uOttawa

L'Université canadienne
Canada's university

FACULTÉ DES ÉTUDES SUPÉRIEURES ET POSTOCTORALES

uOttawa

L'Université canadienne
Canada's university

FACULTY OF GRADUATE AND POSDOCTORAL STUDIES

Sepideh Ghanavati
AUTEUR DE LA THÈSE / AUTHOR OF THESIS

M.Sc. (Systems Science)
GRADE / DEGREE

Department of Systems Science
FACULTÉ, ÉCOLE, DÉPARTEMENT / FACULTY, SCHOOL, DEPARTMENT

A Compliance Framework for Business Processes Based on URN

TITRE DE LA THÈSE / TITLE OF THESIS

Dr. Liam Peyton
DIRECTEUR (DIRECTRICE) DE LA THÈSE / THESIS SUPERVISOR

Dr. Daniel Amyot
CO-DIRECTEUR (CO-DIRECTRICE) DE LA THÈSE / THESIS CO-SUPERVISOR

EXAMINATEURS (EXAMINATRICES) DE LA THÈSE / THESIS EXAMINERS

Dr. A. El Saddik

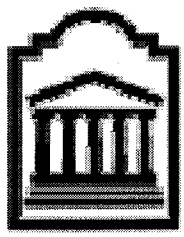
Dr. T. Lethbridge

Gary W. Slater
Le Doyen de la Faculté des études supérieures et postdoctorales / Dean of the Faculty of Graduate and Postdoctoral Studies

A Compliance Framework for Business Processes Based on URN

Sepideh Ghanavati

Thesis submitted to the
Faculty of Graduate and Postdoctoral Studies
In partial fulfillment of the requirements
For the M. Sc. degree in Systems Science



University of Ottawa
Ottawa, Ontario, Canada
May 2007

Your file Votre référence
ISBN: 978-0-494-32448-6
Our file Notre référence
ISBN: 978-0-494-32448-6

Dedication

To my parents Shahpar and Mehdi and my sister Sahar.

Abstract

Compliance with institutional policies, government regulations and applicable legislation is a major concern for any organization when defining its business processes. These regulations are usually complex, hard to understand, and they rarely come with a model or taxonomy. As well, both business processes and regulations are susceptible to change with the potential of introducing non-compliance. This thesis presents a framework that intends to help companies track compliance by leveraging requirements engineering models. Compliance is managed by establishing links between User Requirements Notation (URN) models of government legislation and organizational business process and tracking how they are affected in a requirements management system. Special attention is paid to maintaining compliance as either the legislation or business processes evolve over time. The framework is evaluated by way of a case study from the healthcare industry. The case study centres on the approval process implemented to control access to a data warehouse at a major Ontario hospital and whether or not this process complies with relevant legislation and hospital guidelines. The relevant legislation in Ontario is the new provincial Personal Health Information Privacy Act (PHIPA).

Acknowledgment

I would like to thank my supervisors, Dr. Liam Peyton and Dr. Daniel Amyot, for their guidance, support, comments and encouragement. Their advice greatly improved the quality of this thesis and I am very fortunate to have been supervised by them. The work presented here was supported by the Ontario Research Network for Electronic Commerce (ORNEC) and by Telelogic (who provided tools) and could not have been completed without their help. I would also like to thank my family and friends who stood by me throughout my studies.

Table of Contents

List of Figures

List of Tables

List of Acronyms

Acronym	Definition
ACP	Access Control Policies
AI	Artificial Intelligent
AMR	American Medical Research
BPM	Business Process Modeling
C-GRID	Compliance Global Regulatory Information Database
DOORS	Dynamic Object-Oriented Requirements System
DXL	DOORS eXtension Language
GRL	Goal-oriented Requirement Language
HIPAA	Health Insurance Portability and Accountability Act
IT	Information Technology
ITU-T	International Telecommunication Union - Telecommunication
NFR	Non-Functional Requirements
OMG	Object Management Group
ORCA	OMG Regulatory Compliance Alliance
PHI	Personal Health Information
PHIPA	Personal Health Information Privacy Act
ReCAPS	Requirement-based Access Control Analysis and Policy Specification
PIPEDA	Personal Information Protection and Electronic Documents Act
RMS	Requirements Management System
UCM	Use Case Maps
URN	User Requirements Notation

Chapter 1. Introduction

1.1. Problem Statement

Compliance with institutional policies, government regulations and applicable legislation is of primary concern for any organization when defining its business processes. Organizations strive to improve the quality of the products and services they provide. To achieve this goal, they need to have their processes and services generate data for management purposes. However, since this data is sensitive in nature and can contain personal information, access to it must be carefully controlled and monitored to ensure compliance with institutional guidelines, government regulations and relevant legislation. The cost of compliance management is usually high and every year this cost keeps increasing. As AMR Research stated in a recent report [1], the total spending on compliance management is expected to rise to 29.9 billion in 2007, which is about 8.5% higher than in 2006.

Governments have established rules and passed legislation to protect the privacy of personal information and organizations are obliged to comply with these laws. They are also aware that any violation of these laws comes with a large financial penalty. Organizations, therefore, have every intention of complying with these laws and regulations but can fail in this capacity because of the following reasons:

- difficulty in understanding imposed regulations;
- privacy law is new and is sensitive to amendment;
- organization's business processes are likely to change with the introduction of more IT-based solutions or evolving business contexts; and
- a lack of guidelines and tools to support compliance.

Each of these problems needs to be addressed by management as they are the ones who must manage the business processes and ensure compliance with legislation.

From the existence of these problems comes the need for a method to help organizations maintain compliance with laws and regulations. In order to ensure this compliance, organizations must:

- formalize their business processes;
- derive a relevant set of rules and obligations from the law; and
- establish links between these regulations and their business processes.

When these items are in place, organizations can implement mechanisms to ensure that they remain compliant with legislation and regulations even as they change.

1.2. Motivation and Objectives

The motivation for this work is to help organizations leverage their information technology assets while still ensuring they comply with existing laws, regulations and guidelines. This requirement is especially difficult to resolve given that an organization's business processes and privacy laws are both complex and susceptible to change. Thus, we are motivated to develop a framework that will help guarantee that an organization's business processes comply with legislation even as either of these elements change over time.

The main objectives of this work are to provide organizations with a set of guidelines to help track compliance between their business processes and legislation, ensure that their goals and processes are aligned with published regulations and help them maintain compliance to all applicable laws in the face of possible change or amendment. In addition, these guidelines aim to provide a solution that will help organizations reduce the cost and effort of auditing the compliance of business processes with legislation.

The framework introduced in this thesis is a requirements management framework which helps model regulatory and legislative texts in User Requirement Notation (URN). The framework also serves to connect privacy law to business processes, thus enabling an organization to document and track compliance with legislation as either the legislation or the business processes evolve.

1.3. Thesis Contribution

In this thesis, the following contributions, related to the handling of compliance to privacy laws and regulations, are made:

1. A requirements-oriented framework to aid in the understanding of legislative compliance for business processes, particularly in the area of healthcare.

2. A URN-oriented meta-model that defines a new set of compliance links for modelling the legislative compliance of business processes.
3. A systematic method for managing compliance as legislation or business processes evolve. This method is based on URN compliance links between two URN models and external documents.
4. Enhancements to existing tools (jUCMNav and Telelogic DOORS) to support and validate these contributions.

Most of the above contributions have been published in the following papers:

- Ghanavati, S., Amyot, D., and Peyton, L.: Toward a Framework for Tracking Legal Compliance in Health Care. *Proceedings of the 19th International Conference on Advanced Information Systems Engineering (CAiSE'07)*, Trondheim, Norway, June 2007, Springer.
- Ghanavati, S., Amyot D., and Peyton, L.: A Requirements Management Framework for Privacy Compliance. *Proceeding of the 10th Workshop on Requirements Engineering (WER07)*, Toronto, Canada, May 2007, 149-159.
- Peyton, L., Ghanavati, S., and Amyot, D.: Designing for Privacy Compliance and Performance Management in Health Care. To appear in: *The International Journal of Design Principles and Practices*, Common Ground, 2007.

1.4. Thesis Organization

This thesis is organized as follows. In Chapter 2, we introduce the necessary background material, which includes a description of privacy legislation and laws, URN notation, GRL and UCM models, and tool support for these models. In Chapter 3, we formalize the compliance framework by presenting the types of documents, the framework architecture, and the meta-model developed and the different types of links used. Chapter 4 follows with the methodology implemented to handle both business processes and legislative changes. In Chapter 5, we present a detailed case study of our framework in practice and discuss how it compares to the original paper-based approach in terms of how it models privacy compliance and handles change. We then analyze the different approaches studied in Chapter 6 in terms of the effort required to model, document, and manage. We also

look at the amount of coverage provided by the model, the documentation and the changes to business processes and legislative documents. Finally, we present our conclusions in Chapter 7.

Chapter 2. Background

We present in Section 2.1 an overview of the different privacy laws and their principles. In Section 2.2, we detail the User Requirement Notation and in Section 2.3, we briefly describe how business processes can be modeled with it. Section 2.4 provides an overview of a requirements management system and finally in Section 2.5, we present a review of the work related to modeling legislation and managing compliance.

2.1. Legislation, Laws and Privacy

The collection and processing of information has become easier and faster due to the growth of new technologies and the internet. However, sometimes the data is personal and comes with restrictions on its collection and use. Its privacy must be protected by the collecting entity or data custodian. Among the possible types of personal information, health data is especially sensitive since it can contain information about a person's family history, disease and treatment history, genetic makeup, mental health, and/or sexually transmitted diseases. Accidental disclosure of this information can result in embarrassment, ruin or damage to the individual's career (dismissal from employment or loss of job opportunity), damage to or loss of health insurance eligibility, financial loss and disruption of privacy [31]. Therefore, many individuals are concerned about their information and its protection from misuse and confidentiality.

In response to these concerns, many national and international privacy laws have been established such as The European Union Data Protection Directive, Personal Information Protection and Electronic Documents Act (PIPEDA) and Personal Health Information Privacy Act (PHIPA) in Canada and Health Insurance Portability and Accountability Act (HIPAA) in the United States.

2.1.1 European Union Privacy Legislation

The *European Union Data Protection Directive* [8][17] was adopted in 1995 and took effect in 1998. This Directive applies to any kind of processing of personal data, automatic, semi-automatic or not automatic. The EU Data Protection Directive contains eight basics principles which are:

1. *Data Quality.* Personal data must be processed fairly and lawfully, be collected for specified and legitimate purposes, be adequate, relevant, accurate and up to date, and be kept identified no longer than what is necessary for the purpose of its collection or processing.
2. *Legitimization of Data Processing.* Personal data can only be processed if it has the data subject's consent, and the processing of the data is necessary for the performance of a contract, compliance with legal obligation, protection of the vital interest of the subject, etc.
3. *Particular Categories of Processing.* The processing of personal data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or which relates to the health or sex life of an individual is prohibited.
4. *Information Rights.* Specifies the rights of the data subject. For example, he has the right to be informed about data that is collected from him.
5. *Rights of Access for the Person Concerned.* The data subject is guaranteed certain rights to access to his own personal information which was obtained by the legal person.
6. *Right of Opposition of the Person Concerned.* The data subject has the right to object freely to the processing of his personal information which the controller intends to use for direct marketing.
7. *Confidentiality and Security of Processing.* Controllers and processors who access personal data must not process it except on instructions from the controller, unless required by law to do so.
8. *Transfer of Personal Data to Outside Countries.* Personal data can be transferred outside the European Union only if its protection is guaranteed.

2.1.2 United States Privacy Legislation

Unlike the European Union, the United States does not have an integrated and comprehensive privacy law to protect personal information in general, but there is legislation that addresses personal health information. The Department of Health and Human Services established HIPAA in 1996 for healthcare organizations [33]. HIPAA has two titles: Title I intends to protect health insurance coverage for workers and their families; and Title II (the Administrative Simplification) specifies the requirements for the establishment of national standards for electronic healthcare transactions and for national identifiers for providers, health plans, and employers [34]. HIPAA includes seven principles [27] which are:

1. *Quality and Availability of Care.* HIPAA rules should not interfere with the quality of healthcare delivery and should not threaten the financial stability of healthcare organizations.
2. *Notice.* The patient has a right to know about the information kept and the way it may be used or disclosed.
3. *Minimum Necessary.* Only the minimum necessary of a patient's information should be used by personnel of healthcare organizations.
4. *Onward Transfer.* The patient is the owner of his confidential information and has the right to control its use and disclosure.
5. *Data Security/Privacy/Integrity.* Confidential patient information has to be protected from unauthorized alterations by those who store, process and use them.
6. *Access.* The patient has the right to examine his personal information to ensure its accuracy and completeness and ask for its corrections.
7. *Enforcement.* The patient has the right to address any privacy violation. Healthcare organizations must prevent and detect any privacy breach of personal data.

2.1.3 Canada Privacy Legislation

In Canada, the PIPEDA is a federal legislative act that protects personal electronic information. PIPEDA has been recognized by the European Commission as being compliant

with the European Union Data Protection Directive on Privacy and Electronic Communication [7]. PIPEDA includes ten principles that any organization who wants to collect, use or disclose personal information for a commercial activity must comply with. These principles are:

1. *Accountability.* Organizations are accountable for the personal information which they have under their control and custody.
2. *Identify Purpose.* Organizations must identify the purpose for which the personal information is being collected prior to its collection.
3. *Consent.* Information can only be collected with the knowledge and consent of the individual
4. *Limiting Collection.* The collection of personal information is limited to what is necessary. Data collection must be done lawfully
5. *Limiting Use, Disclosure & Retention.* Information can only be used and disclosed for the purposes identified prior to collection and will only be retained as long as it is required for the purpose.
6. *Accuracy.* Information must be accurate, complete and up-to-date.
7. *Safeguards.* Information must be protected by adequate safeguards.
8. *Individual Access.* An individual must have the right to access, review and correct his personal information
9. *Challenge Compliance.* An organization must provide the means for an individual to challenge the organizations' compliance.
10. *Openness.* The privacy policies of an organization must be available to the public [16].

PIPEDA is general and refers to any kind of personal information including health information. However, most of the provinces such as Ontario have established their own laws to specifically protect personal health information. In Ontario, PHIPA has been in effect since 2004 to protect the privacy and confidentiality of personal health information. Any healthcare organization in Ontario which complies with PHIPA is exempt from applying Part 1 of PIPEDA [11]. PHIPA establishes a set of rules pertaining to the collection, use and disclosure of personal health information with the goal of protecting the privacy of the individual, i.e. the patient, and the confidentiality of his data. PHIPA is based

on the same 10 principles of PIPEDA explained above and hospitals and healthcare organizations must follow them when engaged in the collection, use or disclosure of personal health information [21].

2.2. User Requirements Notation

The User Requirements Notation is a draft ITU-T standard that combines goals and scenarios in order to help capture, model and analyze user requirements in the early stages of design [18]. It can be applied to describe most kinds of reactive and distributed systems as well as business processes. URN is suitable for applications ranging from goal modeling and user requirements to high-level design. It helps software engineers define requirements for a proposed or evolving system and express the relationship between goals and system requirements [2]. URN is expected to help engineers reduce development costs, decrease product delivery time and increase customer satisfaction.

URN is composed of two complementary notations: Goal-oriented Requirement Language (GRL) and Use Case Maps (UCM). These notations together connect goals and business processes. GRL is used to model business objectives, rationales, tradeoffs, and non-functional aspects (the "why" aspects) while UCM focuses more on architectures and functional or operational aspects of business processes (the "what" aspects).

2.2.1 Goal-oriented Requirement Language

The Goal-oriented Requirement Language (GRL) is a goal modeling notation based on the Non-Functional Requirements (NFR) framework. GRL combines components of the NFR framework with those of the i* framework [26]. In particular, it applies the syntax of the i* framework (i.e. actors, intentional elements and links) with the NFR framework's evaluation mechanism (i.e. qualitative labels associated to lower-level intentional elements to measure the degree of satisfaction for the high-level intentional elements). GRL is used to support requirements analysis tasks especially for non-functional requirements, by capturing business or system goals and demonstrating alternative ways of achieving those goals. GRL focuses on "why a certain behaviour or goal was chosen", "what alternatives have been considered" and "what are the criteria in selecting an alternative over others" [2][14].

GRL is a graphical notation composed of concepts such as goals, softgoals, and tasks (solutions) collectively called intentional elements. Such elements can be connected to each other via links. These links represent different types of relationships such as contribution, correlation, and decomposition.

A softgoal is a kind of goal that can never be concretely achieved. For example in Figure 1 *Prevent unauthorized disclosure* is a softgoal. This type of goal represents a high-level goal for the system. Softgoals are indicated as cloud shapes and can be linked by contribution or decomposition links. Contribution links can have different levels of effect on the softgoals connected to them. Links of type *make*, *help*, and *some+* indicate positive relationships that are respectively sufficient, insufficient and unknown. Those links that are labelled as *break*, *hurt* and *some-* are used for negative contributions that are sufficient, insufficient and unknown. At times, some goals do not directly contribute to others but still have a positive or negative side-effect. These side-effects are shown using correlation links. This type of link can also be assigned a weight to indicate the relative importance of the impact.

Goals, related to the business or the system, represent the conditions which must be achieved with certainty, e.g. *Limit disclosure to certain people.* Both softgoals and goals are decomposed until they are operationalized into tasks. Tasks represent the operational solutions to the system and are shown as hexagons. Tasks are usually decomposed, using decomposition links, into several sub-components such as tasks, goals or softgoals themselves. Although decomposition links are mainly used for tasks, they can also be used for other types of intentional elements. Actors are the only active entities in GRL that carry out actions (usually tasks) to reach goals. For example, in Figure 1, the hospital (actor) is in charge of the task *Ask for a research plan.*

Beliefs, modeled as ellipses, represent the rationales used to justify or explain links. This type of element is useful in stakeholder meetings when there is disagreement over a particular link.

Figure 2 provides a summary overview of the GRL notation elements.

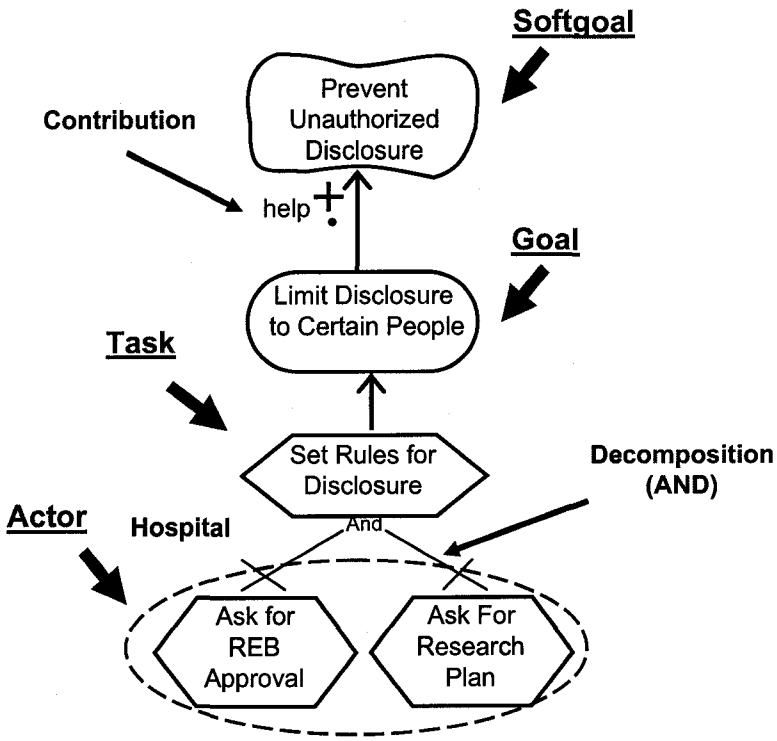


Figure 1 GRL Example

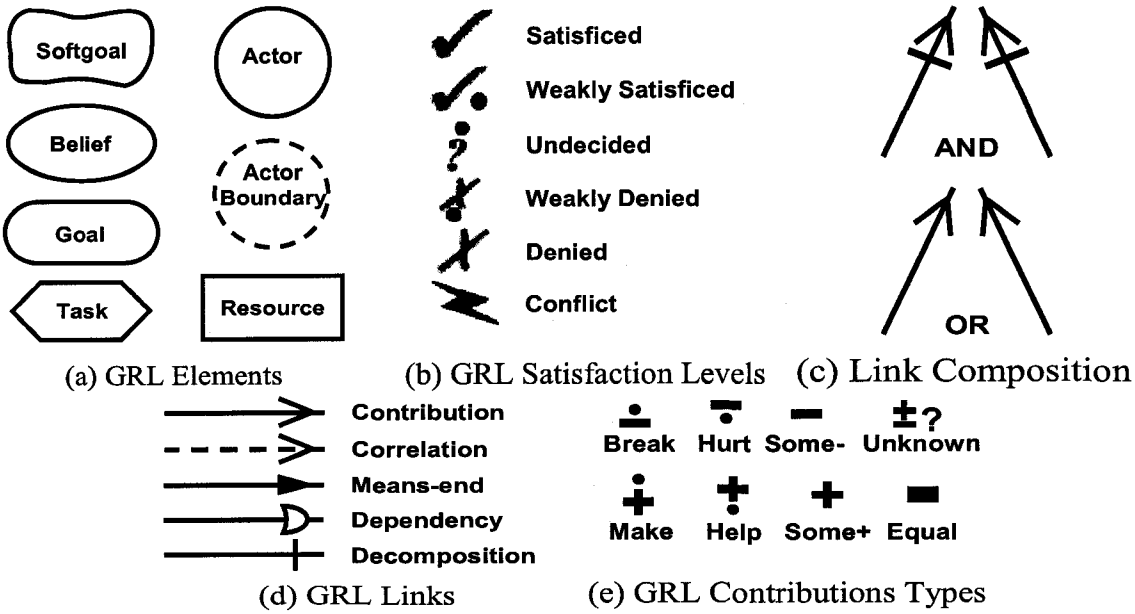


Figure 2 Summary of the GRL Notation

2.2.2 Use Case Maps

Use Case Maps (UCMs), a scenario-based notation, is the second part of URN that focuses mainly on the functional requirements of a system and the causal relationships between the responsibilities of different use cases. Functional requirements define the functions and operations of the system and are usually captured in the form of use cases and scenarios. UCMs help bridge the gap between requirements and the design stage and can be applied in different situations such as with use case capture and elicitation, use case validation and test case generation [2].

UCM models often start with a top-level map called a root map and are applied to depict scenarios. In UCM, scenarios or partial descriptions of a system are represented as paths. Scenarios, as shown in Figure 3, evolve and progress along paths from the start points (filled circles) to end points (perpendicular bars). Start points capture preconditions and triggering events while end points capture post-conditions and resulting events. A scenario activity or responsibility is used to transfer an input to an output while satisfying the preconditions and post-conditions. They come in the form of operations, actions, tasks, and functions and are represented by crosses along the path [2][36]. The responsibility, *fillOutForm*, in Figure 3 is an example of such an element. Responsibilities can be associated with components in UCMs. Components are generic or abstract entities that can either represent software elements such as objects, processes, databases, and servers or non-software elements such as actors and hardware resources. Components are illustrated as rectangles, have names and attributes and a type such as agent, team or actor. Agent and actor components represent actors in GRL. For a given map, only the components that are involved in that part of the process need to be shown. In Figure 3, *researcher* is an actor component and *hospital* is an agent component.

UCMs allow for some scenarios to be repeated in different parts of the process. As such, some maps can be involved in more than one use case. With the ability to encapsulate scenarios, there is the potential for maps to be complex. In order to apply the same map in different parts and keep the level of complexity low, we can define maps as sub-maps using stubs and plug-ins. Diamond symbols in the top level map are called stubs and are used as containers for those sub-maps. As a result, these sub-maps are called plug-in maps. An example of a stub is shown with the *submitDocuments* element

in Figure 3. Stubs are connected to the start and end points of the plug-in map by their input and output segments (IN1, OUT1, ...). This binding relationship ensures that the integrity of the path from the parent map to the sub-map, and back to the parent map is maintained. There are two types of stubs: Static Stubs and Dynamic Stubs. Static stubs only include one plug-in map while dynamic stubs can contain several sub-maps. For dynamic stubs, the sub-map followed is decided based on existing preconditions. The preconditions are collectively referred to as the selection policy [2][36].

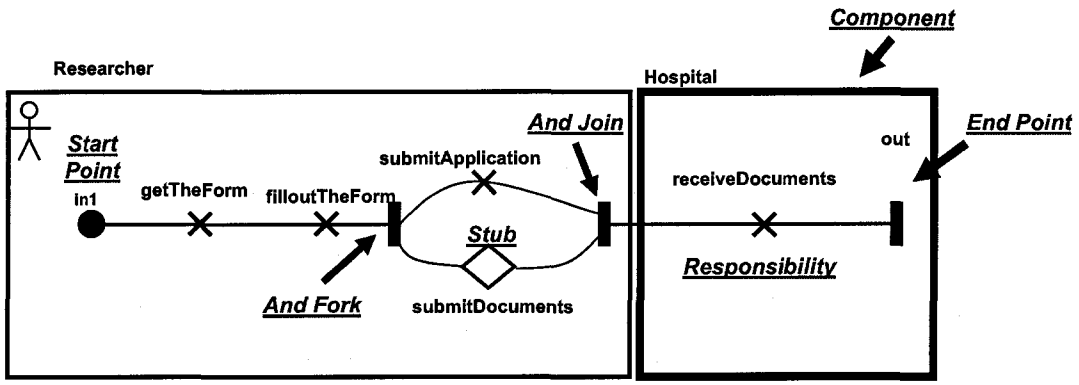


Figure 3 UCM Example

Sometimes as part of a scenario, certain activities are presented as alternatives and performed on condition. These conditions are called guard conditions and are indicated with square brackets. Thus, when a path is split into two or more paths via an OR-fork, the path that is taken is the one for which the guard condition is true. In other cases, the paths are shared and are joined with an OR-join. Conversely, there is also the need to model concurrency in a scenario. The concept of concurrency is supported with AND-fork and AND-join elements. All of the resultant paths in an AND-fork have to be followed in order to proceed with the remainder of the scenario.

