specified, explicit and legitimate purposes through the definition of filtering policies. Namely, the CHINO filtering task provides anonymisation mechanisms to remove sensible information on a purpose-based approach. For example in case the data need to be used for statistical purposes, a filtering policy that eliminate personal identifiable information can be defined.[66] These purpose-based policies can be defined quite easily in healthcare domain given the availability of the taxonomy of possible purposes for which healthcare data can be requested and used.[67]

By analysing more deeply the data security features, CHINO guarantees confidentiality and integrity of information against unauthorised access, disclosure or alterations. Moreover, it improves personal data traceability, so that each communication and each data transaction can be tracked back to a certain entity that can be easily audited. In order to assure data traceability, CHINO provides features to clearly identify all the actors and entities involved in the process execution. This allows identifying data controllers and data processors (and other involved entities) when executing operations over data and addressing specific and defined liabilities to data controllers and processors at any step of the processing. Logging ensures accountability on operations over data in compliance with the Italian Data Protection Code (Articles 28ff) and with the Guidelines on the EHR development.[68]

CHINO allows data controllers to keep privacy-sensitive data on their own servers if they have restrictions about data storage administrative locations, as it is the case in Italy.[69] Regarding the data stored inside CHINO, it is encrypted with standards algorithms (e.g. AES-128 and SHA-258 for hashing). The deployment of CHINO could be done also in Cloud-based environments. Although this aspect

[65] Article 29 Data Protection Working Party, *Opinion 3/2013 on purpose limitation*, Adopted on 2 April 2013, wp 203.

[66] Giampaolo Armellin et al., "Privacy preserving event driven integration for interoperating social and health systems," *Secure Data Management 7th VLDB Workshop* (2010): 6368; Jovan Stevovic et al., "Business process management enabled compliance-aware medical record sharing," *Int. J. Business Process Integration and Management* (2013):6.

[67] Italian Ministry of Innovation and Technology, *InFSE: Technical Infrastructure for Electronical Health Record Systems, v1.2*. (2012).

[68] Italian Data Protection Authority, *Guidelines on the Electronic Health Record*.

[69] Italian Data Protection Authority, *Guidelines on the Electronic Health Record*.

needs a deeper analysis, the combination of the possibility to decentralise record storage and encryption techniques satisfy the requirements recommended by Art. 29 Working Party in 2007.[70]

Relatively to the second question, we tried to analyse the healthcare software lifecycle that is depicted in Fig. 16.5 with particular focus on the compliance aspects that have been underlined in two specific phases. Namely, Fig. 16.5 shows the situations where the "Chief Compliance Officer", that is usually a privacy expert or a Data Protection Officer, is involved in the verification of the business processes developed at Step 5 and has the responsibility to approve or reject them. The other situation is related to recent Inspection Plan undertaken by the Italian Data Protection Authority in which medical record systems has been included as one of the potentially analysed systems.[71] This means that the Data Protection Authority will seek for documentation to check if the data lifecycle and data management procedures are compliant with legislation in order to assure protection to data subjects' rights.

Both situations shown in Fig. 16.5, describe tasks that could have significant impact on projects developed without considering exhaustively privacy related aspects (i.e. fines to responsible organizations or, in extreme cases, systems suspension or disposal).

To answer to this question we focus on the analysis of the CHINO technology and understanding if it could provide more transparency, documentation and details about the data management lifecycle in case of verifications and inspections. We focus mainly on the analysis of the BPM technology, as the core innovative technology, that can facilitate inspection procedures. Due to its visual representations, CHINO data management operations can be easily verified even by people with non-technical background such as Compliance Officers. Similarly to other scenarios and context,[72] visual representations can simplify the process of revision by lawyer and privacy experts due to its simplification of understanding for people with non IT background. CHINO expresses in a more clear way which privacy requirements are satisfied when compared to standard textual documentation making easier to identify different steps and related rights, duties and liabilities.

[70] Article 29 Data Protection Working Party, *Working Document on the processing of personal data relating to health in Electronic Health Records (EHR),* Adopted on 15 February 2007, wp 131.

[71] Italian Data Protection Authority, *Newsletter about the Inspection Plan. February 14 2013*, Available at http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2256479.