There is also a provision in UCM to model the concept of delay. This delay is indicated with waiting places (filled circles on a path) and timers (clock symbols). The wait time is complete when the waiting place or timer receive an event from external entities that exist as part of the environment or as entities in other UCM scenarios. If no event is triggered during a pre-specified amount of time, the timer will stop and its timeout path is taken instead. The timeout path is indicated by a zigzag symbol.

An overview of the UCM entities is provided in Figure 4.

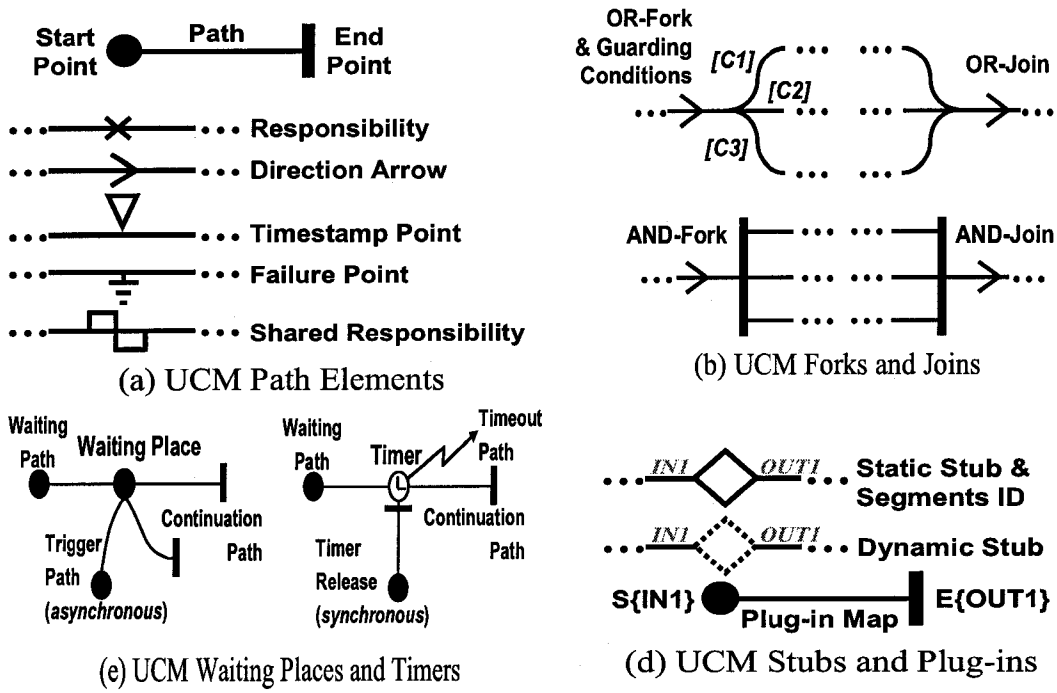


Figure 4 Summary of the UCM Notation

2.2.3 Links between GRL and UCM Models

URN combines goals and scenarios (business processes) by providing traceability links between GRL and UCM models. GRL intentional elements such as goals and tasks can be linked to UCM elements such as responsibilities, path segments, components, or plug-in maps. In GRL, softgoals and goals will refine to tasks and these tasks will refine to responsibilities in UCM. This type of link is used to explain *why* certain scenarios and responsibilities exist (rationale). It also describes the activities in UCM that have to be done for a specific business goal (refinement). An explanation of how goals and scenarios can be integrated in URN using the jUCMNav tool (described the next section) is provided in [25][26].

2.2.4 Tools Support – jUCMNav

jUCMNav is a Java-based Use Case Map (UCM) editor. It is designed as a plug-in to the Eclipse IDE [1][30]. It allows the user to create, load, modify and save a UCM model.

The editor also supports defining GRL models as well as creating links between the elements of a GRL model and a UCM model. It also has an export filter component that can be used to export and maintain GRL and UCM elements in the Telelogic DOORS requirements management system (described in Section 2.4.1 below), including internal links [20]. Figure 5 illustrates both the UCM and GRL views provided in jUCMNav.

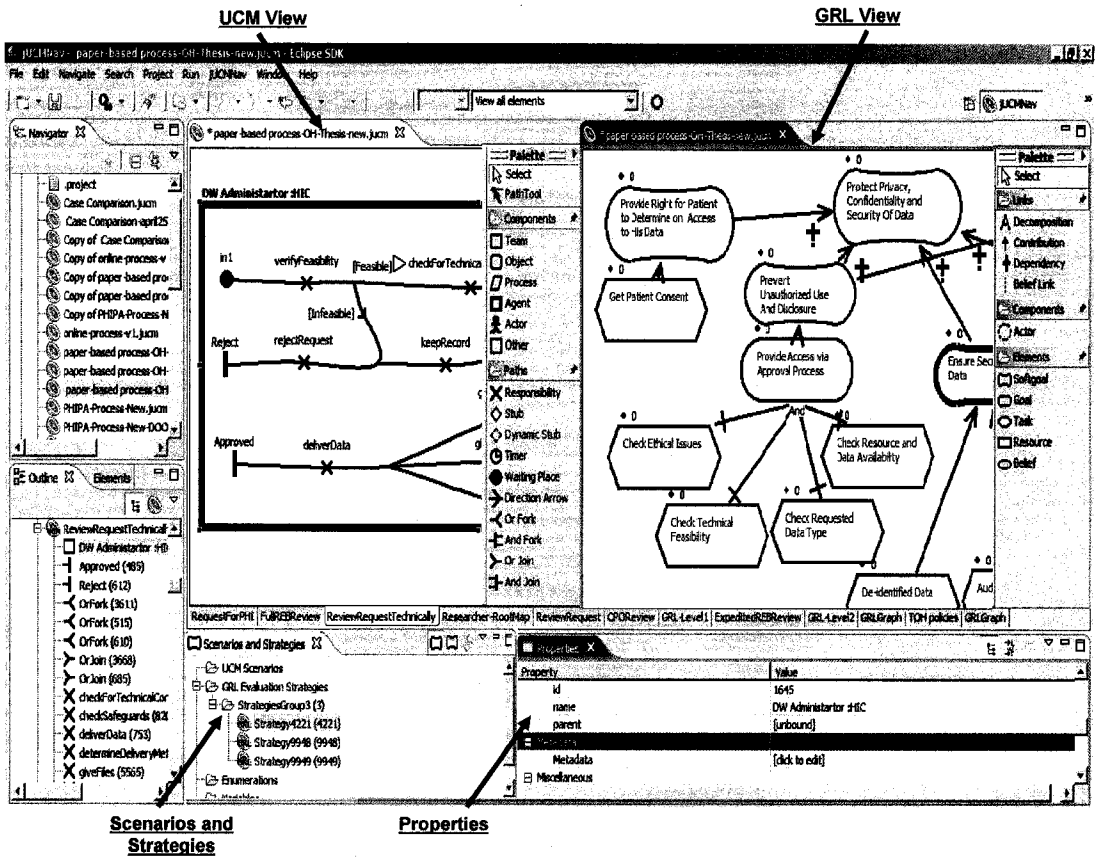


Figure 5 jUCMNav View

jUCMNav also supports UCM scenarios to help analyze and test the UCM model. It also supports GRL strategies, used to evaluate the global impact of the various sets of alternatives that can be taken in a GRL model.

2.3. Business Process Modeling and URN

Business process modeling (BPM) is a structured method used by an organization to represent its current and planned business processes. This representation establishes a basis for improving the mechanisms used to achieve business goals while taking into consideration the interests of the various stakeholders [5][28].

BPM methods aim to answer the "W5" questions of "Why do this activity?", "What should this activity be precisely?", "Who is involved in this activity?", "Where and when should this activity be performed?" [35].

In [35], the authors illustrate how GRL and UCMs (the components of URN) can answer these questions and be effective in modeling business processes and goals while including stakeholders in the modeling process. In other words, GRL helps to:

- Model the risks and benefits for different alternative business processes;
- Model the dependencies between all participants; and
- Refine high-level business goals into high-level tasks and/or low-level UCM responsibilities, scenarios and plug-ins.

The different roles involved can be defined by UCM components and GRL actors. UCM models enable us to define how responsibilities are allocated to the different business components, as well as how they are arranged temporally via constructs for expressing sequence, choices, concurrency, and synchronization.

2.4. Requirements Management System

A requirements management system (RMS) is a tool used to collect, organize and link requirements in a database to improve collaboration and communication between various stakeholders. It includes a change management component that provides support for evolving requirements. An RMS uses links to represent relationships between requirements. These links help to analyze the impact of change and monitor the level of conformance to the stakeholders' needs. In our work, we extend an RMS, Telelogic DOORS, and use it to track the compliance of business processes with regulations and laws.

In this section, we first introduce the tool we employed in our work, namely Telelogic DOORS [29]. We then describe how URN models can be integrated with

DOORS via jUCMNav to support linkages to external models and to monitor requirements change.

2.4.1 Telelogic DOORS

Telelogic DOORS is a requirement management system that is generally considered to be the market leading tool in the area of requirements management. Other comparable commercial tools include IBM Requisite Pro, Borland Caliber-RM and Analyst Pro. DOORS supports text, diagram, and document objects. There is also support for user-defined scripts or automatic links to support traceability between these objects.

DOORS uses a database to store data including folders and projects. These folders and projects contain formal and link modules. Formal modules are files which contain textual or graphical requirements. Formal modules are composed of objects, their attributes and views of objects. Figure 6 presents part of a DOORS database view.

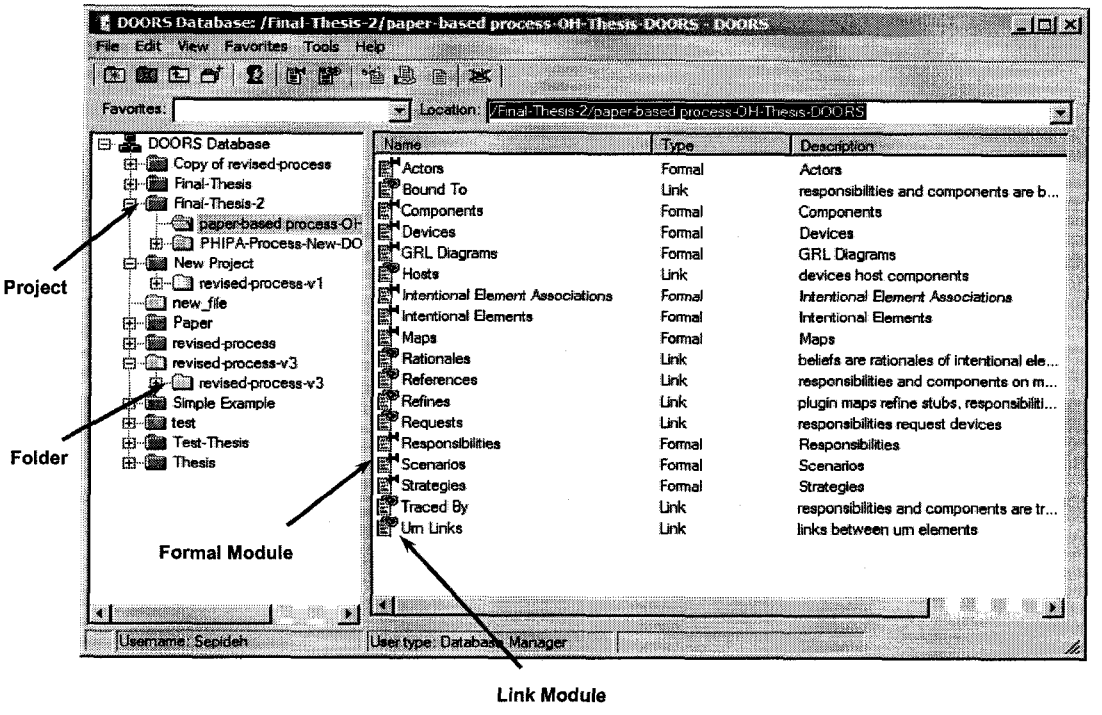


Figure 6 DOORS Database View

Links represent the relationships between source and target objects. Link modules keep track of links of a given type. Traceability is handled by storing some link informa-

tion in the source object. This ensures that if an object with incoming links is deleted, all its incoming links are also deleted first. When an object is modified, all of the objects to which it is connected are flagged as suspect links to indicate that these objects need to be inspected. A suspect link can be cleared manually or by modifying the offending object. When a formal module changes or is updated, the change-bar illustrates this change with a red color if it is not saved or a yellow color if the module is saved. Figure 7 illustrates how information is displayed in DOORS.

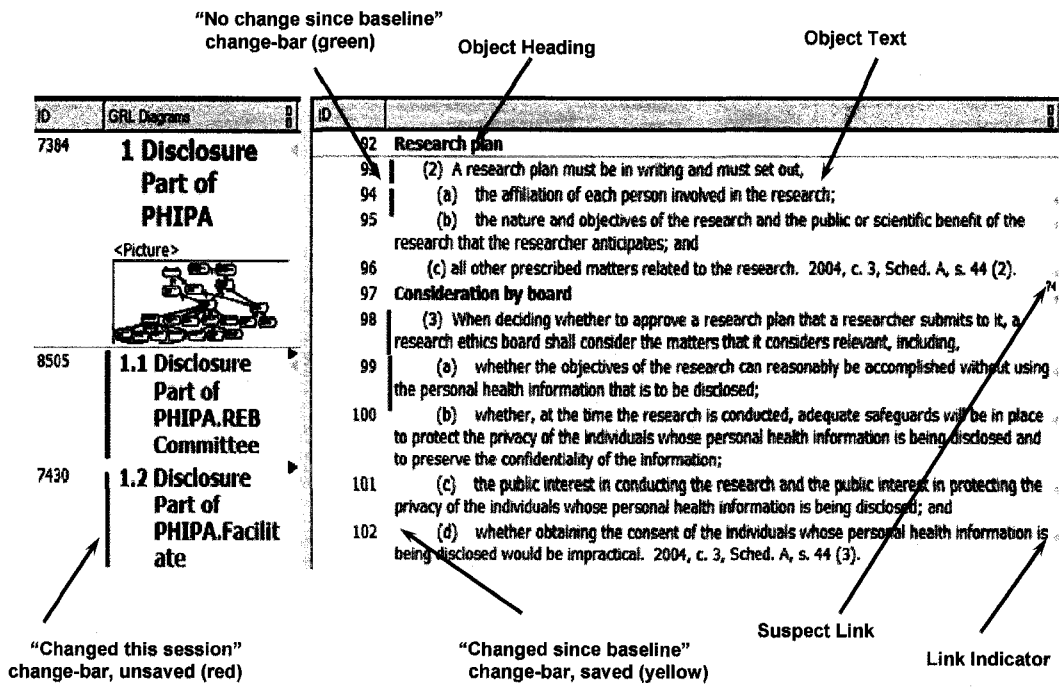


Figure 7 DOORS Displayed Information

DOORS uses a C-like interpreted programming language called DOORS eXtension Language (DXL), which can be used to develop additional features in DOORS. Such additional features include items to perform impact and traceability analysis, linking, import and export of files, and link auto-completion.

2.4.2 Requirements Management System Metamodel

Jiang, Mussbacher and Roy defined a metamodel for representing URN models in DOORS, which is now supported in jUCMNav [19][20][26]. Using DXL scripts and custom libraries, jUCMNav exports DOORS modules including UCM diagrams, GRL dia-

grams, requirements objects (e.g., actors, intentional elements, responsibilities, components, stubs) along with their attributes, and even the links describing internal or user-defined relationships between URN elements. This export mechanism provides a partial view of the URN model and is especially useful for creating links to and from external requirements for the purpose of monitoring evolving requirements and models. There is also the option of using predefined views to perform this function.

Also included in DOORS is an auto-link mechanism, written in DXL, that takes the automatically created internal links and the manually created links in the UCM model and generates new links by transitivity. This helps minimize the number of links that must be established manually. Creating direct links in such a way also enables analysts to use basic DOORS features and perform traceability and impact analysis on evolving models. However, no such auto-link mechanism was provided for the GRL portion of the model.

2.5. Modeling Legislation and Compliance Mapping

Current research focuses on applying requirement engineering concepts and tools in order to provide methodologies that ensure regulation compliance and traceability between textual documents, goals, and business models.

Darimont *et al.* describe such a method for how to apply one of the main goal-oriented requirements engineering methodologies (KAOS) to model regulations [6]. They explain how to incrementally transform regulation documents into three models for goals, objects and threats while maintaining a level of traceability from the source document to the models. This method, however, does not combine the three models into one integrated model. The integration of the models would help provide traceability in a more efficient manner. A modeling language such as GRL, on the other hand, has the capacity to represent high-level goals, actors and tasks (activities) in one model. It employs different strategies to illustrate conflicting objectives and their impact on the high-level goals and the main objective of the system.

He *et al.* introduce the Requirement-based Access Control Analysis and Policy Specification (ReCAPS) method [15]. This method integrates the components of access control analysis, improves software quality and ensures policy- and requirements-

compliant systems. It places an emphasis on compliance between different policy levels, requirement and system designs. ReCAPS includes a set of process descriptions and heuristics to help analysts derive and specify Access Control Policies (ACPs). It also provides traceability from source documents to these ACPs. This traceability helps ensure compliance between policies, system requirements and software design. This approach is presented in the context of the software development process and thus applies less generally than what we introduce in this thesis. Our method provides traceability for a compliance mechanism between business processes and legal documents, with consideration for how they evolve.

In [24], Rifaut *et al.* apply goal-based models to perform goal-oriented requirements engineering on the implementation of a financial system to ensure that it is compliant with Basel II regulations. In this method, the organization and its business processes are divided with respect to the different organizational layers. The objectives, strategies, policies and indicators (based on the definition of a goal model) are defined for each layer and provide a structure for the design of a regulation-compliant financial system. This method does not provide a traceability mechanism that highlights situations of non-compliance for the goals and business processes of the organization.

Breaux *et al.* describe how to apply semantic parameterization to HIPAA privacy rules to extract rights and obligations from the HIPAA text [4]. They provide some strategies to help define exceptions, and solve ambiguities. Their work only focuses on the analysis of regulations and the balance between rules and obligations. It does not include any mechanism for traceability between regulatory and organizational documents.

The OMG Regulatory Compliance Alliance (ORCA) [3] has developed an open intellectual property project to help organizations handle the compliance management burdens they are facing due to the increase in the number of regulations. In their research, they found out that in order to have an automated compliance management, it is necessary to standardize the representation of compliance documents including rules, regulations, and guidance documents. To solve this problem, they first developed a Compliance Global Regulatory Information Database (C-GRID) system to collect detailed regulatory documentation as well as other information. Currently, they aim to provide dynamic mappings between rules, common frameworks of objectives and internal controls related

to these objectives. This mapping will help organizations ensure that their businesses meet all the regulatory requirements and help them predict the impact of change to controls. However, ORCA still does not connect the business processes to the regulations. Their work mainly focuses on integrating the different regulations and creating mappings between regulations and organization policies.

These papers tend to focus on only one aspect of regulation compliance, i.e. either the goals and objectives or the business processes. In our work, we consider both aspects in the context of an information custodian in using URN to connect the business processes to the legal documents and GRL to trace instances of non-compliance no matter how either aspect may change over time.

Chapter 3. Compliance Framework

In this chapter, we describe our proposed framework architecture. We combine the User Requirements Notation, a requirements management system and compliance concepts to build a compliance framework. We also extend the metamodel used to represent URN models in DOORS.

In Section 3.1, we define the different approaches that can be taken to verify legislative compliance of business processes. In Section 3.2, we explain the proposed framework architecture and how it is based on a model-based approach. In Section 3.3 we describe the metamodel of the framework and in Section 3.4 we analyze the different types of links in the proposed framework. Finally, in Section 3.5, we explain how the auto-completion mechanism works and summarize the chapter in Section 3.6.

3.1. Definition of Approaches

3.1.1 Document-based Approach

In this approach, the organization's policies and procedures documents are inspected and manually compared with actual laws and legislation documents to verify their compliance.

Organizations sometimes use a requirements management system such as DOORS to provide tool support for the creation of manual links between the documents and to track and verify compliance.

3.1.2 Model-based Approach

In this approach, the organization's policy and procedure documents as well as the legislation documents are modeled with URN mainly in terms of goals, tasks and actors. Having models for the business processes and legislation gives some advantages over just having documents. The main benefit of the model over verbose documents is that with a

model comes an increased ability for people to understand business processes. Moreover, having the laws modeled improves the comprehensibility of these laws by non-specialists. Finally, having both the law and the business processes described in the same modeling language helps when linking them together in a more uniform and organized way. The alternative is to insert miscellaneous references all over the textual documents.

In this approach, with the help of a requirements management system as tool support, the URN model of the organization is linked to the URN model of the law. It is in this way that compliance between the organizations' policies and the law can be established.

In addition, such an RMS tool allows the models to be linked to their source documents. The existence of such links provides the opportunity to combine the document-based approach with the model-based approach.

3.2. Compliance Framework Architecture

3.2.1 Full Compliance Framework

Our compliance framework is based on the combination of model-based approach and document-based approach. It includes two separately built URN models and a set of links between them. The URN model of the legislation is built separately from the URN model of the organizational business processes in order to allow the legislation model to be re-used by different organizations.

The model of the legislation is defined, for the most part, in terms of goals, actors and tasks and specifies the legal requirements of the organization. The model of the organization is also defined by goals, actors and tasks. It also includes definitions for business processes that have been implemented at the organization. Each model includes some internal links that capture the relationships between the different levels of abstraction within the model. Compliance can be tracked by defining and managing external links between the two models.

In Sections 3.2.2 and 3.2.3, we explain the legislation and organization models and their internal links separately and then in Section 3.2.4 we add external links between two models for tracking compliance.

3.2.2 Legislation Model

Legislation documents are composed of clauses and definitions which can be modelled with intentional elements and actors respectively. Clauses are usually described as *purposes,* and sets of *rules* and *obligations.* The purposes of the legislation can be modeled as softgoals since they are fuzzy in nature and they can never be fully satisfied. Rules and obligations are modeled as goals or tasks based on whether they are requirements to be achieved (goals) or operationalizations (tasks). In addition, clauses usually have some conditions which can yield either a positive or a negative effect. These negative or positive effects can be modeled with contribution links types, i.e., *Make*, *Help*, *Some+*, *Break*, *Hurt*, *Some-*. Definitions are expressed in terms of phrases and the actors for whom they apply. Actors in the documents are modeled as actors in the GRL but phrases cannot be modeled with GRL. In summary, the mapping is:

- Purposes → Softgoals
- Rules and Obligations → Goals and Tasks
- Definitions:
    a) Actors → Actors
    b) Phrases → None

An example of how to model the legislation with GRL is given here:

> *An Organization shall not use the personal information of an individual unless a) it has the individual's consent and b) the information is necessary for a lawful purpose.*

The purpose of this law is to prevent unauthorized use. This purpose can be modeled as a softgoal. The conditions a) and b) are modeled as tasks with positive effects on the softgoal (*Help*). Figure 8 represents the GRL model corresponding to this legal statement. The GRL model is based on the interpretation of the law by the organization that builds the model and it is only a mechanism to document the legislation in a declarative way. The GRL model needs to be inspected by lawyers for validating its correctness and preventing a false sense of security.

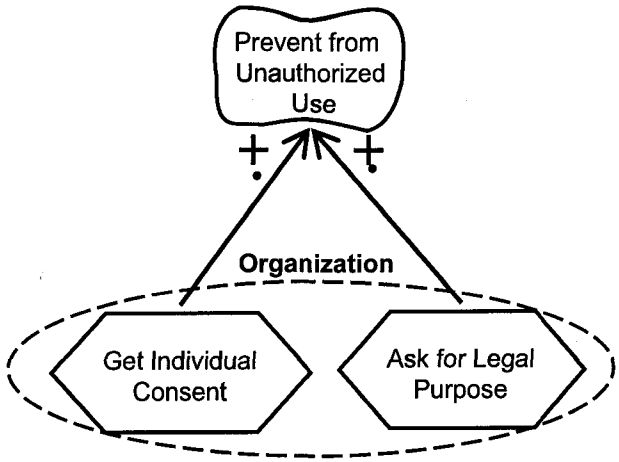


Figure 8 GRL View of the Law

It is also necessary to link the actual legislative documents to the model to be able to keep track of the changes and determine the parts of the law that cannot be modeled with GRL. These links are called *Source* links and connect various GRL elements to their definitions in the original text documents.

Figure 9 shows a high-level overview of the legislation model with its defined links.

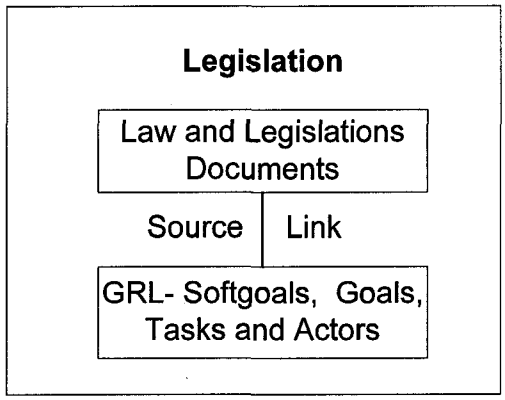


Figure 9 Links in a Legislation Model

Figure 10 shows an example of a legislation model. It illustrates the source links between the tasks of the GRL model and the related source documents.

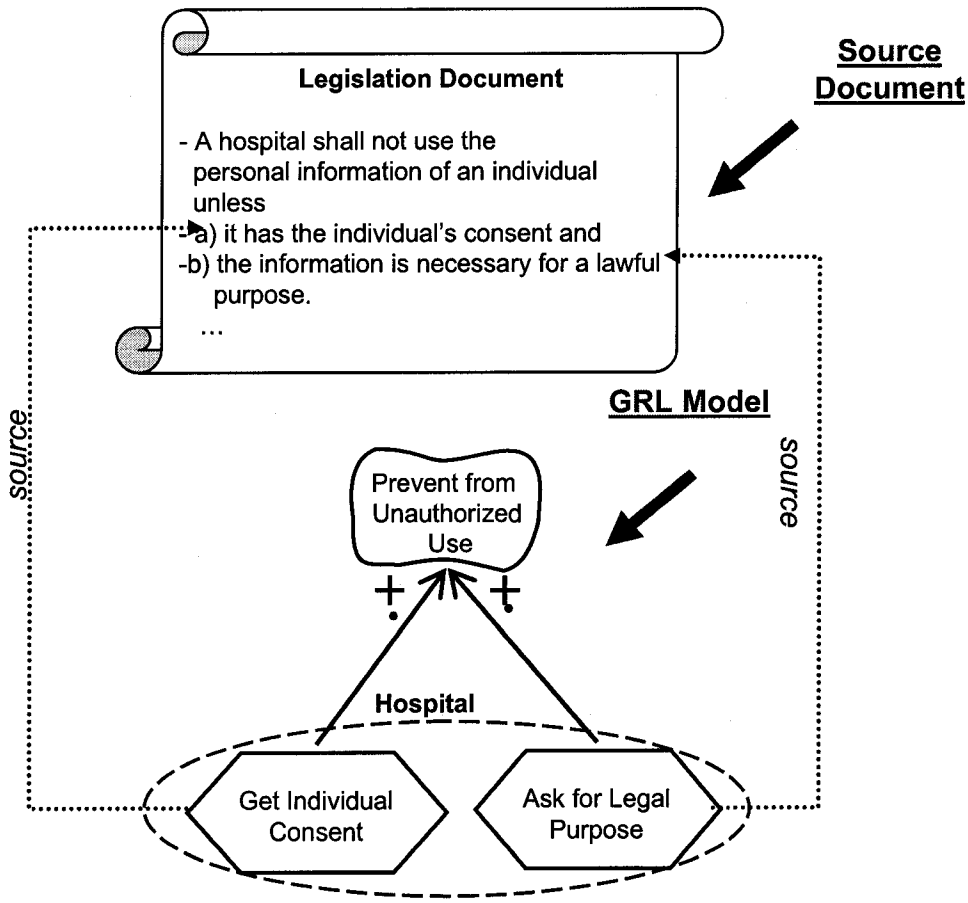


Figure 10 An Example of a Legislation Model

3.2.3 Organization Model

Organizations have policy and procedure documents that define their business processes and implicitly their goals. However, these goals and processes need to be aligned with the legislation. Therefore, it is necessary to link these business goals and processes to laws and legislation to investigate the potential instances of non-compliance and track changes due to evolution. To do so, we need a model for the organization similar to the legislation model to be able to compare the organizations' goals and business processes with the legislative documents. Previous work in [36], provides the model of the business processes with URN. In addition, different approaches for how GRL elements can be linked to UCM elements are discussed in two related papers [25][26].

An overview of the organization model shown in Figure 11 resembles the one shown for the legislation in Figure 9. This model contains the policy and procedure

documents of the organization, the GRL model that captures those policies and business processes as softgoals, goals and tasks, and the UCM model that represents the business processes operationalizing GRL intentional elements.

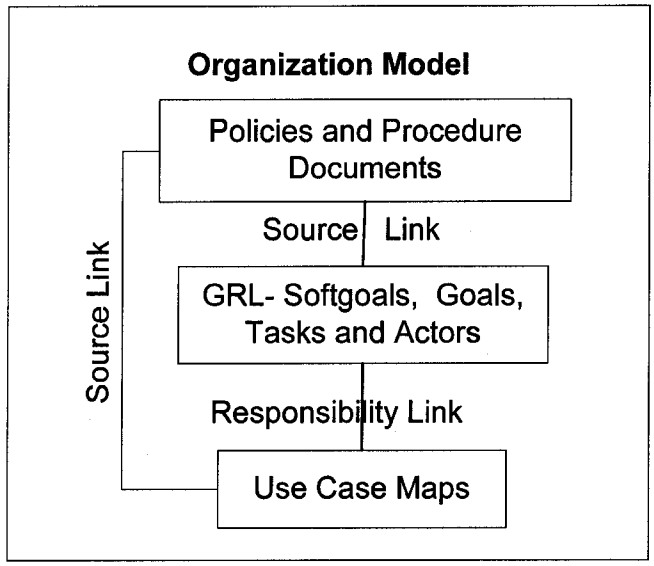


Figure 11 Links in an Organization Model

In order to track the internal changes in the organization, two types of links are defined between the elements of this model. These links are *Source* links and *Responsibility* links.

Source links are used to connect the actual policy and procedure documents and the organization's GRL or UCM elements. They link these elements to their definitions in the original textual documents. Source links in the organization model are exactly the same conceptually as source links used in the legislation model.

Responsibility links, on the other hand, link a GRL element to one or more UCM elements. For example, softgoals and goals can be linked to maps in the business processes UCM model while tasks and actors can be linked to UCM elements like responsibilities and agents.

In Figure 12, we present an example of an organization model. At the top of the figure the source document is shown with its links (tagged as *source*) to the GRL and the UCM diagram. In the middle of the figure, is the GRL model which includes a softgoal, *Prevent from Unauthorized Use*, and the goals and tasks which help achieve the softgoal.

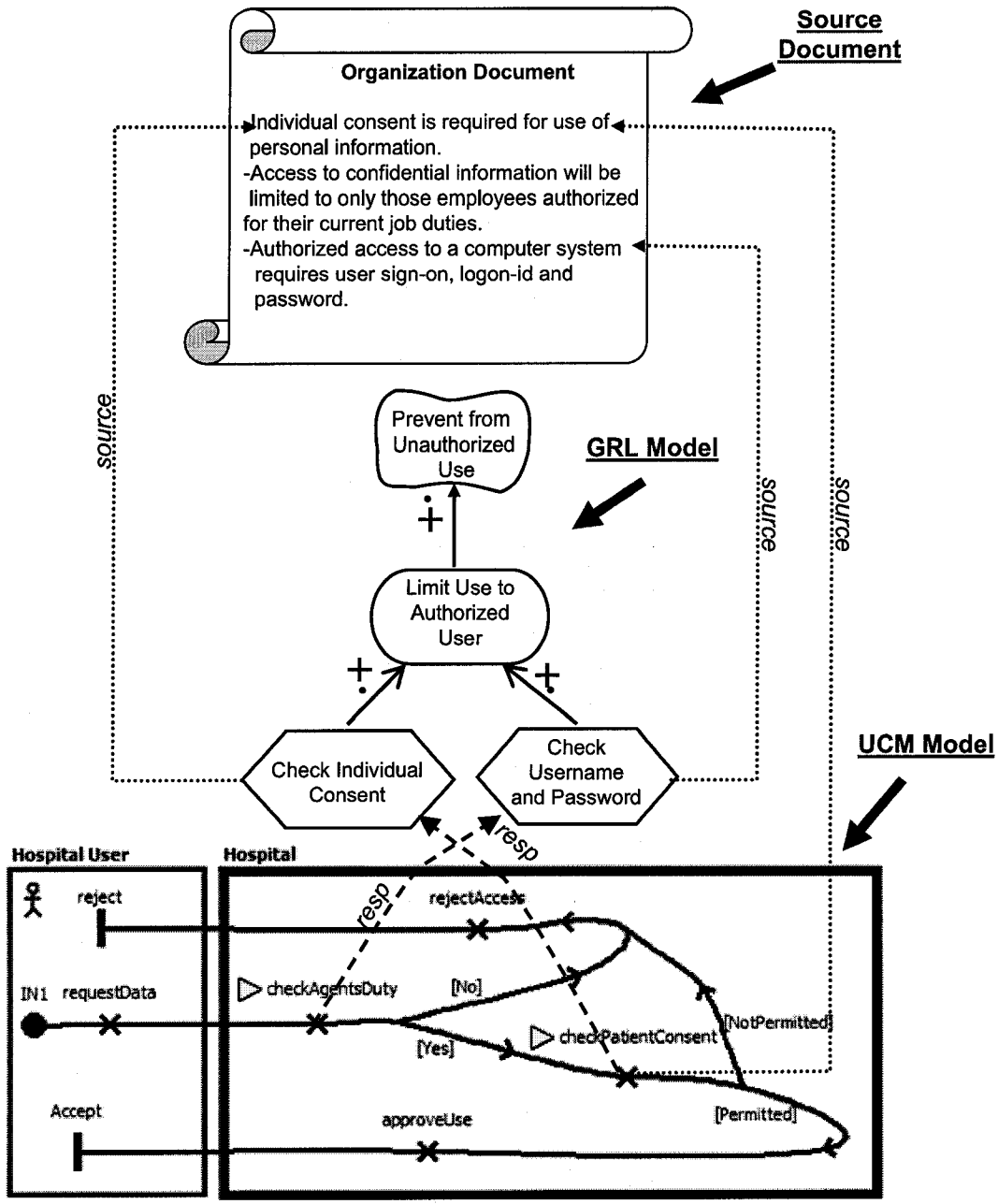


Figure 12 An Example of an Organization Model

At the bottom of the model, the UCM diagram shows the business process related to the use of personal data. This model links to the source document through *source* links, e.g. *checkPatientConsent* to *individual consent is required for use of personal informa-*

tion. It also links to the GRL model via *responsibility* links (tagged as *resp*), e.g. *Check Individual Consent* (task) to *checkPatientConsent* (responsibility).

3.2.4 Compliance Framework

As we explained in Section 3.2.3, organizations need to ensure that their policies and processes comply with legislation. In order to do this, it is necessary to establish some link types between the organization and the legislation models. There can be several links between these two models.

One potential link that can be established between the policies and procedure documents and the legislation documents is shown in Figure 13. However, this link is not very helpful since both organizational and legislative documents are very complicated and are usually written with different language structures. Therefore, establishing such links is usually hard or impractical.

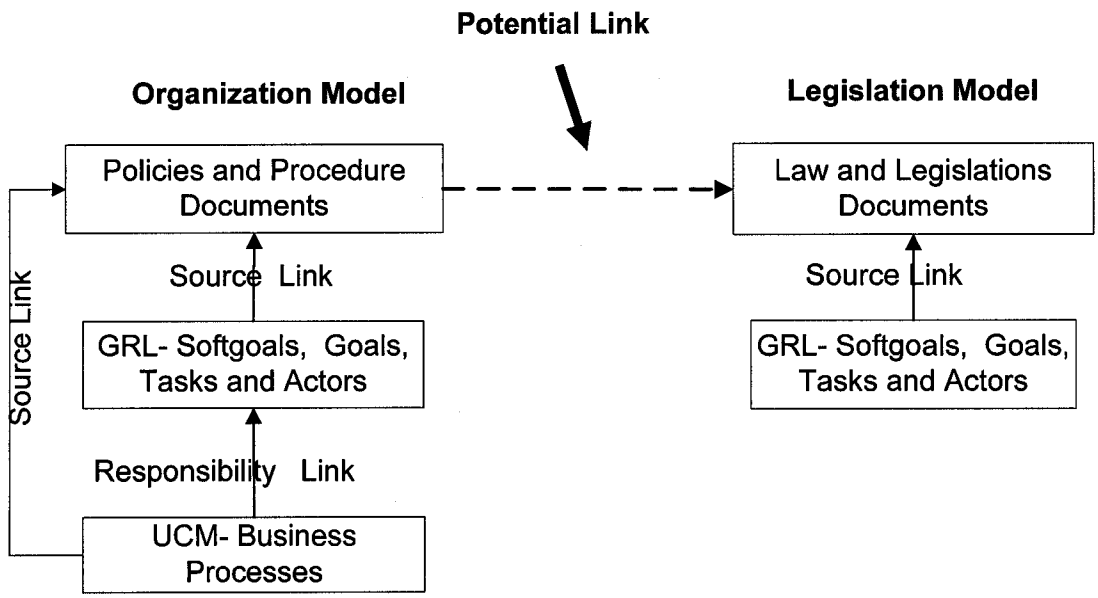


Figure 13 Link between Organizational and Legislative Documents

Other potential links considered are those defined between:

- the organization GRL model and the legislation GRL model;
- the organization GRL model and laws and legislation documents;

- the organization UCM model and the legislation GRL model; and
- the organization UCM model and laws and legislation documents.

These potential links are depicted in Figure 14.

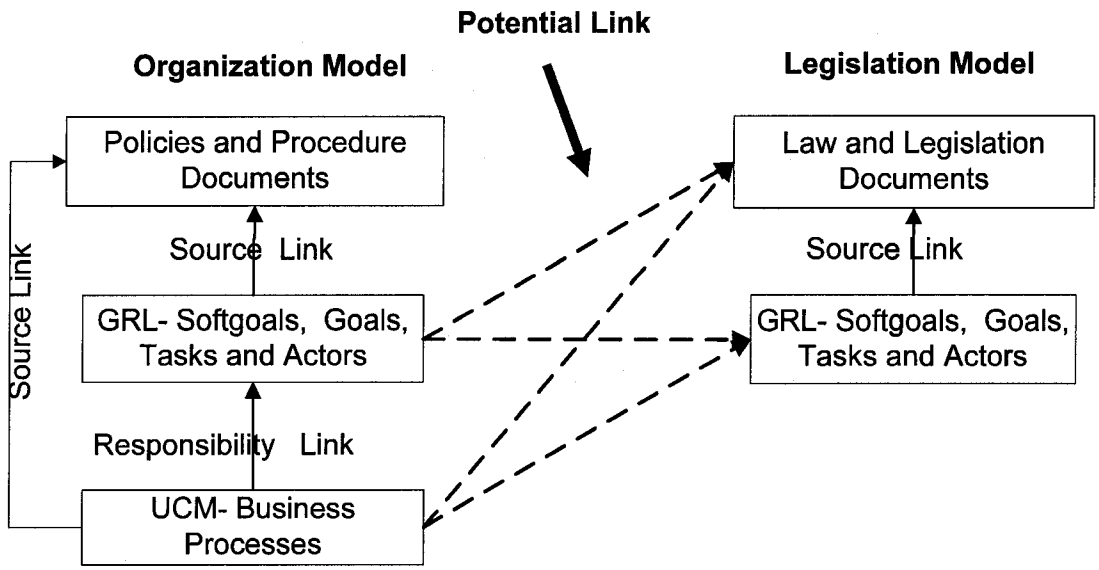


Figure 14 Link between Organization Model and Legislation Model

However, as we mentioned earlier, legislation documents usually do not have many operational procedures and therefore linking the organization UCM to the law and legislation document is often not worth it. As a result, our framework contains three types of links between the organization and the legislation model. Figure 15 illustrates a high-level overview of this compliance framework with links identified between the organization model and the legislation model.

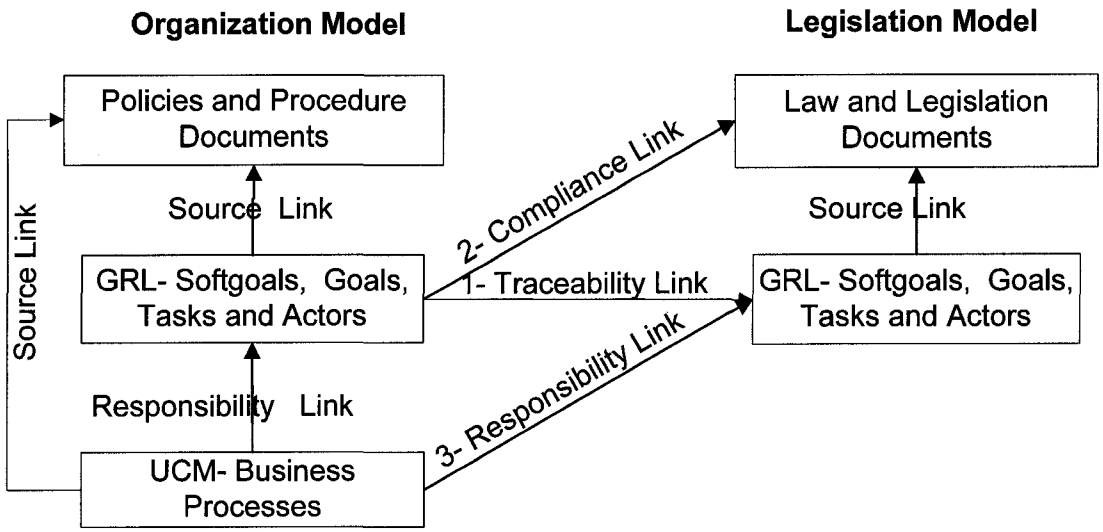


Figure 15 Requirements Management Framework

The identified link sets for this compliance framework are:

1. *Traceability Links*
2. *Compliance Links*
3. *Responsibility Links*

As shown in Figure 15, *traceability links* are used to connect GRL elements of the organization to GRL elements of the legislation. These links are used to trace, at a high level, the intentional elements and actors identified in legislation with the ones related to the business processes of the organization. Traceability links, although created manually, are usually not difficult to establish since the two models are expressed at similar levels of abstraction and use similar concepts.

Figure 16 shows an example of how traceability links are created between two GRL diagrams. This type of link (tagged as *traces*) connect any two actors, tasks, goals or softgoals. For example, there is a traceability link between the goals "Limit Use to Authorized Users" and "Limit Use". There is also such a link between the tasks "Have an Individual Consent" and "Check the Individual Consent."

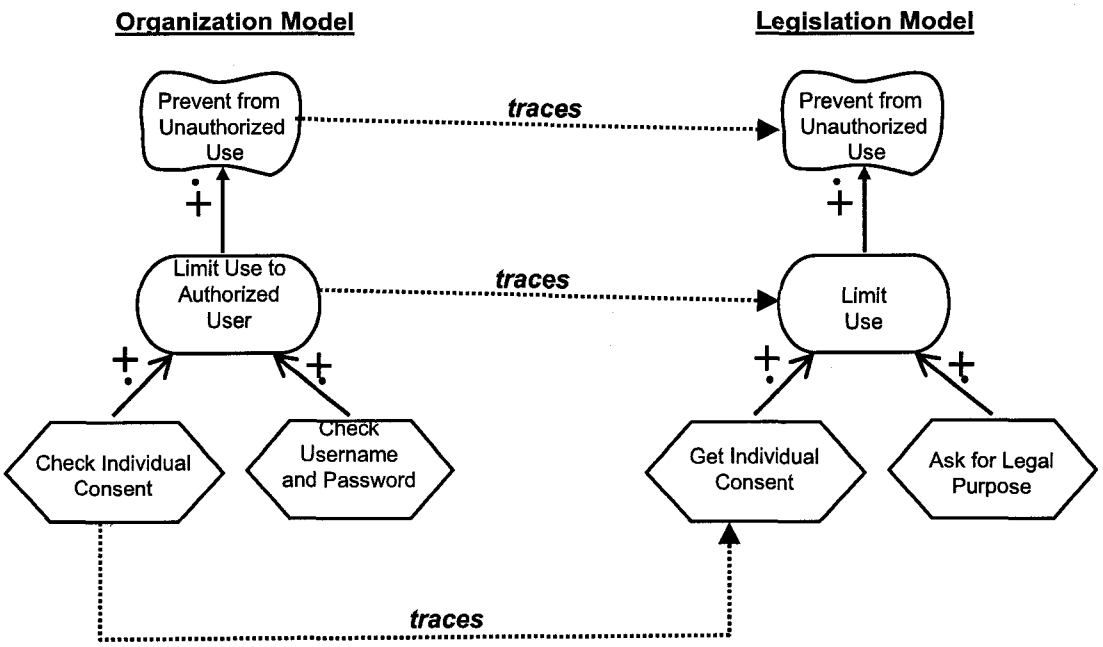


Figure 16 Traceability Links Example

Compliance Links (Figure 15) are links between organization GRL elements and the actual text of the law and legislation documents. These links are useful in highlighting exceptions and additional descriptions in the legislation that are not easily communicated in diagrams. They are, therefore, very precise and provide additional information about the legal requirements. These links can be created manually or can be inferred from previously created links, by transitivity.

Figure 17 provides an example of compliance links between GRL elements and the legislation documents. These links (tagged as *complies*) are found between actors, tasks or softgoals of the organisation model and the actual text of the legislation. For example, there is a compliance link between "Hospital" and the "HIC" definition (actor → legislation document) and between "Prevent from Unauthorized Use" and "Purpose of the Act" (task → legislation documents). This type of link clearly adds some detail to the model by indicating how the organizational elements are represented in the legislation and vice versa.

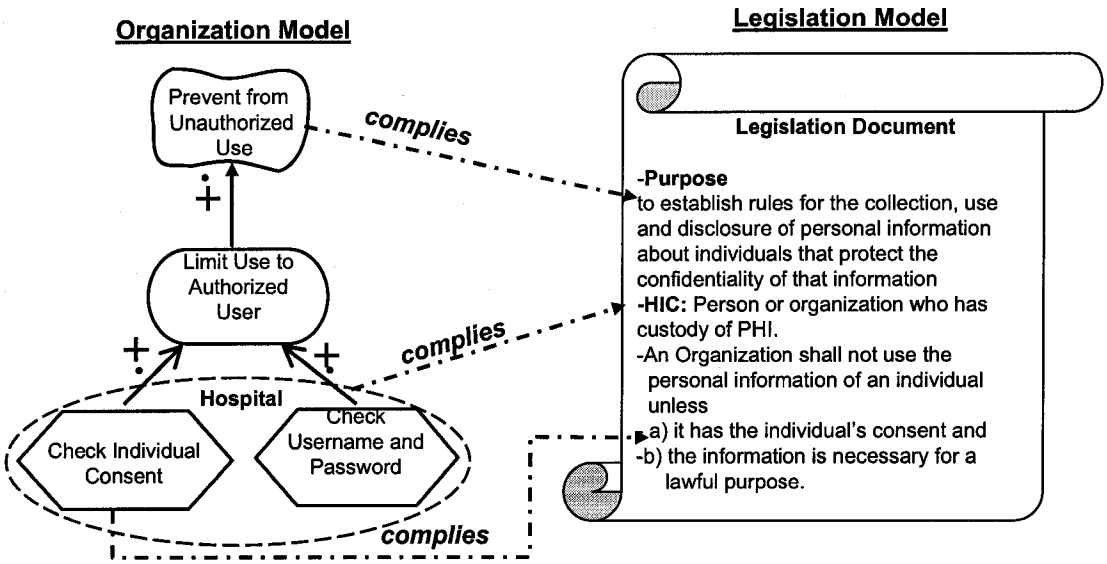


Figure 17 Compliance Links Example

From Figure 15 we see that *responsibility links* are used to connect UCM elements of the organization business processes and GRL elements of the legislation documents model. This type of link is very similar to that of traceability links but serves to more directly link the detailed scenarios and business processes to the tasks and actors of the legislation model.

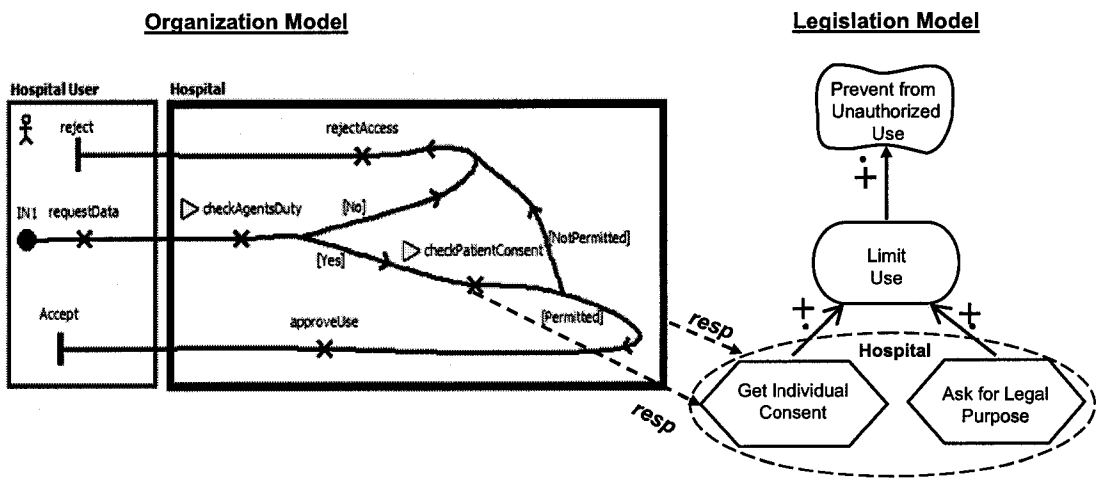


Figure 18 Responsibility Links Example

An example of responsibility links established between the organization UCM model and the legislation document GRL model is illustrated in Figure 18. These links

(tagged with *resp*) and are found between components, and responsibilities of the UCM model and the actors and tasks of the GRL model. There is, for example, a link between "Hospital" in the UCM model and "Hospital" in Legislation GRL model (component → actor) and between "checkPatientConsent" and "Check Individual Consent" (responsibility → task) in their respective models.

3.3. Framework Metamodel

3.3.1 Framework Metamodel Definition

In previous sections, we described how to model the legislation and organization documents with URN and the types of links required in order to provide compliance traceability. The link sets proposed in the previous section are not part of the representation of URN models exported to the DOORS RMS and, therefore, this representation (defined as a metamodel) needs to be extended.

In this section, we explain the framework metamodel. This metamodel extends the URN-to-DOORS metamodel (discussed previously in Section 2.4.2) in order to implement the framework presented in Figure 15. The new metamodel is summarized in Figure 19 and extends the metamodel of Section 2.4.2 to support the presence of links between URN models and between each URN model and its source document.