[72] Rachel K. E. Bellamy et al., "Seeing is believing: designing visualizations for managing risk and compliance," *IBM System Journal* (2007): 46; Avner Ottensooser et al., "Making sense of business process descriptions: An experimental comparison of graphical and textual notations," *Journal of Systems and Software* (2012): 85; Jan C. Recker and Alexander Dreiling, "Does it matter which process modelling language we teach or use? An experimental study on understanding process modelling languages without formal education," in *18th Australasian Conference on Information Systems* (University of Southern Queensland, 2007).

16.6 Conclusions

Privacy law compliance is a challenging and complex goal to achieve while developing IT solutions that manage and share sensitive data. This paper shows how CHINO framework is able to tackle compliance issues in medical data sharing by exploiting the advantages of visual representations such as BPM technologies.

By performing different tests; starting with extracting policies from Italian, European and HIPAA legislations, modelling and executing corresponding processes and policies and with user studies, we have proved the overall CHINO methodology and technology applicability and its soundness relatively to Privacy by Design principles. From the privacy legislation analysis has emerged that CHINO provides all the necessary features to develop data management processes that are compliant with examined legislations. In addition, the BPM technology simplifies the process development and revision tasks that are done by Compliance Officers. The adoption of the same visual representations from the first stages of analysis up to the execution, simplifies the collaboration and sharing of knowledge among stakeholders with different backgrounds.

A potential evolution of the CHINO platform is the deployment on Cloud-based infrastructures to give to users the possibility to define their own data management strategies for their personal data. It could also enable users and organisations to share processes among them and collaboratively improve them.

Furthermore, the proposed solution, and in particular the positive validation with privacy experts, enabled us to apply the CHINO methodology (and potentially also the technology) into industrial projects. Namely, we are currently adopting the CHINO methodology and BPMN diagrams as the documentation technology to interact with stakeholders (i.e., analysts, assistance providers, governance and compliance experts from a legal consulting firm). The initial feedback about the proposed approach suitability is extremely positive and the reporting of these experiences will be part of the future work on this project.

References

Activiti BPM Platform, Available at http://activiti.org/.

AQ2 Armellin, Giampaolo, Dario Betti, Fabio Casati, Annamaria Chiasera, Gloria Martìnez, and Jovan Stevovic. "Privacy preserving event-driven integration for interoperating social and health systems." In *Proceedings of the 7th VLDB Conference on Secure Data Management, SDM'10,* 6368 (2010): 54–69.

Article 29 Data Protection Working Party, *Working Document 01/2012 on epSOS*, Adopted on 25 January 2012, wp 189. (2012)

Article 29 Data Protection Working Party, *Working Document on the processing of personal data relating to health in Electronic Health Records (EHR)*, Adopted on 15 February 2007, wp 131. (2007)

Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, Adopted on 13 July 2011, wp 187. (2011)

Article 29 Data Protection Working Party, *Opinion 3/2013 on purpose limitation*, Adopted on 2 April 2013, wp 203. (2013)

Article 29 Data Protection Working Party, *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, wp 168. (2009)

Awad, Ahmed, Rajeev Goré, James Thomson, and Matthias Weidlich., "An iterative approach for business process template synthesis from compliance rules." In *Advanced Information Systems Engineering, LNCS* 6741 (2011): 406–421

Balboni, Paolo, and Milda Macenaite. "Privacy by Design and anonymisation techniques in action: Case study of Ma^{3}tch technology." *Computer Law and Security Review* 29, (4) (2013): 330–340

Bellamy, Rachel K. E., Thomas Erickson, Brian Fuller, Wendy A. Kellogg, Rhonda Rosenbaum, John C. Thomas, and Tracee Vetting Wolf. "Seeing is believing: designing visualizations for managing risk and compliance." *IBM System J.* 46(2) (2007): 205–218

Breaux, Travis D, Matthew W. Vail, Annie I. Anton. "Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations." In *Requirements Engineering, 14th IEEE International Conference* (2006): 49–58

Cavoukian, Ann, "Privacy by Design." Information & Privacy Commissioner, Ontario, Canada http://www.ipc.on.ca/images/Resources/privacybydesign.pdf. (2009)

Cavoukian, Ann, "Privacy in the Clouds." *Identity in the Information Society* 1(1) (2009): 89–108

Cavoukian, Ann "Personal data Ecosystem (PDE) – A Privacy by Design Approach to an Individual's Pursuit of Radical Control." In *Digital Enlightenment Yearbook 2013: The Value of Personal Data*, edited by Mireille Hildebrandt et al., 89–101. IOS Press: 2013

European Parliament and Council: Directive 95/46/EC: Directive on protection of individuals with regard to the processing of personal data and on the free movement of such data

European Parliament and Council: Directive 2011/24/EU: Directive on the application of patients' rights in cross-border healthcare

European Parliament and Council: Proposal for a regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

epSOS European eHealth project, http://www.epsos.eu/

Gordon, David G., and Travis D. Breaux. "Reconciling multi-jurisdictional legal requirements: A case study in requirements water marking." *Requirements Engineering Conference*, IEEE, 2012.