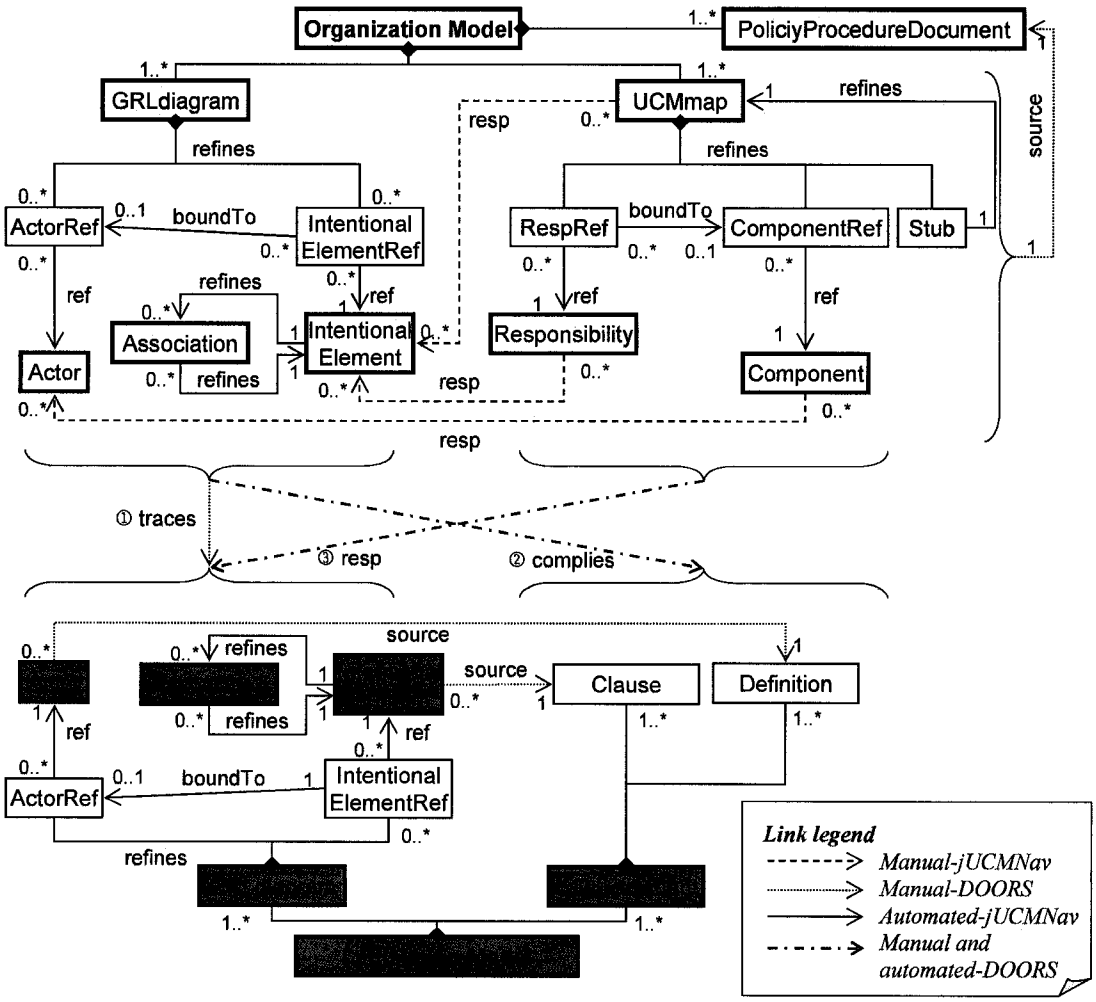


Figure 19 Framework Metamodel

The legislation model (bottom part of Figure 19) includes the legislation documents and GRL diagram introduced in Figure 15. The *LawDocument* class defines the clause and definition objects and the *GRLdiagram* class defines the intentional element, association and actor objects. Between the objects of this model, source links are defined, for example, from intentional elements to clauses and from actors to definitions.

At the top of Figure 19, the organization model is composed of GRL diagrams (goals) and UCM maps (business processes). Also present is the source policy and procedure document. The *UCMmap* objects (i.e. Responsibility and Component) have responsibility links (*resp*) to the *GRLdiagram* objects (i.e. intentional element and actor). Also

the *PolicyProcedureDocument* class links to the *UCMmap* and *GRLdiagram* objects via source links.

In addition to the internal links between the objects of each model, three type of external links between the two models themselves exist in the new metamodel. As already presented in Figure 15, these links are one directional. Traceability links (*traces*) connect the actors and intentional elements of the organization model to the actors and intentional elements of the legislation model. Compliance links (*complies*) are set up between the actors and intentional elements of the organization model and the definitions and clauses of the legislation model. Finally, responsibility links (*resp*) are built from the maps, responsibilities, and components to the intentional elements and actors of the legislation model.

Figure 20 illustrates how this framework metamodel can be instantiated in the context of a hospital business process that has to comply with PHIPA. In this excerpt of a larger model, we observe part of the hospital policy document, its goal model, and the corresponding business process. On the right side, the PHIPA legislation document is modeled with GRL. URN internal links (*ref*, *refines*, *boundTo*, etc.) are not shown here; they correspond to the regular relationships illustrated in the diagrams themselves and are all the same exported to the RMS. Also shown are several source and traceability links that were manually created in DOORS. Internal responsibility links are also manually created between the UCM and GRL views in jUCMNav. Compliance links and external responsibility links are inferred automatically by transitivity.

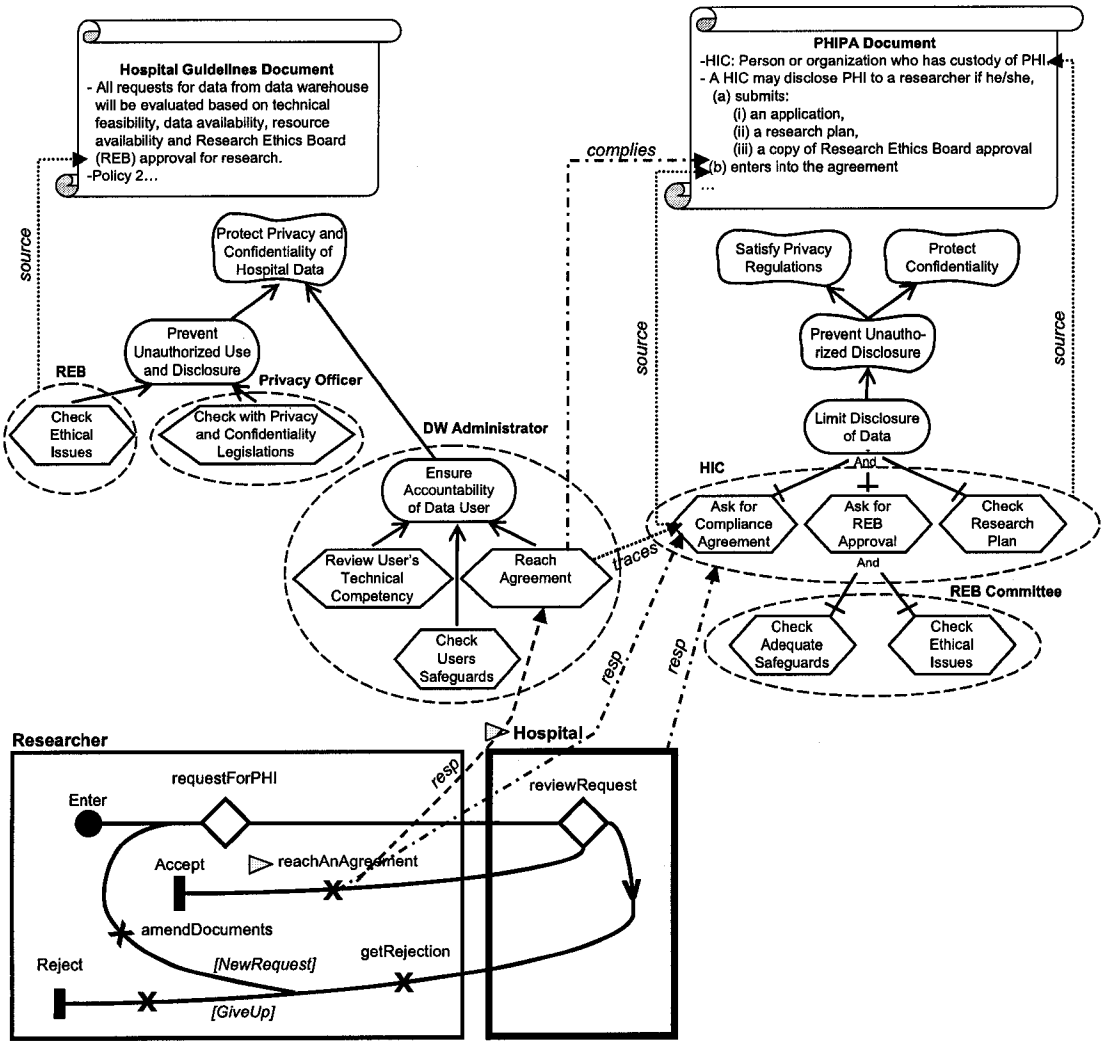


Figure 20 Example of Privacy Compliance Links in a Hospital (Excerpt)

3.3.2 Tool Support for the Framework

Our new metamodel helps to provide tool support for the full compliance framework but there is not a single tool that can model the documents and provide link support at the same time. Therefore, we use jUCMNav for modeling documents in URN and Telelogic DOORS to support links since jUCMNav is integrated with DOORS via an export mechanism. In order to identify which elements of jUCMNav are necessary to be exported to DOORS, we use the metamodel of the proposed framework explained in Section 3.3.1 and depicted in Figure 19.

Similar to the work of Jiang, Mussbacher and Roy, explained in [19][20][26], the only URN model elements exported from jUCMNav to DOORS are those likely to be useful from a requirements linking and management perspective. Importing all links into a requirements management system would lead to performance degradation and usability issues because there would be too many unnecessary details. In the class diagram, shaded classes represent separate formal modules in DOORS, and named associations represent link modules. Note that although some associations have directions, corresponding link instances can be navigated in either way in DOORS.

The part of the metamodel related to legislation documents shows both the source documents and the GRL models. The source document, which defines clause and definition objects in a textual way, is imported "as is" into DOORS. A GRL model is created with jUCMNav out of the source document and then exported to DOORS. The source links from the intentional elements and actors are then manually added. Note that this task only needs to be performed once for each law. With a requirements management system such as DOORS, missing links can be easily identified when there is no mapping for a requirements object (e.g. a GRL element) to the source document.

The portion of the metamodel related to the organization includes the source documents and a URN model composed of UCM and GRL diagrams. The UCM and GRL diagrams are exported to DOORS from jUCMNav with many of the internal links generated automatically from the URN model. The source policy and procedure documents are again imported "as is" and linked manually. Responsibility links are established between the UCM and GRL diagrams in jUCMNav and subsequently exported to DOORS.

Once both the organization model and the legislation model are available, traceability links between the two GRL models can be added manually using DOORS. Compliance and responsibility links are then set up manually or by auto-completion.

The metamodel also helps us determine which links need to be created manually and which ones can be inferred automatically. If the creation of a link can be automated, then this will help reduce the amount of effort required to implement the compliance framework. On the other hand, inferring too many links will make the tool less usable,

especially during evolution. A single change could lead to the situation where the entire model needs to be revisited, which is not helpful.

3.4. Analysis of Links

In this section we analyze the three types of links based on the following criteria: granularity, functionality, precision, quantity of manual links, difficulty, and importance of completeness. The analysis of this part is subjective and based on the experience that we got during establishing the links.

3.4.1 Definition of Criteria

Granularity

This criterion explains what types of models and elements are involved in the links.

Functionality

This criterion explains the purpose of each link.

Precision

This criterion explains how accurate compliance or non-compliance can be tracked by each link.

Quantity of Manual Links

This criterion refers to the number of manual links which need to be established.

Difficulty

This criterion explains the level of difficulty required to establish each link type.

Importance of Completeness

This criterion refers to how important it is for the links of each type to be created to have full coverage and compliance.

3.4.2 Analysis of Link Types

Based on the criteria defined in the previous section, each link type is now analyzed.

Traceability Links: This link type is found between the organization GRL elements and the legislation GRL elements. The link set includes links between the organization softgoals, goals, tasks and actors and those in legislation. It shows what is missing or unnecessary in terms of the organizational goals and tasks (and by consequence in their processes) and who is in charge of what activity. A missing softgoal, goal or task can be a strong indication that the organization does not completely comply with the law. Therefore, this link set is very precise and it can help organizations to measure their compliance very accurately. The traceability links are created manually. However, establishing this link set is not very difficult since both models are expressed at the same level of abstraction. It nevertheless improves the ability to properly answer the main goal of good traceability, and comply with legislation.

Compliance Links: This set differs from the traceability link in that instead of using GRL elements to model the legislation document, we use the document itself. This has the advantage of being able to deal with all the exceptions and special definitions. In practice, this set only contains those links between the GRL and the special constraints and exceptions in the text documents which cannot be modeled by GRL. Therefore, compliance links are very precise and provide organizations with some additional information in order to define or improve their processes in terms of legal compliance. Creating this link set manually requires much effort but the number of manual links is fairly small and most of the links can be created through an auto-completion (transitivity) mechanism. Compliance links do not need to be complete and only partial links between missing parts of the legislations in GRL and the organization GRL are satisfactory.

Responsibility Links: The main difference between these links and the traceability links is that the organization UCM model is linked directly to the privacy legislation GRL model. That is, responsibilities and components are directly linked to the tasks and actors in the legislation GRL. This link set is very precise since it includes fine details of the business processes, so the traceability between processes and legislation GRL is much easier than with the other links. However, in terms of functionality, responsibility links are most similar to the traceability links. Thus, it is only necessary to create one of these two alternatives. In addition, as with traceability links, this link set needs to be complete

and the number of links involved is high. Moreover, most of these links can be created automatically.

With respect to the different link options presented, we evaluated each of them based on the criteria mentioned above. Table 1 gives a summary of our analysis.

Table 1 Evaluation of Different Link Types

Links / Criteria	Traceability Link	Compliance Link	Responsibility Link
Granularity	Softgoals, Goals, Tasks & Actors	Legislative Text	Responsibilities, Components (Actors), Maps (Operational Processes)
Functionality	Handle Traceability of Non-Functional Requirements and Tasks	Handle Exceptions and Constraints	Handle Traceability of Business Processes
Quantity of Manual Links	Many	Small	Small
Precision	Very Precise	Very Precise	Very Precise
Difficulty	Moderate	Difficult	Moderate
Importance of Completeness	Very Important	Not Important	Very Important

As we see in Table 1, traceability and responsibility links are very similar in what they achieve and in the amount of effort required. In particular they both require complete coverage in order to be useful. Responsibility links are a bit more specific and precise but there is much overlap in the content they communicate, namely the mapping of organization roles and tasks or actors and processes to GRL elements in the legislation model. It would only make sense for one or the other of these two types of links to be used in order to track legal compliance. Responsibility links are a bit more specific but either set is sufficient.

Finally, if the organization wants to ensure that their processes comply thoroughly with the legislation, it is necessary to use compliance links as well. These links are used to highlight exceptions and specific constraints not captured in GRL or UCM notation but which are critical for ensuring compliance. They can be difficult and time consuming to

define, since they require direct references to legal text, but this is only necessary for specific critical parts of the legislation documents. Therefore, their completeness is not as critical as the traceability and responsibility links.

3.5. Auto-Completion Mechanism for Links in DOORS

3.5.1 Overview

In this section, we explain the auto-completion mechanism for the links between two models (i.e. model of the legislation and model of the organization) in DOORS.

DOORS uses a hierarchy of projects, folders and modules. As Roy defined in [25], URN models are imported from jUCMNav in a project in DOORS and for each of the URN model, a new folder with the name of the URN model is created. In our framework, both legislation and organization models are also imported in the same project in two folders called "Legislation" and "Organization". The URN models contain defined formal and link modules. The formal modules which are important to our framework are: *actors, intentional elements, components* and *responsibility* modules and the only link module that is needed in our framework is the *URN links* link module which covers "responsibility" links in our framework. Such link is created manually in jUCMNav between GRL and UCM elements and imported into DOORS.

In each of the folders (legislation and organization folders), the source documents are also imported in formal modules. These modules are called *law document* and *policy, procedure document* formal modules. To set the links between these formal modules and the URN models, two link modules need to be created. These link modules are called *sources* link modules. The *sources* link module for legislation in DOORS includes the links between:

a) Actors → Legislation Definitions
b) Intentional Elements → Legislation Clauses

The *sources* link modules for organization in DOORS includes the links between:

a) Actors and Components → Organization Definition
b) Intentional Elements and Responsibilities → Organization Clauses

Traceability, responsibility and compliance links are defined in the organization folder. Therefore, the formal modules in the organization folder are source objects and the formal modules in the legislation folder are target objects. The link modules which are created in the organization folder are *traces, complies* and *resps* link modules.

Traceability links are created manually. The *Traces* link module includes links between:

a) Organization Actors → Legislation Actors

b) Organization Intentional Elements → Legislation Intentional Elements

After establishing the traceability links, the compliance and responsibility links are created automatically with the help of a user-defined DXL library installed in DOORS. The way that compliance and responsibility links are created is shown in Figure 21 and Figure 22.

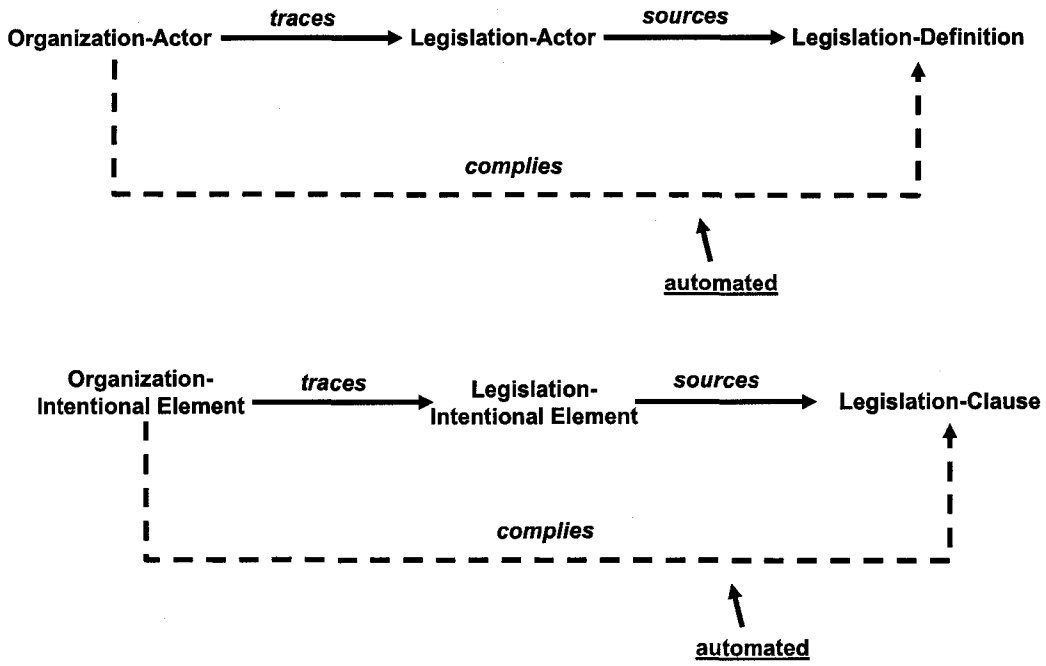


Figure 21 Compliance Links Creation

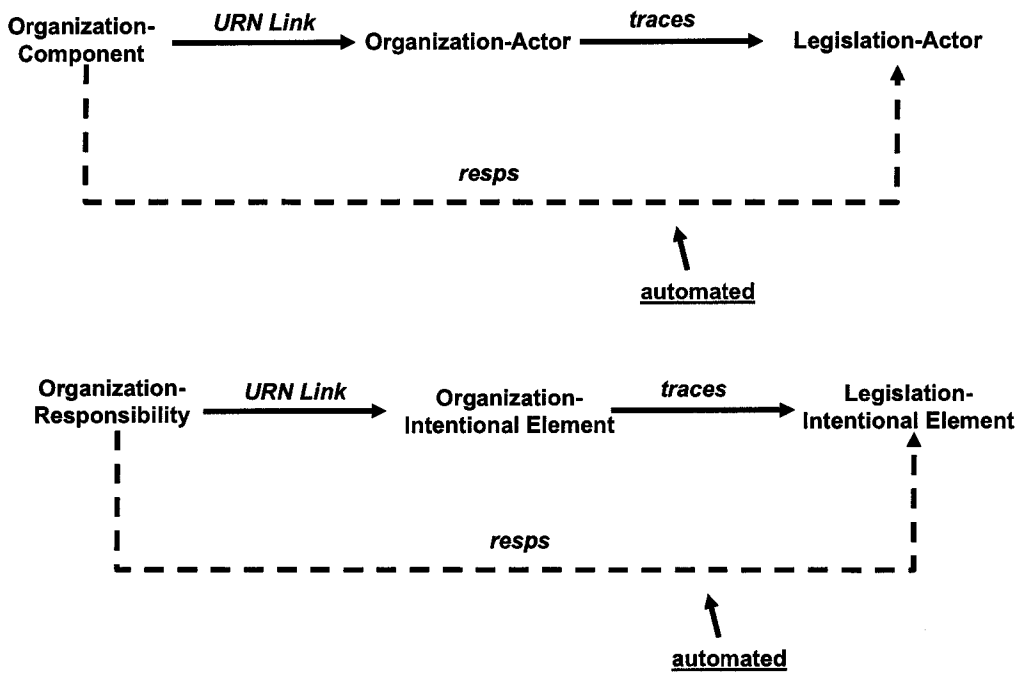


Figure 22 Responsibility Links Creation

3.5.2 Implementation

DOORS has the capability to implement user functions via its script interface. The interface supports the DXL (DOORS eXtensible Language) language. Libraries are added to DOORS by including a subdirectory to the addins directory in `TELELOGIC_HOME\DOORS_8.0\lib\dxl\`. In our case, we called our library *Compliance*. Inside this folder, 2 files must be provided:

File Name	Description
Compliance.hlp	A help file describing the library
Compliance.idx	A file used to build the menu item visible within DOORS

After providing these files, an additional menu item is added in DOORS as shown in Figure 23.

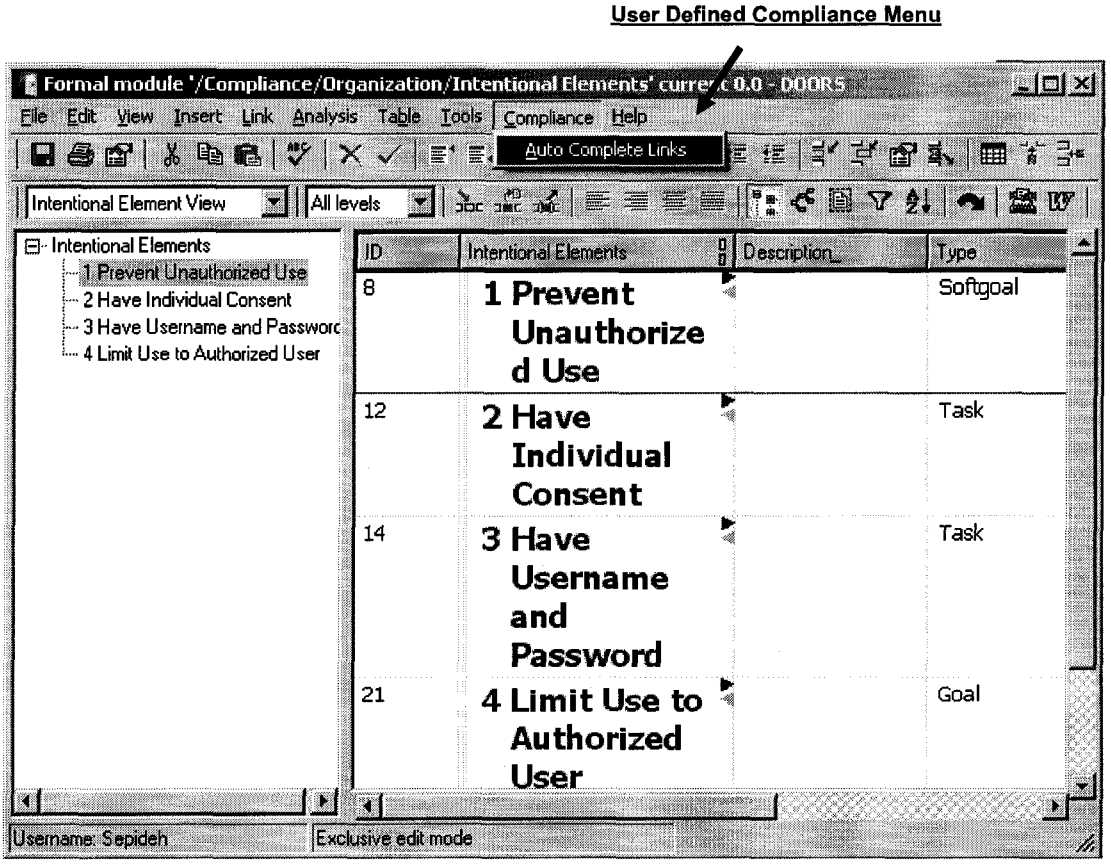


Figure 23 DOORS User-defined Menu Item

The Compliance.idx file specifies the function called when the menu item is selected. In our case, the function was called completeLinks(). Once called, it loads in required external files as part of the library and sets up the global variables. DOORS then brings up a confirmation box shown in Figure 24. Once confirmed, the script continues to execute the function and results in links being added to the URN folder in DOORS. The output is shown in Figure 25 demonstrating the created links between the organization and legislation URN models.

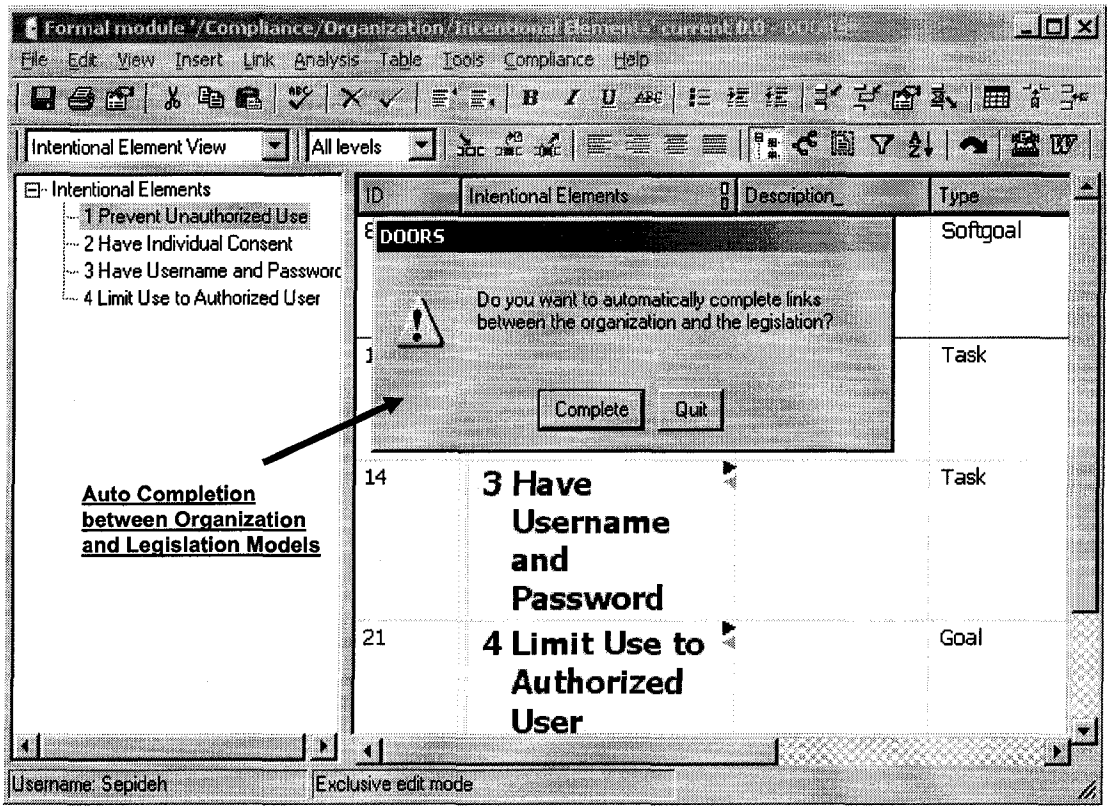


Figure 24 DOORS Confirmation Box

The specifics of this function are provided in a description of the steps below. Please refer to Appendix E for the full source code.

`completeLinks`

Description

- set current folder to the **Project Folder**
- confirm with the user to proceed with auto-completion
- open modules in the **Organization Folder**
  - set **orgIntentionalElements** = intentional elements module
  - set **orgActors** = actors module
  - set **orgComponent** = component module
  - set **orgResponsibility** = responsibility module
- open link modules in the **Organization Folder**
  - set **orgTraces** = traces link module
  - set **orgResps** = resps link module

    - set **orgComplies** = complies link module
    - set **UrnLinks** = URN responsibility link module
- open modules in the **Legislation Folder**
    - set **legDef** = definitions module
    - set **legClause** = clauses module
    - set **legIntentionalElements** = intentional elements module
    - set **legActors** = actors module
- open link modules in the **Legislation Folder**
    - set **legSources** = sources link module
- auto-complete complies links
    - call **completeTransitiveLinks** for **orgIntentionalElements**
    - call **completeTransitiveLinks** for **orgActors**
- auto complete resps links
    - call **completeTransitiveLinks** for **orgComponent**
    - call **completeTransitiveLinks** for **orgResponsibility**
- save and close

completeTransitiveLinks

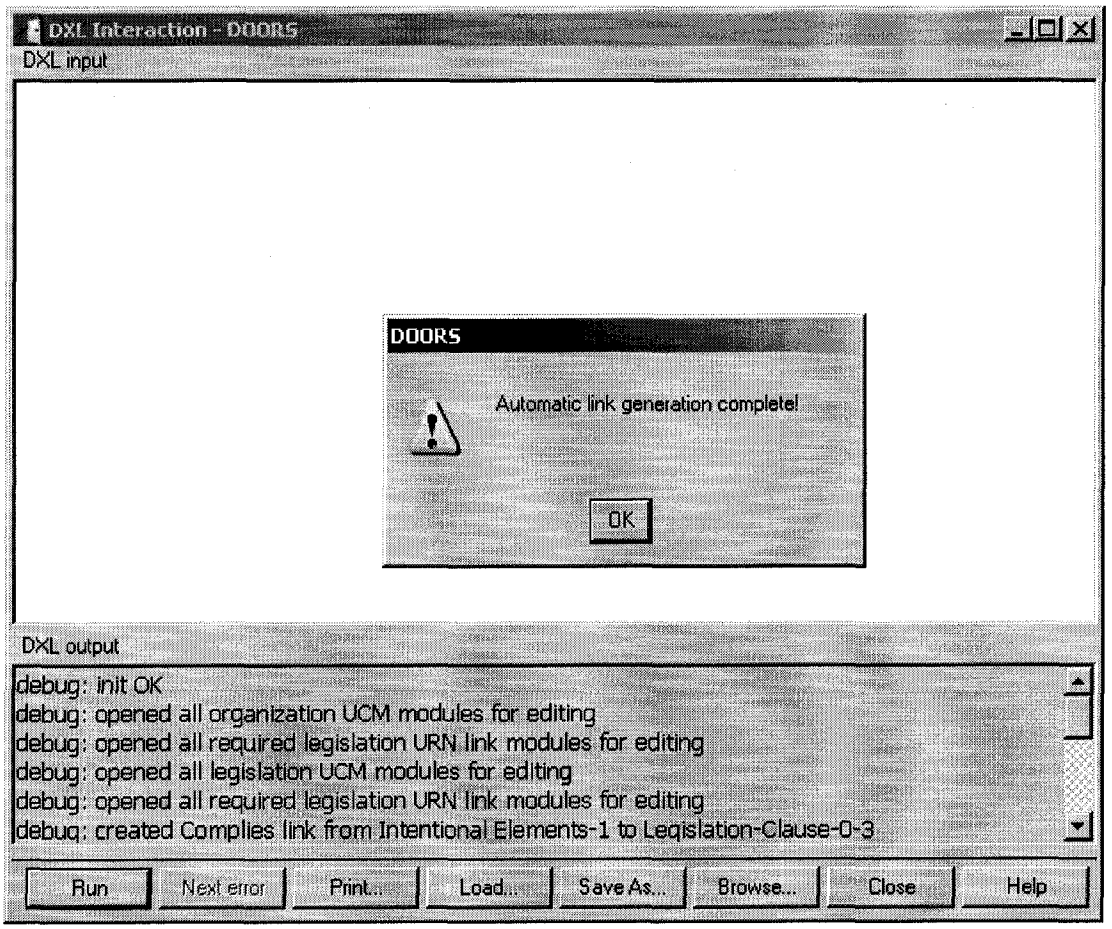
Parameter Type and Name	Description
Module startModule	The starting module for the automatic associative compliance links
string link1	The linkset of manual links connecting the first module to the second module
string link2	The linkset of manual links connecting the second module to the third module
string transitiveLink	The linkset used to create the transitive link

Description

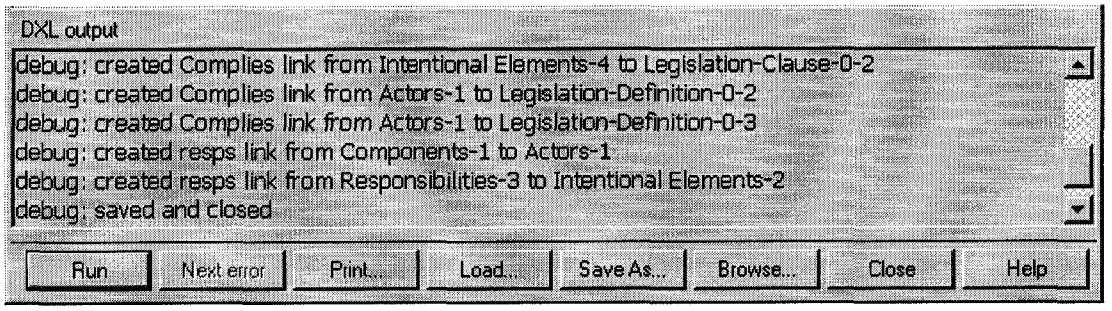
- iterate through the objects in the **startModule**
    - for each outgoing link **L1** from this module to the linkset **link1**
    - set **source1** = the source of **L1**
    - set **target1** = the target of **L1**
    - iterate through all objects in each **target1** module
        - for each outgoing link **L2** from **target1** to the linkset **link2**
        - set **source2** = the source of **L2**
        - set **target2** = the target of **L2**
        - iterate through all objects in each **target2** module

- create a new link from **source1** to **target2** in the linkset **transitiveLink**

- return **true**



a) Opening the Modules



b) Creating Auto-Links

Figure 25 Output of Link Creation Script

3.6. Summary

In this chapter, we defined the different approaches that can be undertaken by an organization to ensure compliance to the law. Based on these approaches, we established our compliance framework, a combination of the document-based approach and model-based approach. We then defined a metamodel of the framework to help decide which links can be created automatically and which need to be created manually. Using this metamodel, we analyzed the links according to different criteria and explained how the auto-completion mechanism works. In the next chapter, we will explain how the framework can be used as a tool for managing evolution to either the legislation documents or to an organization's business processes.

Chapter 4. Evolving Legislation and Processes

This chapter presents the methodology followed in using the compliance framework introduced in this thesis to maintain and track compliance in the face of changing legislation and business processes. The methodology will be explained via an example for which compliance must be maintained according to applicable legislation for an organization. In Section 4.1, we will discuss the evolution likely for both legislation documentation and business processes. In Section 4.2, we will explain the impact of legislation changes on business processes and how our framework handles these effects. Finally, in Section 4.3, we present the impact of business process change.

4.1. Legislation and Business Processes Evolution

One of the main goals of this thesis is to manage the evolution of legislative clauses and business processes. Both legislation and business processes can change quite abruptly and, therefore, handling the resulting impact is a major concern for organizations.

Privacy legislation (especially in healthcare) is new and still evolving. The laws have been amended several times since coming into effect. For example, the Personal Information Protection and Electronic Documents Act (PIPEDA) has been amended several times since it was passed in April 2000 [22]. Similarly, the Personal Health Information Privacy Act (PHIPA) was passed in 2004 and has been amended 5 times [13]. As for business processes, they are also susceptible to change, especially when there is a desire to leverage new information technology.

When legislation changes, an organization needs to verify whether their business processes are still compliant with legislation. However, since legislation documents are complex, it will be very time consuming to figure out which part of the law has been amended and whether this new amendment will affect their business processes or where they have to apply the changes. In addition, when an organization aims to improve its business processes, it has to make sure that this improvement does not violate the law. In

this case as well, it is also desirable to identify the elements of the law that are related to the improved business process.

With the help of the compliance links defined in Section 3.2.4, we are able to manage the impact of the different types of change and ensure that compliance will be maintained.

4.2. Managing Compliance as Legislation Evolves

In this section, we look at the different scenarios by which legislation documents can be amended. The scenarios are considered in the context of an organization that must maintain legal compliance for its business processes. The relevant cases to consider are:

1. A new clause is added to the source documents for legislation;
2. An existing clause with links to the organizational requirements models is modified;
3. An existing clause with links to the organizational requirements models is deleted;
4. An existing clause without links to the organizational requirements model is modified.

The impact of these changes on the organization's business processes and goals can be tracked through the link sets identified in Chapter 3. When legislation or other legal documents (source documents) are modified, the source links targeting these documents and the compliance links of the organization GRL model are directly affected. In turn, the modified legislation GRL model may affect the traceability and responsibility links along with the corresponding source elements in the GRL or UCM models of the organization. Note that deleting an existing clause without links to the organization's requirements models will not have any impact on the model. Also note that the clause term in this chapter refers to either clause or definition defined in chapter 3.

Next, we explain the net impact of each of the above scenarios. Each scenario is described using a specific example.

4.2.1 Addition of a New Clause

When a new legislative clause is added, one of the following two cases applies:

1. The new clause refers to an existing actor, softgoal, goal, or task. In this case, the clause could be an additional description, an extension or exception for the existing actor, or intentional element. Therefore, this new clause must be linked to the legislation GRL model through a source link. In doing so, the GRL model itself will not change but through the links defined between the models of the organization and the legislation, the impact of this additional information can be examined. Since the compliance link is a direct link between the legislation document and the organization's GRL model, this new clause requires adding a new compliance link between the GRL model and the new clause. However, adding this link can be performed automatically. Using the existing traceability link, the impact of the new clause on the GRL model can be traced. The responsibility link will model the potential effect of this new clause on the overall UCM model.
2. It introduces a new actor, softgoal, goal or task. This case is similar to the situation where an organization has developed the link sets between two models for the first time. The GRL model of the legislation needs to be updated and new elements added to the model. The organization GRL model may also need to be updated. The organization has to decide whether the new clause is relevant to their business process or not. If the organization GRL model changes, the existing UCM business process may need to be modified to address the newly added elements. Furthermore, the link sets would also have to be updated.

4.2.2 Modification of a Clause with Links

If a clause is modified, the legislation GRL model must be updated. This modification can be made to either clauses or definitions. The effect of this change on the legislation GRL model can be traced by a source link. Modification of the definition usually implies a change to the definition of the actor in the GRL model, whereas a modification to a clause translates into an update of the intentional element.

The effect of these changes to the legislation GRL model can be traced using either traceability links or responsibility links. If a traceability link is used, the part of the organization GRL model requiring attention will be highlighted. If the GRL model of the organization needs to be modified, the UCM model will also need to be changed. The

affected part of the UCM model will be highlighted by an internal or external responsibility link. We would also be able trace the impact of this change in the legislation document on the organization GRL model via the compliance link that exists between them.

4.2.3 Deletion of a Clause with Links

When a clause with links is deleted, the corresponding elements in its GRL representation may also need to be deleted. If the deleted clause is related to a required task or goal then this element may also be deleted. If the clause is just an extra definition of an existing element, then its deletion will not impact the legislation GRL.

Clauses and their corresponding GRL elements also have links to the organization model. As a result, when a clause is deleted the impact is highlighted in the GRL and UCM models of the organization. This may in turn lead to updates of the corresponding UCM model since certain functionality might no longer be necessary. Also, having fewer constraints may lead to new optimization opportunities. After the impact is confirmed and the GRL and UCM model changes have been made, these links can also be deleted.

4.2.4 Modification of a Clause without Links

This case is largely identical to the one in Section 4.2.1 with the exception that here the modified clause is more likely to be irrelevant to the task of managing compliance. However, in terms of its impact on the organization, the modification of a clause without links can be treated the same as if an entirely new clause were added.

4.2.5 An Example of Legislation Evolution

In this section we give an example for the legislation evolution. In the legislation model given in Chapter 3, this clause is modified:

An Organization shall not use the personal information of an individual unless a) it has the individual's consent and b) the information is necessary for ~~a lawful purpose.~~ providing required services or payment.

This clause already has a source link to its legislation GRL model. Therefore, the intentional element (task: Ask for Legal Purpose) related to this clause needs to be modified. After updating the legislation GRL model, the impact of this modification is traced through traceability link on the organization GRL. Via responsibility links between organization UCM and either of legislation or organization GRL, the effect of this change on the business process can be highlighted. Moreover, to check the detail of this modification, we can use the compliance link.

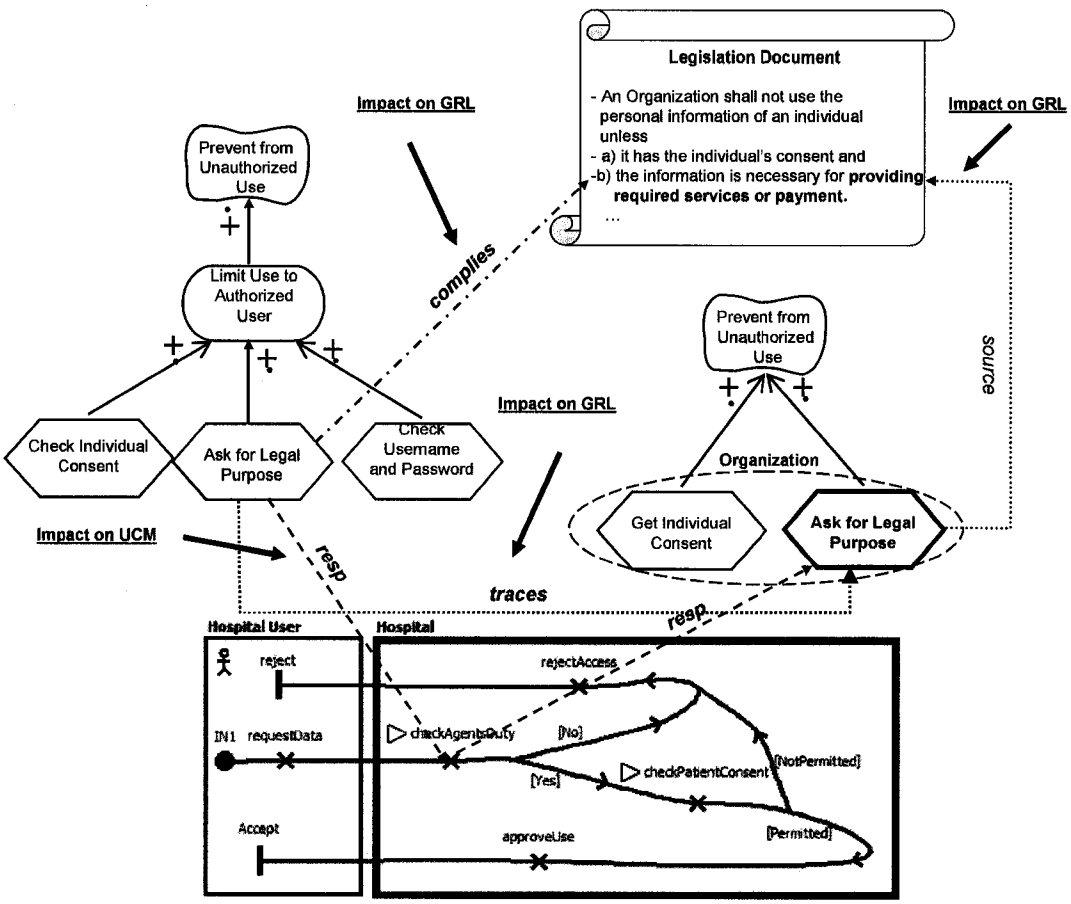


Figure 26 Modification of a Clause with Links

Figure 26 shows the links and possible modifications in the organization model. In this GRL model, the task, *ask for legal purpose*, can be change to "*check for payment or required services purpose*" and in the UCM model, the responsibility *checkAgentDuty* needs to become more specific or be transformed into a stub with a suitable sub-process.

4.3. Managing Evolving Business Processes or Policies

The business processes or policies of an organization are also susceptible to change. As they evolve, the organization needs to verify whether their business processes and policies still comply with the law and other applicable regulations. As illustrated in Figure 15, when a business process changes, it may directly impact the responsibility links connected to the organization or legislation GRL model. These, in turn, can also affect the source links, compliance links and traceability links. The impact on the above links has to be carefully managed in order to ensure that compliance is still maintained. Similarly, when policy documents change, this impact will be directly highlighted in the organization's GRL or UCM models via source links and then, through traceability, compliance or responsibility links, the compliance or non-compliance can be examined.

The following three cases are addressed in the evolution of policies and procedures:

1. An existing process or policy element is modified;
2. A new process or policy element is added; and
3. An existing process or policy element is removed.

In this section, we briefly explain each of these cases and the way they are handled.

4.3.1 Modification of an Existing Process or Policy

The modification of a business process is handled differently depending on which of the following two cases applies.

1. The existing process or policy has links to its corresponding GRL model as well as to the legislation GRL model. In this case, compliance can be quickly verified using the various kinds of links, i.e., responsibility links, traceability links, or compliance links.
2. The existing process or policy does not have links to its corresponding GRL model or legislation GRL model. In this case, it is necessary to check manually whether or not this modification is affected by components of legislation. In the unlikely event that it relates to the legislation, it becomes necessary to add links.

4.3.2 Addition of a New Process or Policy Element

When a new process element or policy is added to the model, the organization GRL model and the UCM model need to be updated and appropriate source links should be added. Then this GRL model will be compared with the legislation GRL model to determine whether this new element complies with the legislation or not or if it is irrelevant with respect to the law. If it is relevant, then the link sets need be updated as well.

4.3.3 Removal of a Process or Policy Element

When part of a business process or of a policy is removed, it becomes necessary to also remove all of its outgoing links (i.e. source links). In addition the related element in GRL model, the UCM model and responsibility link between them may also need to be deleted. If this happens and these elements are connected to the legislation GRL model by way of responsibility or traceability links, then the removal might result in an incomplete and non-compliant process. If no such link is present, then this part can be safely removed.

4.3.4 An Example of Business Process Evolution

In this section, we give an example for removing a part of the business process. In our previous model, we assume that the responsibility *checkAgentDuty* has been removed from the process (see Figure 27).

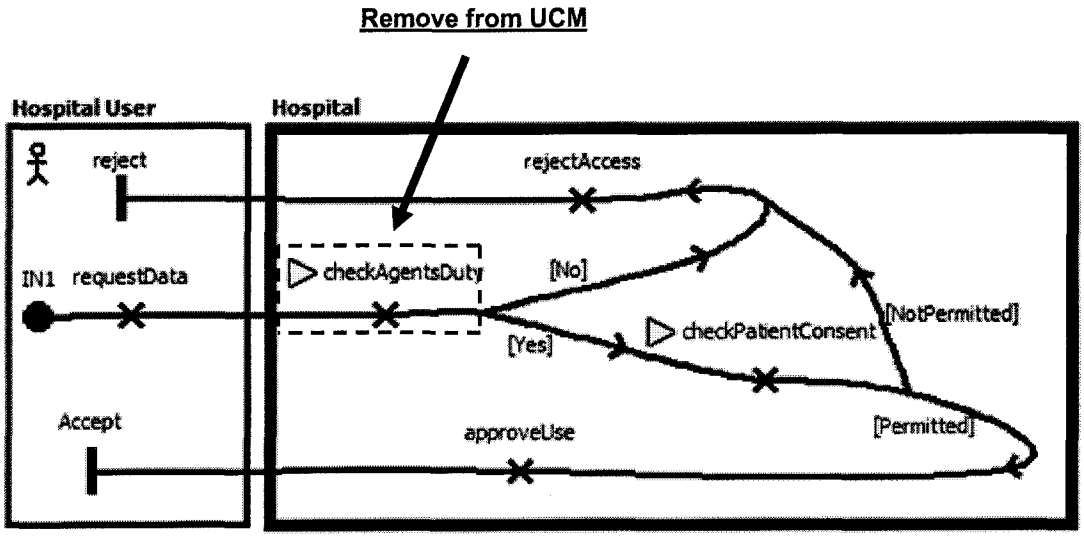


Figure 27 Changed UCM Model

As illustrated in Figure 26 this responsibility is connected to both organization and legislation documents via responsibility links. Having these links indicates that removing the responsibility may cause non-compliance to the legislation. Therefore, the organization may have to prevent removing the *checkAgentsDuty* responsibility from the business process.

4.4. Summary

In this chapter, we explained the usefulness of our framework in managing change as it affects (privacy) compliance. We defined several key scenarios of likely evolution to legislation and examined the resulting impact on the organization's business processes. Conversely, we also defined scenarios the manner in which an organization's business processes can change and demonstrated that using the framework links can help ensure that compliance is maintained with the legislation. Two examples were provided to illustrate each of these scenarios. In the next chapter, we analyze our framework by way of a case study derived from a business process in place at a major teaching hospital in Ontario.

Chapter 5. Case Study

In this chapter, we evaluate the compliance framework developed in this thesis by way of a case study. The case study is concerned with business processes followed at a major teaching hospital in Ontario. The business processes under scrutiny are those for accessing the hospital's data warehouse given the privacy legislation in place. Given that the hospital in question is in Ontario, the main applicable legislation is the Personal Health Information Privacy Act (PHIPA).

The case study will be analyzed in several ways. In Section 5.1, we will first evaluate a privacy compliance mechanism that uses existing documents to represent the business processes and privacy constraints. This manual yet realistic approach will serve as a baseline for further comparisons. A variation of this mechanism that uses DOORS as a tool to track privacy compliance with source privacy legislation documents is also considered. Next, in Section 5.2, we study a model-based approach that uses URN as the modeling language. An evaluation of the hospital's business process compliance with PHIPA is presented in Section 5.3 by instantiating our framework and all relevant models. Finally in Sections 5.4 and 5.5, we evaluate the framework in terms of its ability to handle legislative amendments and the hospital's evolution from a paper-based approval process to an online one.

5.1. Document-based Compliance

In this section, we give an overview of PHIPA and the hospital's process for granting access to its data warehouse. We will then compare these two elements in their paper form and evaluate how privacy compliance is established. This section refers to the section 3.1.1.

5.1.1 Personal Health Information Privacy Act (PHIPA)

PHIPA, the Ontario legislation for protecting personal health information, is divided into seven parts with a total of 75 sections. Each of these sections contains several rules which specify that health information custodians (e.g., hospitals) must obtain data with consent; that they use it only for the purposes stated; and that they do not disclose the data without the consent of the individual.