Hillestad, Richard, James Bigelow, Anthony Bower, Federico Girosi, Robin Meili, Richard Scoville, and Roger Taylor. "Can electronic medical record systems transform health care? Potential health benefits, savings, and costs." *Health Affairs* 24(5) (2005) 1103–1117

Integrating the Healthcare Enterprise (IHE), "IHE IT infrastructure (ITI) technical framework", Integration Profiles, v. 8, (2011)

Italian Data Protection Authority. *Guidelines on the Electronic Health Record and the Health File*, [doc. Web 1634116] July 16, 2009, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1634116

Italian Data Protection Authority. *Newsletter about the Inspection Plan. February 14 2013*, Available at http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2256479

Italian Ministry of Innovation and Technology. *InFSE: Technical Infrastructure for Electronical Health Record Systems, v1.2.* (2012)

Legislative Decree No. 196/2003

Koops, Bert-Jaap, and Leenes, Ronald. "Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law." *International Review of Law, Computers & Technology* (2013): 1–13.

Kung, Anthony, Johann C. Freytag, and Frank Kargl. "Privacy-by-design in its applications." In *IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM),* IEEE. 1–6.

Lenz, Richard, and Manfred Reichert. "It support for healthcare processes premises, challenges, perspectives." *Data Knowledge Engineering* 61(1) (2007): 39–58

Lu, Ruopeng, Shazia Sadiq, and Guido Governatori. "Compliance-aware business process design." *BPM Workshops* 4928 (2008): 120–131

Milosevic, Zoran, Shazia Sadiq, and Maria E. Orlowska. "Translating business contract into compliant business processes." In *EDOC'06*, 211–220, IEEE Computer Society, 2006

Municipality of Trento. *Regulations for the protection of personal data of the municipality of Trento*. http://www.comune.trento.it/, 2007. Accessed: 2013-12-20.

Municipality of Trento. *Operational guidelines to privacy*. http://www.comune.trento.it/, 2009. Accessed: 2013-12-20.

Office for Civil Rights. *HIPAA, medical privacy national standards to protect the privacy of personal health information*, 2000

OMG. *BPMN - Business Process Model and Notation v2.0 Specification* (2011), Available at http://www.omg.org/spec/BPMN/2.0/.

Ottensooser, Avner, Alan Fekete, Hajo A. Reijers, Jan Mendling, and Con. Menictas. "Making sense of business process descriptions: An experimental comparison of graphical and textual notations." *Journal of Systems and Software* 85(3) (2012): 596–606

Pagallo, Ugo. "On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law". *European Data Protection* 2012: 331–346

Practice Fusion, *Free Web-based Electronic Health Record*, www.practicefusion.com.

Recker, Jan C., and Alexander Dreiling. "Does it matter which process modelling language we teach or use? An experimental study on understanding process modelling languages without formal education." In *18th Australasian Conference on Information Systems*, University of Southern Queensland, (2007).

Schaar, Peter."Privacy by Design." *Identity in the Information Society* 3(2) (2010): 267–274

Siena, Alberto, Giampaolo Armellin, Gianluca Mameli, John Mylopoulos, Anna Perini, and Angelo Susi. "Establishing regulatory compliance for IS requirements: an experience report from the health care domain." *29th Int. Conf. on Conceptual Modelling*, 6412 (2010): 90–103

Sharp, Helen. "Interaction design." Wiley.com. (2003)

Stevovic, Jovan, Jun Li, Hamid Motahari-Nezhad, Fabio Casati, Giampaolo Armellin. "Business process management enabled compliance-aware medical record sharing." *Int. J. Business Process Integration and Management* 6(3) (2013): 201–223

The Guardian, *NHS staff breach personal data 806 times in three years*, 2011, Available at: http://www.theguardian.com/healthcare-network/2011/oct/28/nhs-staff-breach-personal-data-806-times. Accessed on January 2014.

AUTHOR QUERIES

AQ1. Please confirm the inserted affiliation for all authors.
AQ2. None of the references are cited in text. Please check.