The main objectives of the PHIPA are as follows [13]:

- Establish rules for the collection, use and disclosure of personal health information about individuals that protect the confidentiality of that information and the privacy of individuals with respect to that information, while facilitating the effective provision of health care;
- Provide individuals with a right of access to personal health information about themselves;
- Provide individuals with a right to require the correction or amendment of personal health information about themselves,
- Provide for independent review and resolution of complaints with respect to personal health information;
- Provide effective remedies for contraventions. 2004, c. 3, Sched. A, s. 1.

Since PHIPA came into force in 2004, it has changed five times according to the amendments: 2005, c. 25, s. 35; 2006, c. 4, s. 51; 2006, c. 17, s. 253; 2006, c. 21, Sched. C, s. 128; and 2006, c. 34, Sched. C, s. 26.

5.1.2 The Hospital Approval Process

The process under study focuses on researchers as the main information users. Any researcher who wants to gain access to the hospital data warehouse has to go through an approval process. This process is mostly paper-based and consists of the following steps:

- **Submit a data request form:** When a researcher wants to gain access to the data warehouse, he has to submit a voluminous data request form. In this form, he has to specify the data he needs, the intended purpose for the data, the data safeguards in place, and how the data will be disposed of.

- **Review the data request form:** After receiving the request form, the hospital (acting as information custodian) will review the form to decide whether to accept the request or not. In order to complete this process, some sub-processes need to be performed. Initially, the request form is submitted to the data warehouse manager and the feasibility of the request data (i.e. the resources and data availability) is considered. Upon approval of the manager, the request form is submitted to the privacy officer so that it can be checked against existing privacy legislation and the decision to approve or reject the request is made. This decision is based on the hospital's privacy policies and relevant legislation documents. Along with the approval by the privacy officer, the request form is also reviewed by the research ethics board to check that it complies with their requirements. The board will check which data elements are identifiable or de-identifiable, that there are safe disposal mechanisms in place for the necessary identifiable data, and that the patient consent has been given. If the research ethics board approves the request form, the form will be submitted to the data warehouse administrator and the data warehouse support team. The data warehouse support team will check the technical competency of the researcher, the technical, administrative and physical safeguards he will use, and by when he needs the data. If these are acceptable, the support team will grant the access to the data warehouse based on the determined delivery method (paper reports, user ID and password, or files).
- **Amend the data request form:** At any of these steps, the form can be rejected and the researcher is then offered to amend the request and re-submit the form. Usually the rejection will occur as a result of the privacy officer review or research ethics board approval step. In these cases, the typical reason for rejection is an inability to grant access to all the data requested or that the stated data safeguards are not strict enough.

5.1.3 Manual Document-based Compliance

To perform manual document-based privacy compliance, the hospital has defined privacy policies on paper based on PHIPA, PIPEDA and other documents. Likewise, data access to the data warehouse is controlled by paper-based policies, processes and procedures

drafted by the hospital data warehouse team. The approach described in this section is currently implemented as part of the hospital business process for our case study.

Manual document-based compliance measures present several challenges. Although these documents exist and the hospital claims to protect patient privacy, there are few measures in place to verify exactly that their policies and procedures cover all the requirements of PHIPA. Even for the requirements that are addressed, it is necessary to be able to check that the coverage is complete. Considering also that the language structure of PHIPA is different from the language structure of the hospital policies and procedure documents, comparison between PHIPA and hospital policy documents becomes difficult. In addition, since both documents are in paper format, it is not possible to make permanent links between them. As a result, whenever the hospital needs to check one of its processes against PHIPA, it needs to examine the entire PHIPA document thoroughly.

5.1.4 Tool Supported Document-based Compliance

The tool supported document-based approach takes advantage of a requirement management system to collect, organize and link requirements in a database in order to establish and manage associations between documents.

In this approach the electronic versions of the PHIPA document and the hospital policy documents are imported into DOORS and links are established between them manually. Each of the purposes, goals and procedures described in the hospital policy documents are connected to relevant portions of the PHIPA document. The approach described here can be regarded as a potential solution for the creation of links between the approval process document and PHIPA document.

In our case study the hospital document is mainly connected to the part of PHIPA which relates to the *disclosure for research (PHIPA 2004, c. 3, Sched. A, s. 44).* An example of linked documentation is shown in Figure 28.

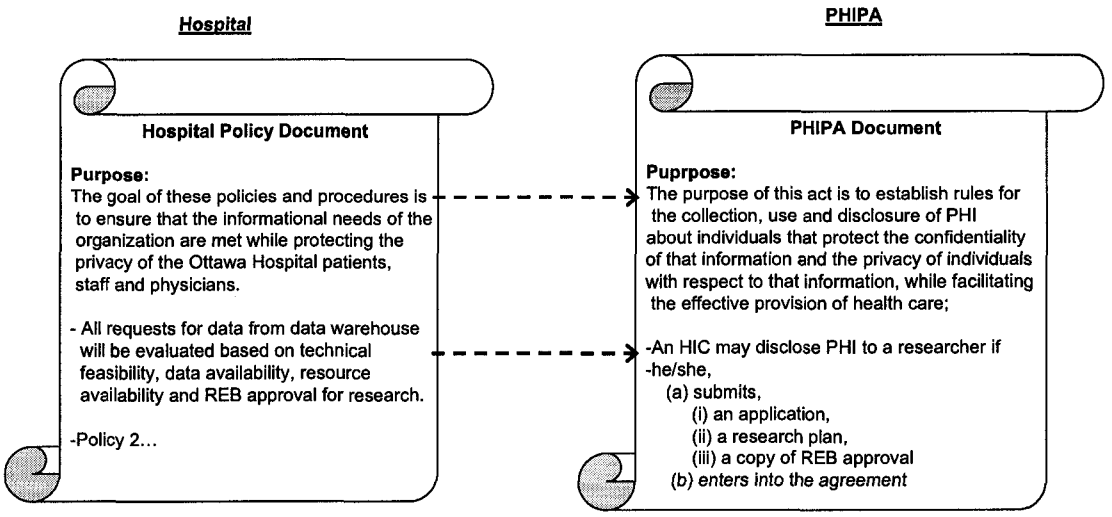


Figure 28 Links between Hospital and PHIPA Documents in DOORS

This approach is better than manual document-based compliance since the links provide some support for traceability. However, given the difference in the language structure and that goals and procedures are mixed in the hospital document, the usefulness of the links established is limited. Furthermore, this difference will result in inaccurate and ad-hoc linking. Therefore, this approach is not a good solution for a hospital.

5.2. Model-based Compliance with URN

In this approach, the PHIPA legislation and the approval process policies and procedures are modeled with URN (in jUCMNav). Each of the two parts is modelled separately. In the following sections, we first explain the steps required to model both documents and then we will examine whether the models help verify that the approval process complies with PHIPA. This section refers to the section 3.1.2 and 3.2.

5.2.1 PHIPA Model

In this section, we describe the URN model developed for PHIPA along with the steps taken to arrive at the final model. The model is provided based on the approach used in section 3.2.2. The PHIPA (GRL) model was built using jUCMNav.

In PHIPA, two major softgoals are defined to represent the two main purposes of this act. These softgoals are: "Satisfy Privacy Regulations and Protect Confidentiality" and "Facilitating Healthcare Provision." The first softgoal has other softgoals which contribute to its satisfaction. These softgoals are derived from the first section of PHIPA which states the *purposes* of the act. The contributing softgoals to the satisfaction of privacy regulations and confidentiality are: "Protect Personal Health Information", "Prevent from Unauthorized Collection, Use and Disclosure," "Provide Individual Right of Access," "Provide Right to Review," "Provide Effective Remedies for Contravention," and "Provide Individual Right for Correction." Each of these softgoals is related to a set of rules and obligations which are defined as goals or tasks. As for the second main softgoal "Facilitate Healthcare," it can be achieved if the data can be available in time. This goal, *availability of data*, translates into "Provide Necessary Data in Time" in the GRL model. An overview of these softgoals is shown in Figure 29.

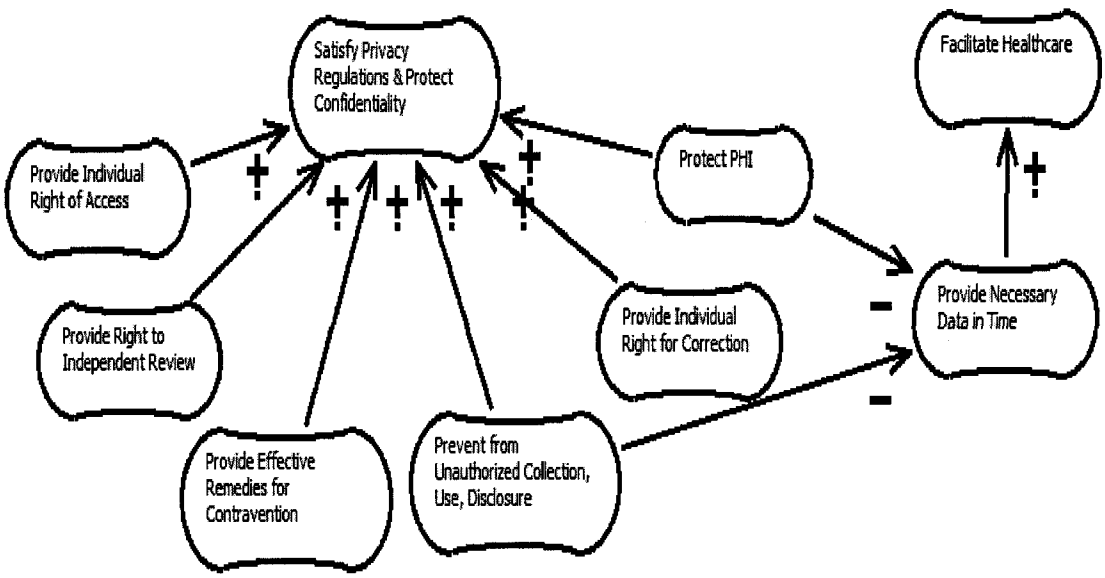


Figure 29 Overview of Main PHIPA Softgoals

In our case study, we modeled the part of PHIPA which relates to the *disclosure of data for research* (PHIPA 2004, c.3, Schedule A, s.44). The details of this section are provided in Appendix A. The rules related to the disclosure of data for research contribute to the softgoal "Prevent from Unauthorized Collection, Use and Disclosure" and are

modeled as tasks in GRL. For example in PHIPA 2004, c.3, Schedule A, s.44 (1), it is written:

A health information custodian may disclose personal health information about an individual to a researcher if the researcher

(a) Submits to the custodian,

(i) an application in writing,

(ii) a research plan that meets the requirements of subsection (2), and

(iii) a copy of the decision of a research ethics board that approves the research plan; and

(b) Enters into the agreement required by subsection (5).

This section is modeled with four tasks, "Submit an Application Form," "Submit a Research Plan," "Submit an REB Approval" and "Enter into an Agreement." Based on the above paragraph of section 44 of PHIPA, the related tasks are broken into different tasks. Figure 30 shows the relevant parts of the GRL model corresponding to this section.

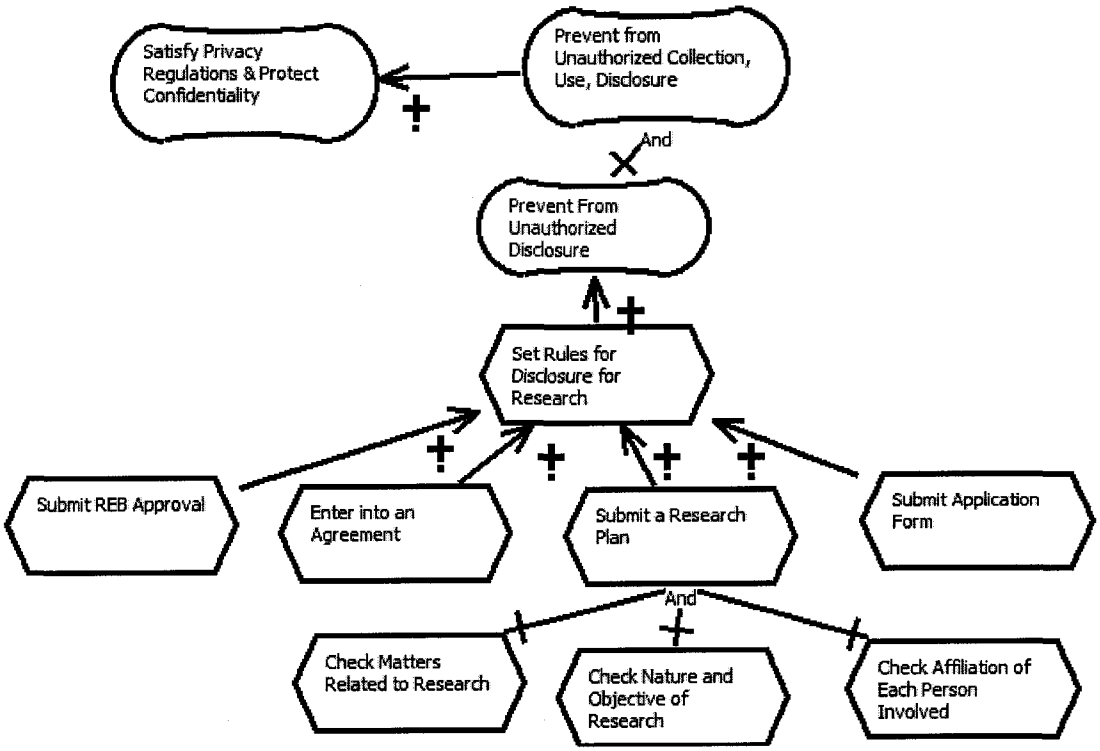


Figure 30 Disclosure for Research GRL Model

Further details regarding this PHIPA model are provided in Appendix B.

5.2.2 The Hospital Approval Process Model

The URN model of the hospital approval process is composed of both a GRL and a UCM model. In this section, we describe these models as well as the *responsibility* links between the GRL and UCM models. The hospital approval process model is built based on the approach taken in section 3.2.3The URN model is based on the approval process described in Section 5.1.2 and the hospital policies and procedure documents given in [9]. This URN model and the links are built manually in jUCMNav.

The GRL model provides a description of the policies and regulation documents the hospital has in place to protect the privacy of personal data stored in its data warehouse. A portion of the complete GRL model is shown in Figure 31. This model only shows some of the softgoals, goals and tasks for the hospital data warehouse team.

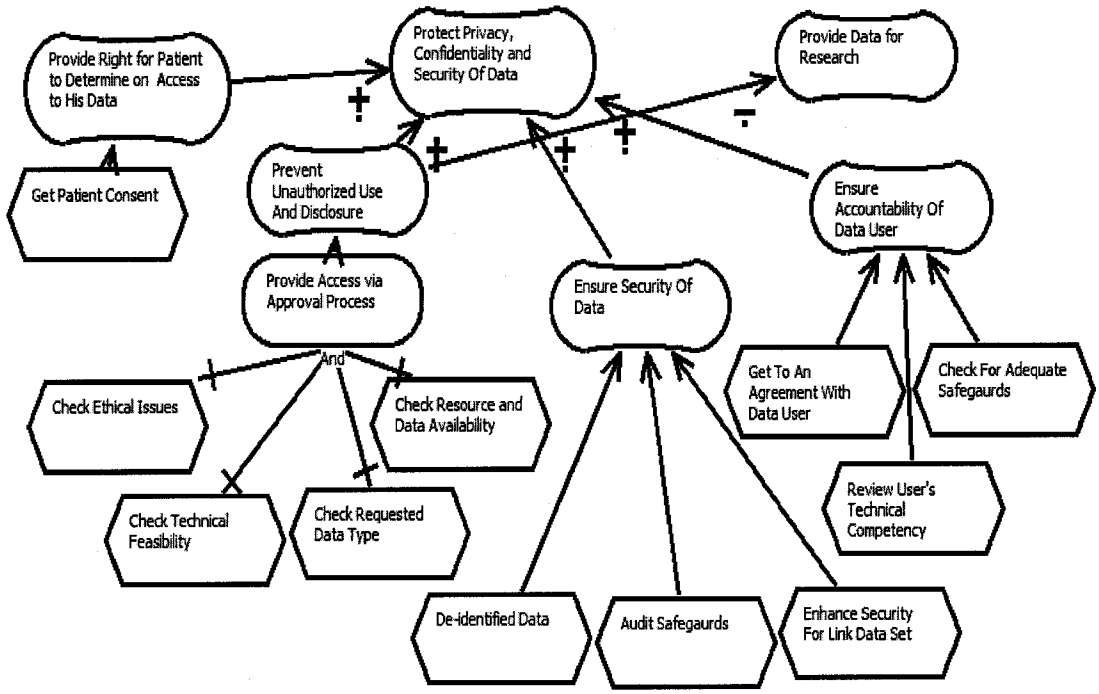


Figure 31 The Hospital Data Warehouse Partial GRL Diagram

The goal of the hospital data warehouse team is to ensure that the hospital is able to get the information it requires while protecting the privacy, confidentiality and security of the health data it manages. Therefore, the GRL diagram shows two main softgoals called "Provide Data for Research" and "Protect Privacy, Confidentiality and Security of Data." To achieve the first softgoal, the hospital data warehouse team must give permission to the researchers to access the data warehouse. On the other hand, they also need to satisfy the second softgoal which strives to protect data confidentiality. The hospital has instituted a set of rules and regulations to satisfy this softgoal. These rules and regulations are depicted as goals and tasks in Figure 31. Some of the softgoals and goals which contribute to this softgoal are: "Ensure Accountability of Data User," "Ensure Security of Data," "Prevent Unauthorized Use and Disclosure" and "Provide Right for Patient to Determine on Access to His Data". Each of these elements (either softgoals or goals) *helps* the hospital reach its main softgoal.

In addition, this GRL model shows how the general goals and concerns are allocated to the respective actors involved in the process. The main actors of the hospital data warehouse team are: the Research Ethic Board (REB Committee), the Data Warehouse Administrator, and the Privacy Officer. Each of these actors is involved in certain activities called *tasks,* which are in turn needed in order to reach the related goals. Figure 32, which focuses on a subset of Figure 31, shows how the tasks and goals can be allocated to actors in GRL.

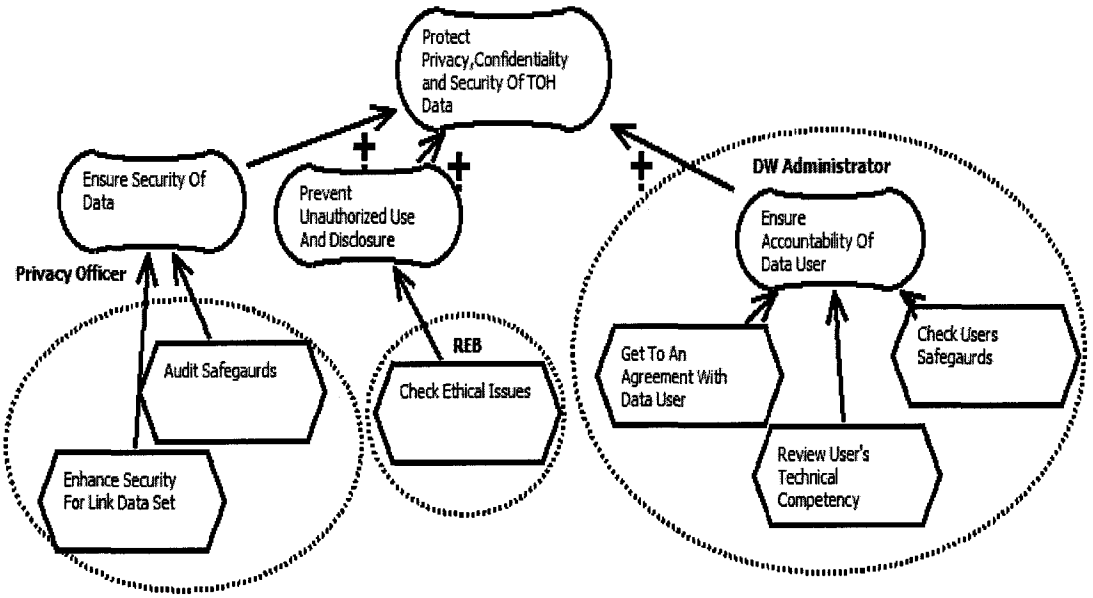


Figure 32 Partial Allocation of Actors in the Hospital GRL Diagram

In the next step the UCM model of the approval process is built. This UCM model includes a top-level (*root*) map, which gives a high-level overview of the process, together with six other sub-maps. This model is based on the approval process explained in Section 5.1.2. The complete UCM model is presented in Appendix C.

The root map (Figure 33) shows the causal relationships necessary between the researcher and the hospital in order to get health information from the data warehouse. This map contains "Request for PHI" and "Review Request" stubs (shown as *diamonds)* which represent the "Submit a request form" process and "Review the Data Request Form" process.

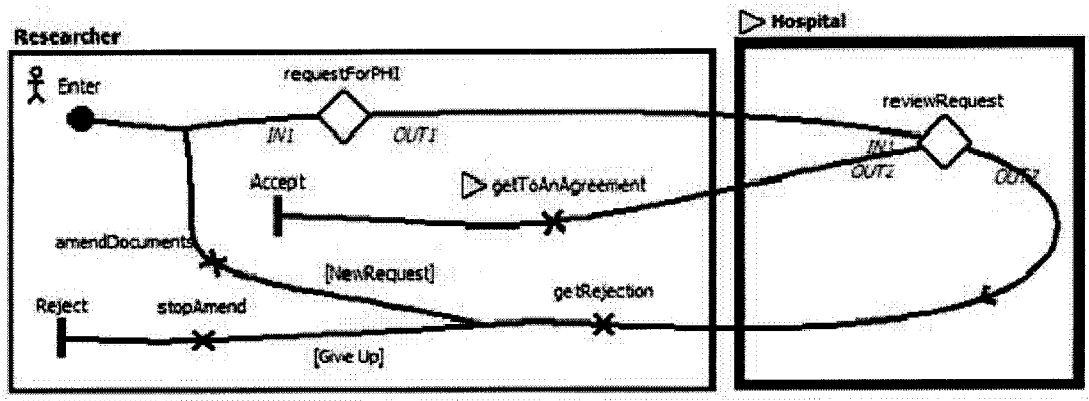


Figure 33 Top-Level Map

In the following sub-maps, the interaction between the individuals and the teams in charge of the approval process (privacy officer, data warehouse administrator, research ethics board, and data warehouse support teams) and the researcher is modeled. For example, Figure 34 shows the "Review Request" sub-map. This sub-map includes a "Privacy Officer Review" sub-map (inside the "CPO Review" stub), a "Research Ethics Board Approval" sub-map (inside the "REBApproval" stub), and a "Review Request Technically" sub-map (inside the "technicalReview" stub), which collectively represent the processes that have to be taken to get approval. These processes are detailed in Appendix C.

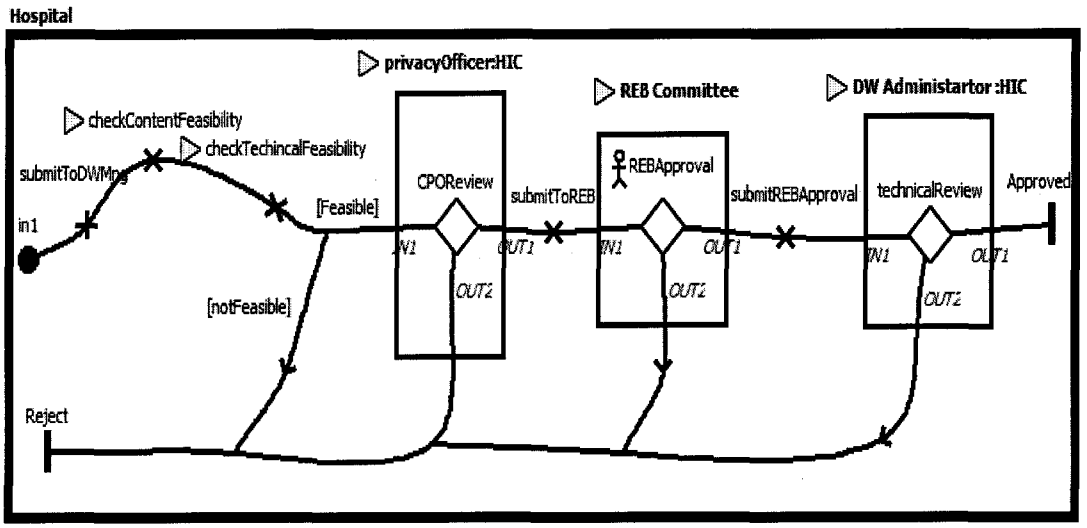


Figure 34 Review Request Map

The responsibility links between the UCM diagrams and the GRL model are created manually inside jUCMNav (which indicates the presence of a link with a triangle next to the corresponding UCM element label). For instance, Figure 35 illustrates responsibility links between the elements of the map "Review Request Technically" and the GRL model for the hospital. In particular, there is a link between the UCM component "DW Administrator" and the GRL actor "DW Administrator." Also shown is a link between the UCM responsibility "checkTechnicalCompetency" and the GRL task "Review User's Technical Competency" (contribution levels are hidden to simplify the GRL diagram)."

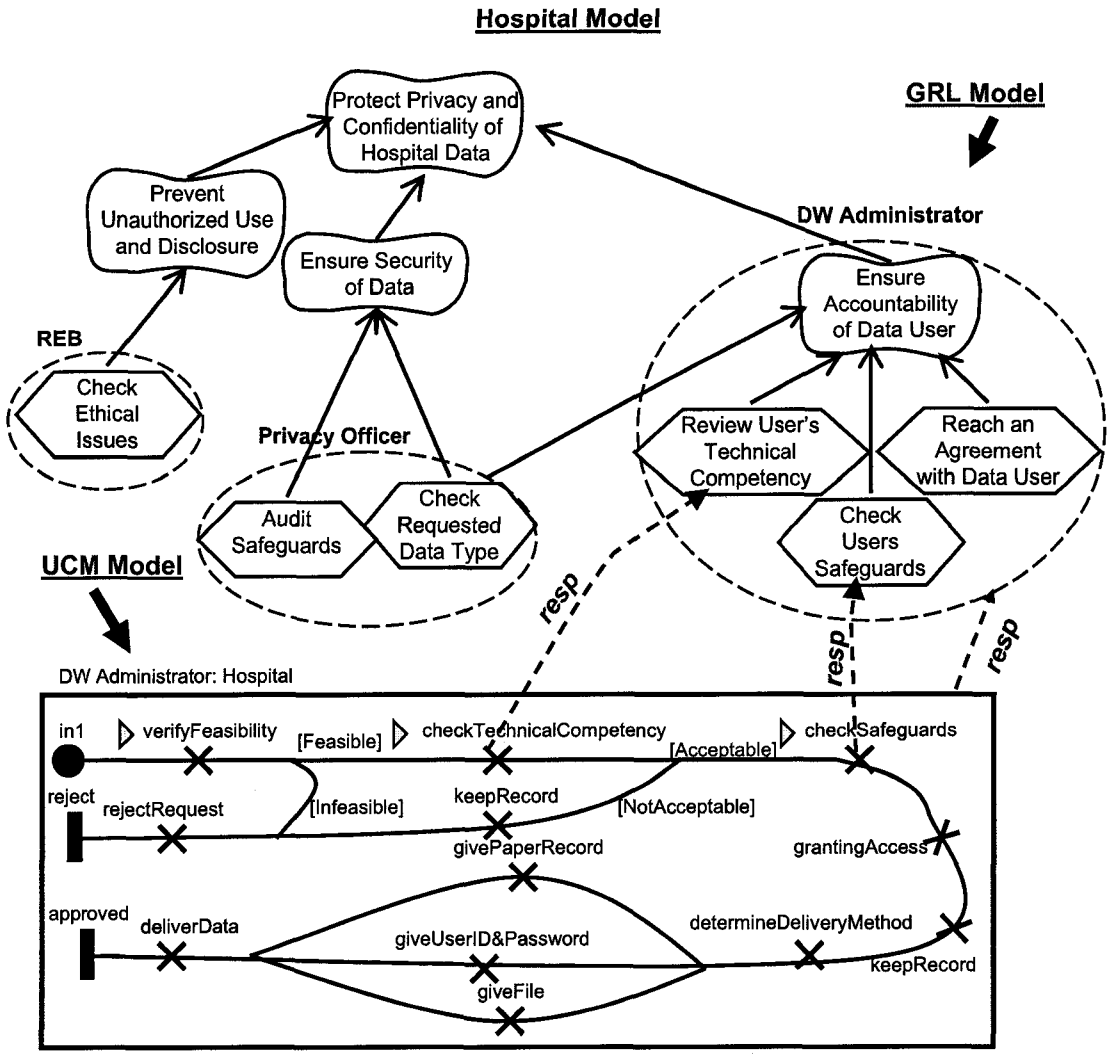


Figure 35 Responsibility Links between Hospital GRL and UCM

5.2.3 Manual Model-based Compliance

In this approach, we modeled both the document for the approval process and PHIPA with URN. As already stated, having a compact model helps increase the degree of comprehensibility in comparison to verbose source documents. The model serves to organize the documentation of the hospital process and PHIPA by defining goals, tasks, actors and relationships between them. However, despite having these models, verifying privacy compliance is difficult without a way to link them together. If they reside as separate files, the two models must be compared manually, which can be difficult and prone to

errors. What is needed here is a mechanism to link the PHIPA model to the hospital process model in order to exploit the relationships that exists between these two elements.

5.2.4 Tool Supported Model-based Compliance

Given the weaknesses of the manual model-based compliance method, we turn to tool support to provide a better alternative. Using the two URN models presented in this section, one for the hospital data request approval process and the other for the PHIPA legislation, we can use an RMS such as DOORS to support the appropriate links. The two models are first imported into DOORS and then links are established between them. However, at this stage the PHIPA and hospital process source documents are not imported into DOORS. Therefore, using only the imported models, we establish only traceability and responsibility links.

To establish traceability links, the actors and intentional elements of the PHIPA URN model are linked to the corresponding elements of the hospital URN model. As for the responsibility links, they are used to connect the actors and intentional elements of the PHIPA URN model to the components and responsibilities in the hospital URN model.

5.3. Compliance of Hospital to PHIPA Model

In this section, we examine the privacy compliance mechanism of the full compliance framework (section 3.2.4). This mechanism verifies that the hospital approval process agrees with the PHIPA model and documentation. The framework itself is the combination of the tool supported documents-based and model-based approaches. It provides both links between the URN models and their source documents and between the hospital model and the PHIPA model. In our framework, we identify 3 types of links for traceability, responsibility and compliance. Once the models are exported to DOORS, these links are used to create relationships between PHIPA and the hospital model. It is with this framework that we are able to evaluate the policies and procedures of the hospital and make sure that they are in concordance with the PHIPA act, and that relevant PHIPA clauses are addressed adequately.

The links between the models and the source documents are what allows the framework to manage privacy compliance. Traceability links, which exist between the

hospital's GRL model and PHIPA's, are manually added in DOORS. These links can be added easily since they exist between two GRL models described at the same level of abstraction. These links help us analyze the hospital model and make a better comparison between hospital policy documents and PHIPA documents. An example of the traceability links between the two models is provided in Figure 36.

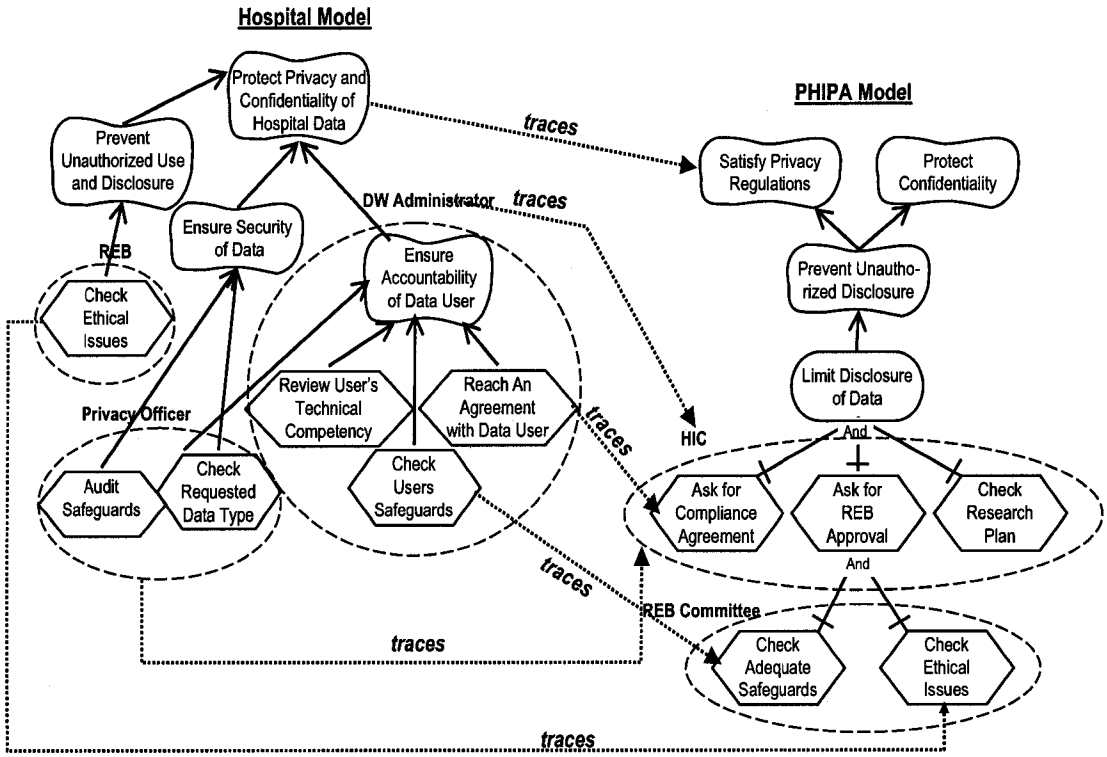


Figure 36 Part of the Traceability Links

As illustrated, most of the elements of the hospital's GRL are connected to a corresponding element in the PHIPA GRL. For example the actors *data warehouse administrator* and *privacy officer* are connected to the *HIC (Health Information Custodian).* Tasks such as *get to an agreement with data user, check users' safeguards* and *check ethical issues* in the hospital's GRL model are linked to tasks *ask for compliance agreement, check adequate safeguards* and *check ethical issues* in the PHIPA GRL model. The existence of these links is evidence that there is some measure of compliance in place.

However, by examining the traceability model, it is clear that some elements do not have any corresponding links and are possible sources of non-compliance. One such element is *check the research plan.* In PHIPA, one of the requirements for enabling the disclosure of data to a researcher is to have him submit a research plan in addition to the application form. However, in the hospital GRL model, there is no task demonstrating this requirement clearly. This is a critical symptom for the hospital approval process. It shows that the hospital may not thoroughly comply with PHIPA. As a result, the hospital needs to add this task to its model and update its business process and policies to satisfy this requirement.

There is also the possibility that some tasks performed by a specific actor in the hospital model are supposed to be handled by a different actor according to the PHIPA model. For example PHIPA specifies that the task, *check for adequate safeguards*, is the responsibility of the REB committee. This task, however, is being performed by the DW Administrator at the hospital. These discrepancies may lead to changes in the hospital model and clarification of the processes that implement the tasks.

Compliance links, which connect the hospital GRL elements to the PHIPA source document, can be established automatically. This link type helps to illustrate any details of PHIPA including exceptions and definitions that cannot be modeled using GRL or UCM notation. For example in the *disclosure data for research* section of PHIPA, specifies the requirements of the researcher who is granted access to personally identifiable information. It states:

Compliance by researcher: A researcher who receives personal health information about an individual from a health information custodian under subsection (1) shall,

(a) Comply with the conditions, if any, specified by the research ethics board in respect of the research plan;

(b) Use the information only for the purposes set out in the research plan as approved by the research ethics board;

(c) Not publish the information in a form that could reasonably enable a person to ascertain the identity of the individual;

(d) despite subsection 49 (1), not disclose the information except as required by law and subject to the exceptions and additional requirements, if any, that are prescribed;

(e) Not make contact or attempt to make contact with the individual, directly or indirectly, unless the custodian first obtains the individual's consent to being contacted;

(f) notify the custodian immediately in writing if the researcher becomes aware of any breach of this subsection or the agreement described in subsection (5); and

(g) Comply with the agreement described in subsection (5).2004, c. 3, Sched. A, s. 44 (6).

This section of PHIPA specifies extra conditions for the researcher's accountability and gives the information about the detail of the agreement signed by the researcher. In order to address this extra information, we use a *compliance link* between the task *get to an agreement with data user* and this section of PHIPA. Figure 37 shows this and other compliance links between various elements of the hospital and PHIPA models. For instance the actor *DW administrator* has a link to the definition of HIC which provides some detail information about the health information custodian and help to verify if the data warehouse administrator is a part of health information custodian or not.

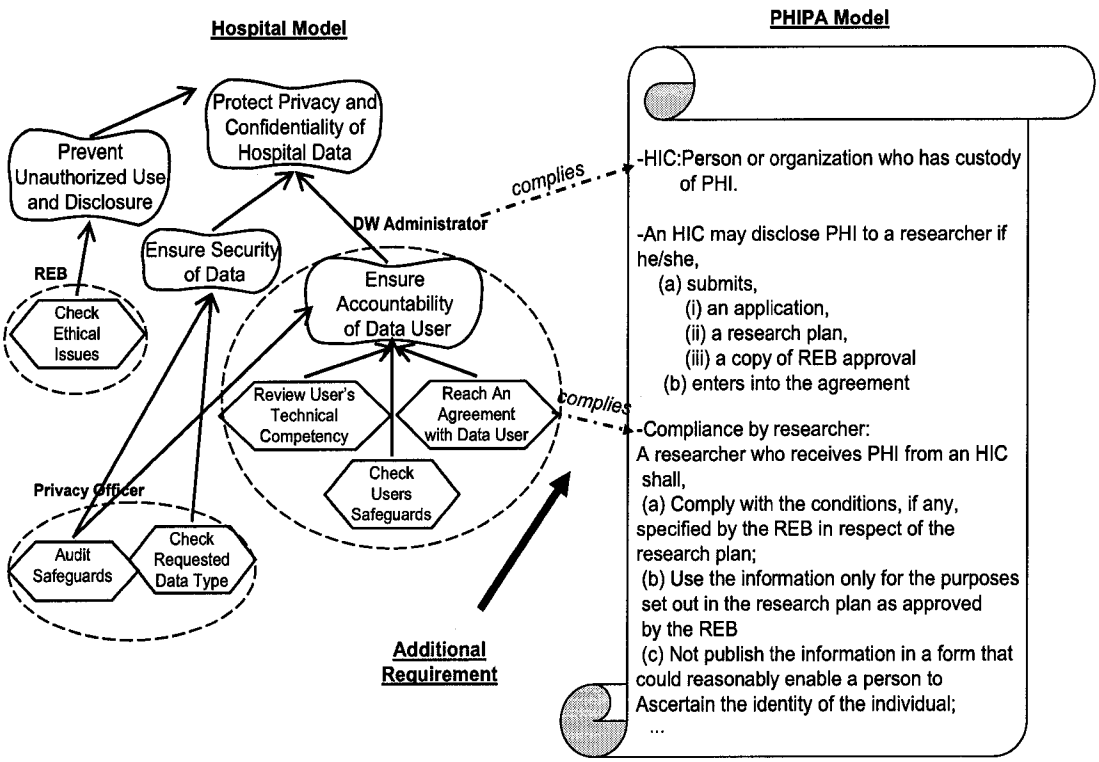


Figure 37 Part of the Compliance Links

Responsibility links are created between the hospital UCM elements and the PHIPA GRL elements. These links are formed between responsibilities, components and maps in the hospital approval process model and tasks, actors, goals and softgoals in the PHIPA model. Some of these links are added manually and some are added automatically. This link type is similar to the traceability type in terms of its utility. In Figure 38, responsibility links are labelled "resp" and are shown to connect UCM elements to the PHIPA GRL model. For example, the responsibilities *checkSafeguards* and *submitREB-Documents* are linked to their corresponding tasks *check adequate safeguards* and *check research plan.* Also shown are the responsibility links that connect the *hospital* and *data warehouse administrator* elements to the *HIC* actor.

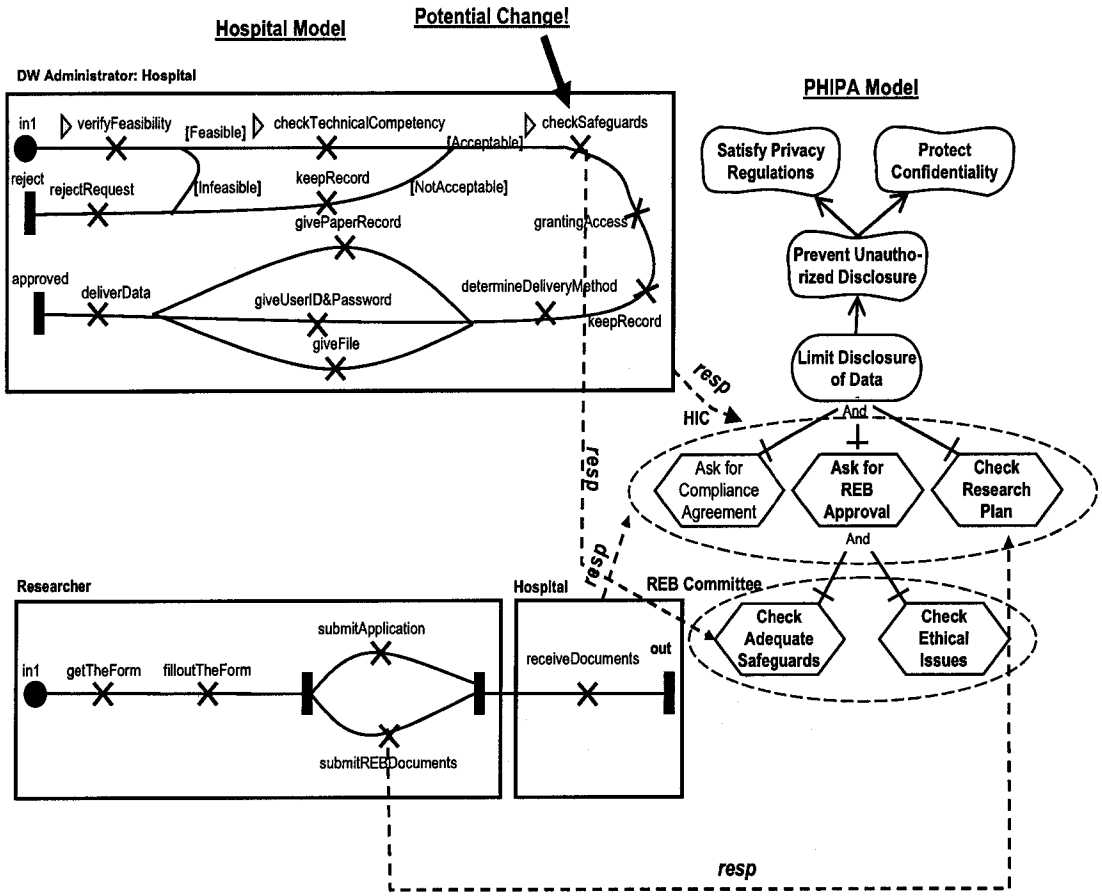


Figure 38 Part of the Responsibility Links

As explained before, one item of potential change relates to the task, *check adequate safeguards*. According to PHIPA, this task should be performed by the Research Ethics Board (REB). However, as seen in Figure 38, the corresponding responsibility *checkSafeguards* indicates that it is the data warehouse administrator who should be responsible for it. This instance of potential non-compliance can be address by revising the UCM model and moving the *checkSafeguards* responsibility to a different part of the process (i.e. to the REB component).

5.4. Compliance as Legislation Evolves

The true strength of our framework comes through its ability to manage changes to either the business process or to the law. In this section we explain how our framework is able to handle amendments to the PHIPA act. The cases explains here are based on the scenarios described in section 4.2. We use actual changes to the act and examine their impact on the approval process.

In one of the PHIPA amendments [12], two clauses are added to the section *disclosure by researcher.* One of the clauses specifies additional requirements for the research plan that was previously specified in *PHIPA 2004, c. 3, Sched. A, s.44 (2)* clause[1]. Since this new clause refers to the research plan task (shown in the PHIPA GRL model), there is already a source link between it and the new requirements. However, the research plan task has already been broken into several other tasks which represent the requirements for the research plan. Therefore, to cover the new requirements in the GRL model, it is necessary to add new tasks. The effect of this change on the hospital model can be traced through its different pre-existing links with the PHIPA GRL model. Note that the hospital model shown in Figure 31 has already been refined according to this amendment. Therefore, it already includes the research plan task.

The legislation task *ask for research plan* has a traceability link to the task *check research plan* in the hospital GRL model, which in turn has a responsibility link to the stub *submitREBDocument* in the UCM (Figure 39). Therefore, the hospital model needs to add the related tasks to its GRL model and appropriate responsibilities to the plug-in map *submitREBDocument.* The compliance link just gives the details of this modification.

[1] The complete requirements are presented in Appendix D.

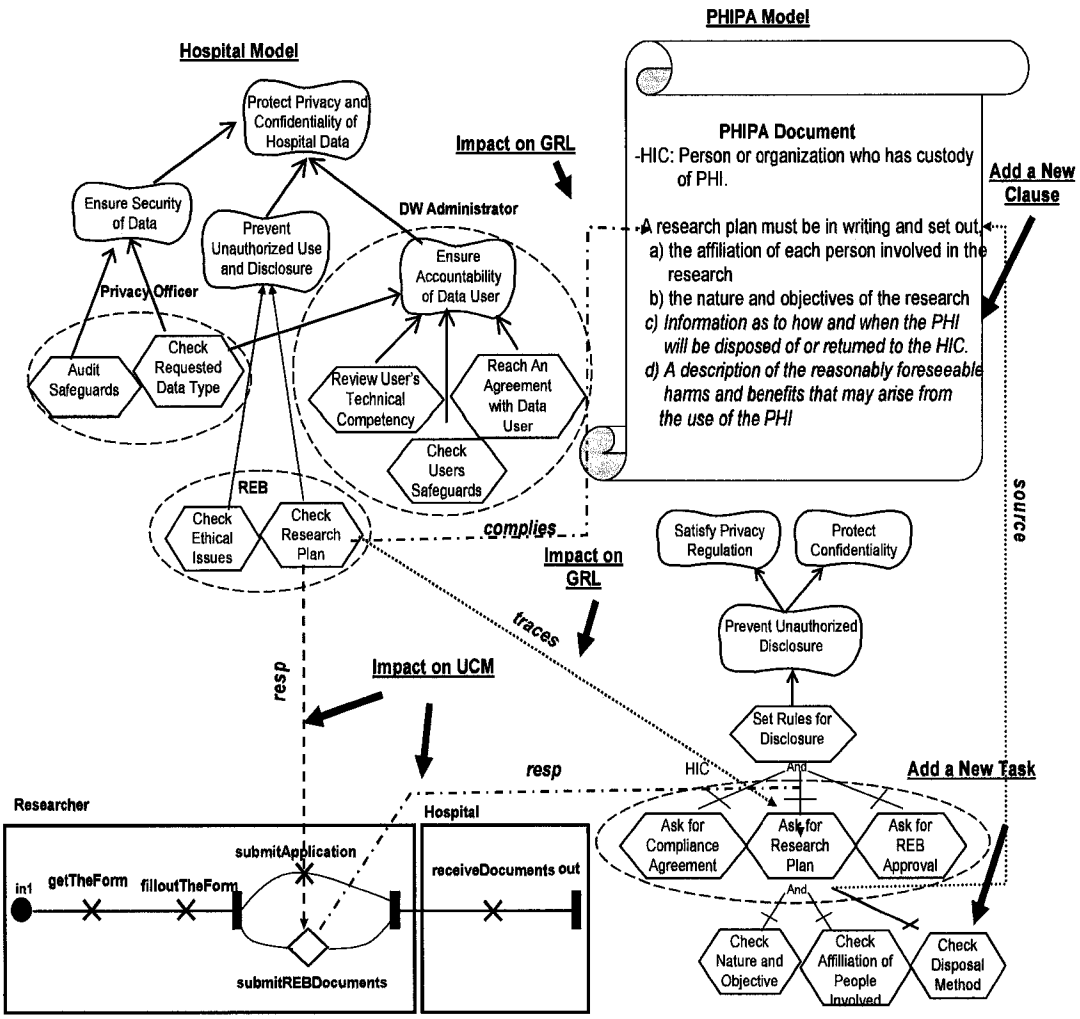


Figure 39 An existing Clause Modified

Another change in the section *disclose for research* is that the clause *disclosure by researcher* was added to the Compliance by Researcher, 2004, c. 3, Sched. A, s.44 (6) clause. This new clause refers to an existing intentional element, namely *Ask for Compliance Agreement*, in the PHIPA GRL model and it only serves to give further explanation. As a result, it is not necessary to add any new intentional element to the PHIPA GRL model. It is only necessary to establish a new internal source link between the task and the clause. However, this intentional element is linked to the hospital GRL model via the *Reach an Agreement with Data User* task, and indirectly to UCM models via responsibil-

ity links. Therefore, with the help of these links, we can trace that the Researcher-Root map and the responsibility *getToAnAgreement* (with the researcher) have to be revisited in order to ensure their compliance with the new legislation. An overview of the impact of this change is shown in Figure 40.

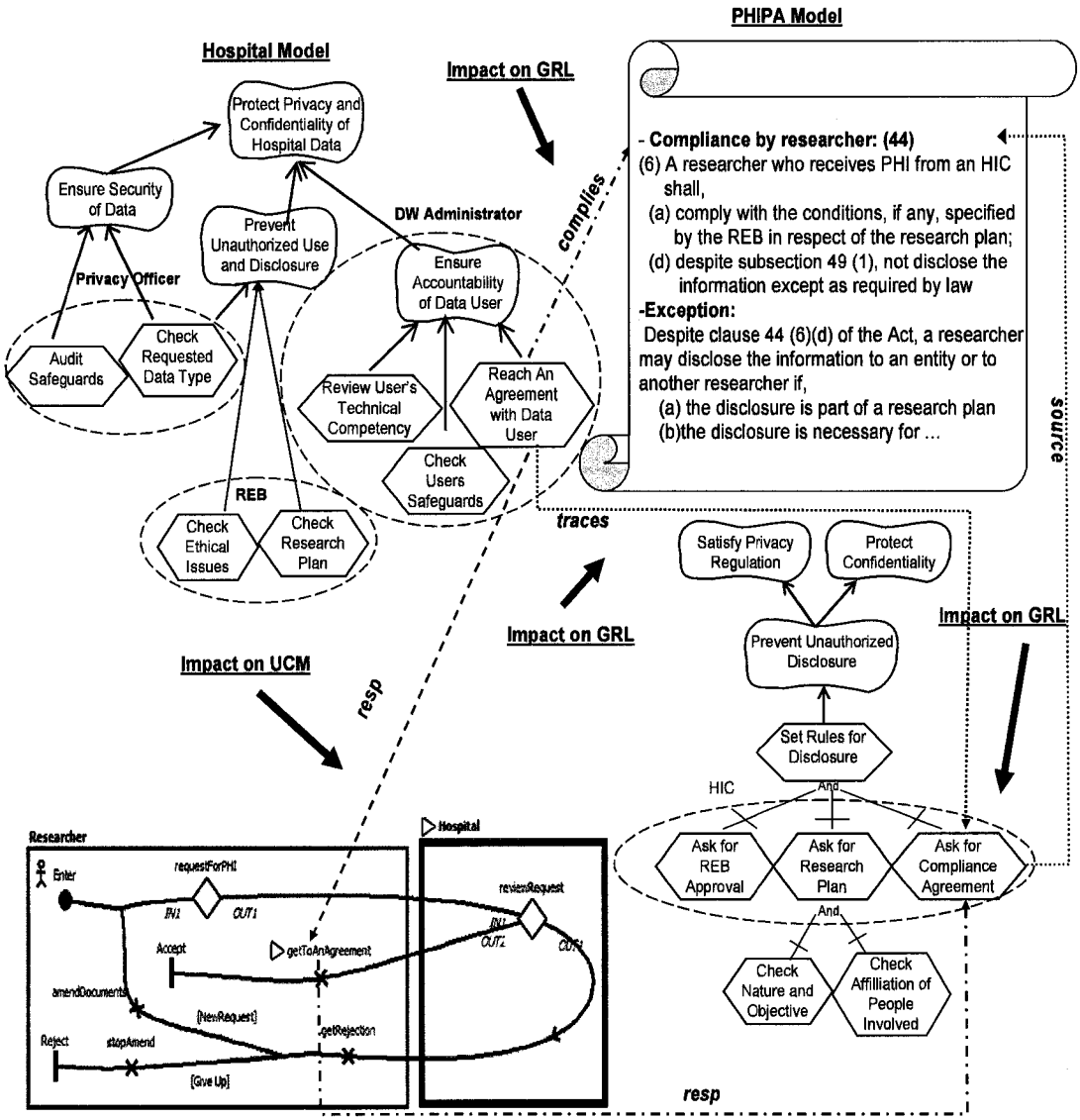


Figure 40 Modify a Clause with Links

In addition, in the latest version of PHIPA, some clauses have been repealed, in particular PHIPA 2004, c. 3, Sched. A, s. 44 (12) and 2004, c. 3, Sched. A, s. 44 (13). The former stipulates details for the transitional period after the law took effect:

Transition:

Despite anything in this section, a health information custodian that lawfully disclosed personal health information to a researcher for the purpose of conducting research in the three-year period before the day this section comes into force may continue to disclose personal health information to the researcher for the purposes of that research for a period of three years after the day this section comes into force.

However, in our model there were no links between this clause and the GRL models. Therefore, the fact that this clause was deleted does not have any impact on the compliance.

5.5. Compliance as Business Processes Evolve

Here we give three examples from our case study that illustrate how the framework can be effective in the face of process change. The first relates to the removal of a responsibility from the business process model. The second is concerned with the modification of a responsibility in the model with links to the PHIPA model. The last example deals with the change where the approval process is converted into an online format.

5.5.1 Removal of a Responsibility with Links

It was suggested that in order to save time during the approval process, one of the responsibilities, *check data feasibility*, could be deleted from the *review request technically* map. This responsibility determines whether the combination of the requested data can result in individuals being identifiable.

This responsibility relates to the task *check data feasibility* via a responsibility link. In Telelogic DOORS, it is not possible to delete an object without first deleting the objects related to it through an out-going link. Therefore, if a responsibility has a link to a part of the legislation, DOORS will prevent deleting this object without first deleting the links to the corresponding object in the legislation model. This responsibility, however, is connected to a sub-task of the research plan in the PHIPA GRL model, namely *check possible linkage of PHI*. Since there is a link between this responsibility and the PHIPA task, the deletion of the responsibility would violate compliance to PHIPA.

5.5.2 Modification of a Responsibility with Links

To evaluate the effect of modifying a responsibility with links, we chose the responsibility *check safeguards* in the *Research Ethic Board review* map. We suggested that it was beneficial to make it more specific and required it to check *physical* safeguards only. This change is illustrated in DOORS by the display of a (red) change bar (Figure 41).

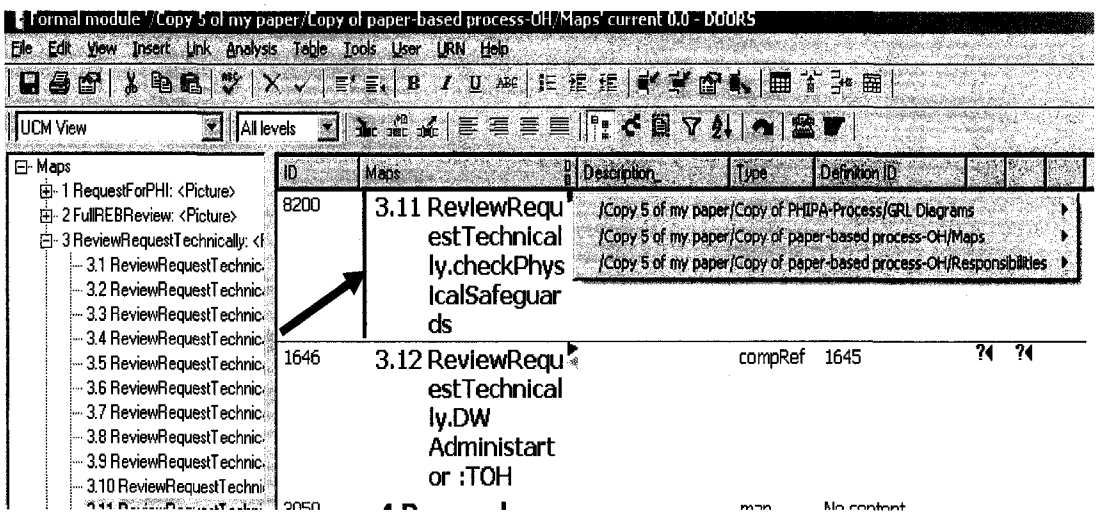


Figure 41 A Responsibility Changed

As indicated by the arrows, this responsibility has some links to the hospital GRL task and to the PHIPA GRL task *check for Adequate Safeguards*. As a result, this task is flagged by a suspect link (as shown by the "?◀" symbol in DOORS, see Figure 42), which indicates that attention must be paid to this element in terms of reassessing compliance. Suspect elements can easily be emphasized by DOORS.

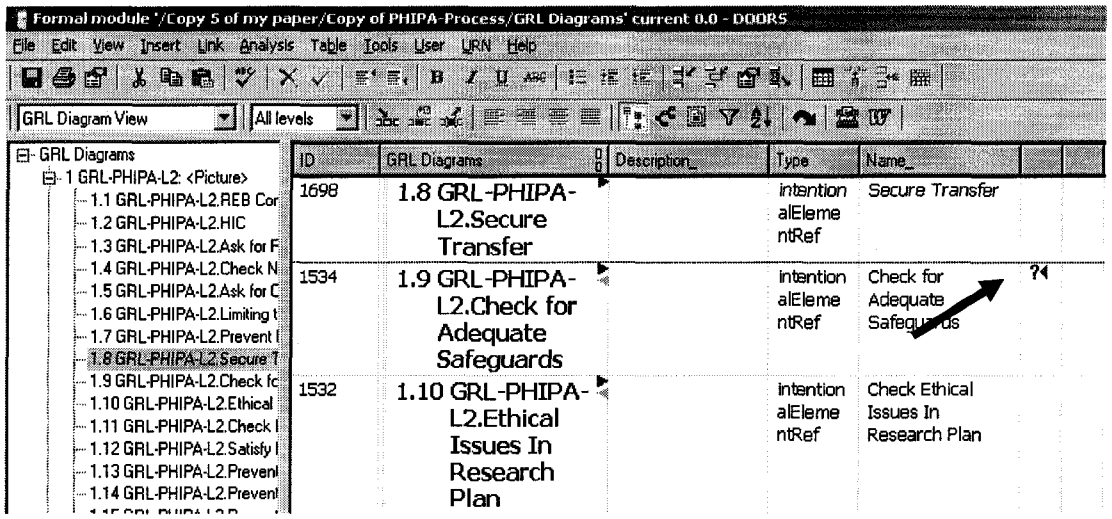


Figure 42 Related PHIPA Elements

Finally, through the source link, the related PHIPA rule can be traced. This task does not restrict itself to any specific safeguard in *PHIPA 2004, c. 3, Sched. A, s. 44 (3) b.* The Research Ethic Board, therefore, is required to check all types of safeguards, not only physical ones. As a result, the modification would result in non-compliance with PHIPA.

5.5.3 Toward an Online Approval Process (Addition of a New Sub-Process)

In this section, we evaluate our framework based on the hypothesis that business processes change over time. To perform this evaluation, we consider the case where the access business process evolves from its current paper-based approval process into computer-based online process. Such a project was actually prototyped two years ago at the University of Ottawa [23].

The main difference between the online approval process and the paper-based approval process is that a new step "Collaborative Review Process" was added. This process is defined as a sub-process to the "Privacy Officer Review" process. As can be observed from Figure 34, there are 3 steps in the approval process in which the request form is reviewed. If at any point during these steps there is a problem with part of the request, the form can be rejected and the researcher is required to amend his written paper request and resubmit it. There is the potential for several iterations that can lead to a significant

amount of delay. The delay could become even worse considering the fact that a paper document has to physically move from individual to individual for each step of the process, and could potentially have to be rewritten every time the request is amended. The collaboration interface intended to help reduce this delay. The proposed collaborative process, shown in Figure 43, would allow the researcher and the reviewer to flexibly submit comments that each could view either asynchronously or in real-time. Together, they could edit and review the application online until it can be approved. The approval by both the researcher and the reviewer would then be formally recorded and signed electronically.

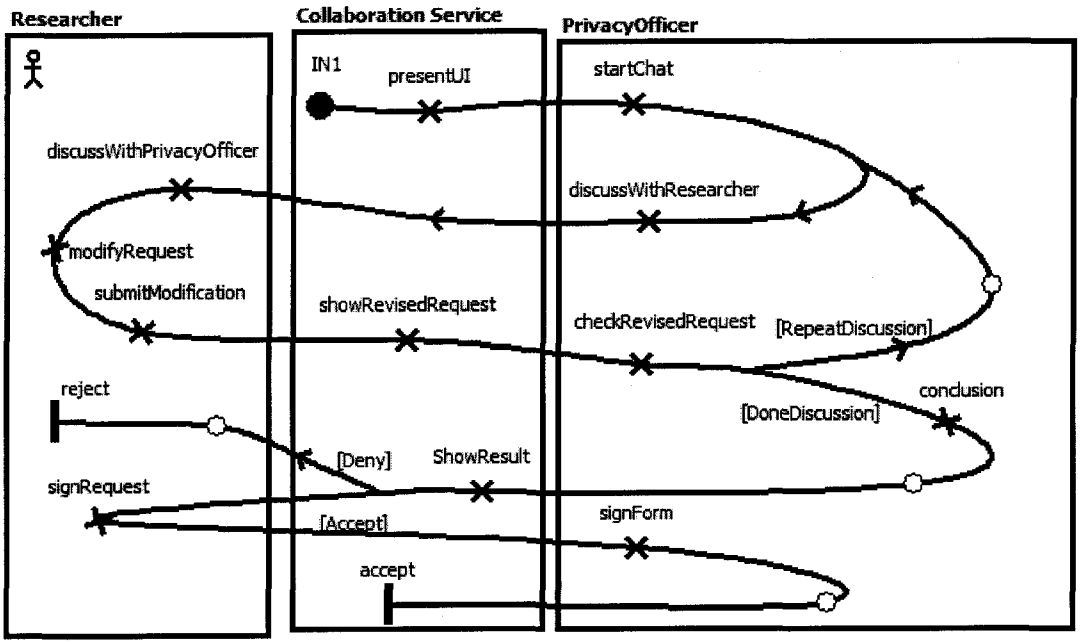


Figure 43 Collaborative Review Process

In our case study we added this map to the paper-based process and made necessary changes in the root map (Figure 44) and the privacy review map, and exported them to DOORS to check the impact of this change on the compliance of the process. In doing so, we examine the two cases identified in Section 4.3.

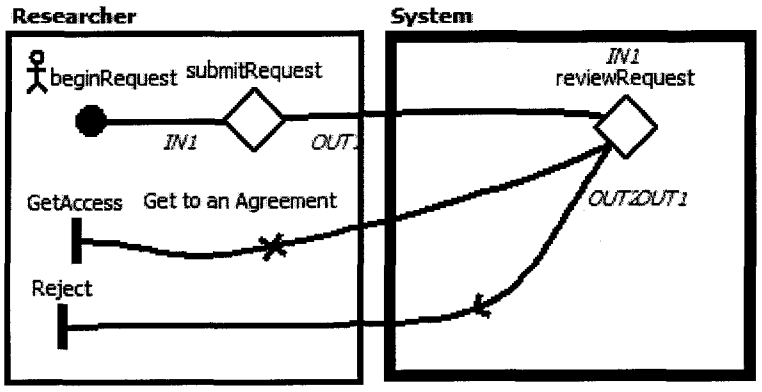


Figure 44 New Root Map

As shown in Figure 44, the responsibility, *amendDocument* has been deleted. However, since this responsibility does not have any link to the hospital GRL or PHIPA GRL models, this change does not result in any non-compliance and therefore its removal is permitted.

In addition, the newly added map, *Collaborative Review Process*, is involved in checking the request form with the legislation to verify the compliance. Therefore, this map and its responsibility *check revised request,* have to be connected to the task, *check requested data type* via a responsibility link. Compliance to PHIPA can be re-established for this improved process.

5.6. Summary

In this chapter, we evaluated our framework through a case study at a major hospital in Ontario. We examined the document-based approach and then described how to build URN models for privacy legislation and for the organization and then established links between these two models. We also examined the framework in terms of handling legislative amendments and business process evolution. In the next chapter, with the help of some criteria, we compare our framework with document-based and model-based approaches, as well as with other related methods.

Chapter 6. Analysis of Results

This chapter provides an evaluation of our compliance framework by comparing it to other available approaches for managing compliance to regulatory documentation. The approaches considered were introduced in Section 3.1:

- Manual document-based compliance;
- Tool supported document-based compliance;
- Manual model-based compliance;
- Tool supported model-based compliance; and
- Our full framework (tool supported, document and model-based compliance).

In terms of the evaluation, the criteria by which we will analyze the different approaches are:

- Effort to model;
- Effort to comprehend;
- Effort to document compliance;
- Effort to manage evolution;
- Level of coverage for the model;
- Level of coverage for compliance documentation; and
- Level of coverage for the evolution management.

In Section 6.1, we define the above criteria in detail. In Sections 6.2 to 6.8 we evaluate the different approaches based on each of the defined criteria. In Section 6.9 we summarize the results of the evaluation and in Section 6.10, we provide a comparison with related methods.

This evaluation does not attempt to quantify or measure the overall benefits associated with adopting any of the approaches. It rather provides an examination of the relative effort and coverage provided by each. Since the analysis is relative in nature, it is not necessary to perform experiments to generate raw data to demonstrate the level of effort (by recording the time required) for example. To do these experiments would require

each of the approaches described to be implemented in an environment where privacy compliance was already in force and compare their success. The same difficulty would apply to quantifying the overall benefit to privacy compliance for the adoption of a particular approach. In [10], for example, the method applied to numerically evaluate their organization's compliance model is to measure metrics such as "the rate of calls to our (complaints) hotline" and "how promptly does the compliance officer addresses these calls". In [32], Tousaw presents a legal model for privacy compliance. He argues the need to "logically speculate" rather than provide numbers to demonstrate that a particular model would aid in the task of privacy compliance. As he further explains, the only method available to quantify the success of a compliance model is to compare results obtained from privacy auditors. Such an evaluation is beyond the scope of this thesis.

6.1. Definition of Evaluation Criteria

This section defines the criteria that are used to evaluate our framework and compare it with the other four compliance approaches identified.

6.1.1 Effort to Model

This criterion examines the amount of effort needed by organizations to establish a model for managing compliance. It is a combined measure of both the effort to model business processes and the effort to model legislation. In cases where there is no formal model, such as with document-based approaches, the value of this criterion is zero since no model is needed.

6.1.2 Effort to Comprehend

This criterion examines the amount of effort needed by organizations to understand their business processes and applicable legislation. Most importantly, it measures whether or not the organization's processes comply with the legislation.

6.1.3 Effort to Document Compliance

This criterion examines the amount of effort needed by organizations to verify whether their processes comply with the legislation.

6.1.4 Effort to Manage Evolution

This criterion examines the amount effort needed by organizations to verify their compliance and find potential instances of non-compliance when legislative documents are amended or when their policies and business processes change.

6.1.5 Coverage of Model

This criterion examines how much of the law and how much of the policies and business processes can be modeled for each of the different approaches.

6.1.6 Coverage of Compliance Documentation

This criterion examines the level of success each approach brings to the organization in terms of documenting the compliance and ensuring compliance to the legislation and laws.

6.1.7 Coverage of Evolution Impact

This criterion examines the level of success each approach brings to the organization in terms of handling the changes and highlighting the complete number of changes and gauging their overall impact.

6.2. Effort to Model

6.2.1 Document-based Approach

Manual Document-based Compliance

The manual document-based approach uses textual documents and therefore there is no modelling effort required. For instance, organizational policies, procedure documents and legislation documents are all in the textual format and they must be compared as such.

Tool Supported Document-based Compliance

With this approach, the actual text documents of the legislation and the organization are imported by DOORS. This step does not need any effort and therefore, no modelling effort is associated with this approach.

6.2.2 Model-based Approach

Manual Model-based Approach

In this approach, the organizational and legislative documents are modeled with URN in a tool like jUCMNav. This modeling task must be performed by a team of experts with the combined knowledge of the law and URN. Given this requirement, this task requires much effort, but the legislative model needs to be created only once.

Tool Supported Model-based Approach

This approach models the source documents with URN and then exports these models from jUCMNav to DOORS. This approach extends the manual method described above by requiring the models be exported to DOORS. Since the effort associated with exporting the models is negligible, the effort to model with tool support is comparable to modeling without it.

6.2.3 Full Compliance Framework

The complete compliance framework is a combination of the document-based approach and the model-based approach. The source documents are modeled with URN and are imported into DOORS. The amount of effort to produce the full compliance framework model is same as the model-based approach,

6.2.4 Summary

Comparing these 5 approaches with each other provides the following results. The document-based compliance approaches (manual and tool supported) require no effort since there is no model involved while model-based approaches need a considerable amount of effort to model the legislation and organization documents with URN. The amount of effort needed to export the models or documents to DOORS is negligible. Therefore the

full compliance framework takes the same amount of effort as the model-based approaches. Table 2 summarizes the analysis for this criterion:

Table 2 Effort to Model

	Manual Document-based	Tool Supported Document-based	Manual Model-based	Tool Supported Model-based	Full Compliance Framework
Definition	No Model	No Model	Effort of Modeling	Effort of Modeling	Effort of Modeling
Effort	Zero	Almost Zero	High	High	High

6.3. Effort to Comprehend

6.3.1 Document-based Approach

The legislative documents are usually complex and hard to understand as they require a great deal of specialization to do so. Since they need to cover all possible cases, they also tend to be vague. The generality of these documents results in different interpretations by different people. It is often up to a judge to determine the correct interpretation given the situation.

6.3.2 Model-based Approach

Modeling legislation helps to increase the level of comprehensibility since it makes the description of the legislation more compact and concise and benefits from having two dimensions over a linear representation. The true benefit of a model is that it makes an organization's interpretation of the law clear to third parties. Therefore with this approach, the level of comprehensibility is higher than with the document-based approaches.

6.3.3 Full Compliance Framework

This approach, since it incorporates both models and documents, helps to better understand the law and documents that apply to an organization. The GRL model provides an index to the details of the legislation. As a result, it draws from the benefit of a visual

model while still including the source documents. The level of comprehensibility is therefore higher.

6.3.4 Summary

The level of comprehensibility for methods that incorporate the model-based approach is higher than the ones that just rely on the document-based approach. Legal documents are especially hard to understand for a non-specialist. When they are modeled however, the relationships that exist between the different parts of the law become more obvious.

6.4. Effort to Document Compliance

6.4.1 Document-based Approach

Manual Document-based Compliance

To perform document-based compliance verification, it is necessary to go through the entire text of the applicable legal documents and examine whether the policies and business process documents are aligned with them. To do this, it is necessary to have a complete and precise knowledge of the law, policies and business processes to be able to match elements of the organizational documents to the law. In addition due to the lack of links between the organizational and legislative documents, each time that procedures are checked against the law, the entire legal document must be read to find any corresponding rules. Therefore, tracking instances of non-compliances in legal text is usually hard and requires much effort and time.

Tool Supported Document-based Compliance

Establishing links between the legal documents and the organization's process documents in DOORS needs considerable effort. This effort can be broken down in terms of the need to read the law, compare each part with the organization's documentation and set up links between corresponding clauses. After establishing links, tracking compliance is simplified. Now whenever the organization wants to verify that a process adheres to the law, it does not need to consult the entire legal document to find the related clauses.

6.4.2 Model-based Approach

Manual Model-based Compliance

In this approach, a URN model is used for each of the legal, policies, and procedures documentation for the organization. These URN models are defined separately without any links between them. Since the legal and business process documentation both have a GRL model defined at the same level of abstraction, documenting and tracking compliance can be easier than the cases where there are only textual documents available. However, since there are no links between the two models, it is still necessary to examine each element of the model when verifying that the model complies with the law.

Tool Supported Model-based Compliance

In this approach, the URN models are defined in DOORS. In order to document the compliance, the links between two elements have to be established. This task needs a considerable amount of effort but once the links are built, verifying the compliance can be done by following the links between the models. As a result, documenting compliance requires less effort than the situation where no links exists. However, since there are no links between the source documents and the URN models, the source documents must still be consulted making the task of documenting compliance more difficult.

6.4.3 Full Compliance Framework

In this approach, the URN models (legislation and organization) and their source documents are imported into DOORS. In order to document compliance, it is necessary to establish links between URN models and also between URN models and documents. This task needs a large amount of effort. Fortunately, the only link types that need to be established manually are traceability and source links. The other link types can be created by transitivity with the auto-completion mechanism defined in DOORS. Therefore, the amount of effort to document the compliance is not much higher than the tool supported model-based approach.

6.4.4 Summary

Comparing the 5 approaches in terms of effort to document compliance leads to the following observations. The manual document-based approach requires the highest amount of effort since the complex source documents are used directly without any links between them. The tool supported document-based approach needs less effort in comparison to the first approach in long term since once the links have been established, documenting compliance will be handled by traversing the links. The manual model-based approach requires less effort than the manual document-based approach since models are used instead of documents. However, comparing this approach with the tool supported document-based approach, one cannot conclude which has more benefit and needs less effort. The tool supported document-based approach only to have links established once but in the manual model-based approach, effort has to be spent every time compliance is verified. The tool-supported model-based approach is better when it comes to documenting compliance than the tool-supported document-based approach because it offers the advantage of dealing with models rather than dealing with documents. It is also better than the manual model-based approach because it has links for traceability. There is, however, still some need to refer to the source documents which results in a higher amount of effort over the full compliance framework. In the full framework, links are provided to the source documents which results in lower overall effort. Also this approach benefits from the auto-completion mechanism. Table 3 summarizes our analysis of this criterion:

Table 3 Effort to Document Compliance

	Manual Document-based	Tool Supported Document-based	Manual Model-based	Tool Supported Model-based	Full Compliance Framework
Definition	No Model and No Link	No Model but Links	Models but No Link	Models and Links between Models	Models and Links between Models and Documents
Effort	Highest	High	High	Medium	Low

6.5. Effort to Manage Evolution

6.5.1 Document-based Approaches

Manual Document-based Compliance

Whenever a legal document is amended, it is necessary to check whether any part of the organization's process is affected. However, since both documents are in paper format, it is hard to track the effect and ultimately the amended law must be verified against the whole process documentation. In fact, when procedures evolve, the complete legislation document must also be verified to ensure business process compliance. Each verification step takes a lot of time and effort since it involves relying on paper documents.

Tool Supported Document-based Compliance

With tool-supported document-based compliance, the documents and their links are set up in DOORS. Since there are links between the sections of the two documents, managing evolution will be more efficient. When a legal document is amended, the effects on the policies and procedures document can be tracked through these links. In addition, if part of business processes change, it is easier to manage compliance with this approach than it is with the manual document-based.

6.5.2 Model-based Approaches

Manual Model-based Compliance

With this approach, there are no links between the two URN models and therefore, tracking compliance is difficult. For example, if the legal document is amended, its effect on the URN model cannot be tracked right away. Similarly, if the business processes change, there would not be a mechanism to identify the areas of the law that are affected and whether the new business process violates the law. It becomes more difficult and time consuming than with other approaches that includes links. In fact, the manual model-based approach is quite poor in handling change to either of the legal documents or the business processes.

Tool Supported Model-based Compliance

As with other tool-supported methods, the URN models and the links between them reside in DOORS. The deficiency of this approach in managing changing requirements is that it lacks the links necessary to identify the dependencies between models and source documents. For example, if a legislative document is amended, the URN model must be checked completely to find whether there is any need to update it as well. As a result, although this approach is easier to follow than the manual model-based approach, it still requires a considerable amount of effort to manage change.

6.5.3 Full Compliance Framework

Managing evolution for the full compliance framework takes the least amount effort among all of the approaches due to the existence of links between source documents and URN models. In fact, when business processes or policies evolve or some part of the legislation document is amended, the impact (the dependent elements) is immediately visualized in DOORS via the links and default analysis mechanisms. The only exception is when new legal clauses or new business processes are added. In this case, the URN models and the link sets need to be updated manually.

6.5.4 Summary

Comparing the five approaches in terms of effort to manage evolution gives us the following results. Manual document-based approach takes the most amount of effort due to the lack of links between the two documents. The tool supported document-based approach is a better way to track the impact of change since it at least has some links. The only issue with this approach is that it still requires dealing directly with the source documents which can be costly. On the other hand, the manual model-based approach requires more effort to manage change in comparison to the other tool supported document-based approach. The tool supported model-based approach needs less effort than the manual approach because with the latter lengthy documents need to be consulted, hence slowing the management process. The full compliance framework requires the least effort in managing the impact of change since it covers both documents and models. It essentially has the benefits of all previous approaches together. The availability of links

allows the affected elements to be identified automatically and without much effort. An overall comparison of this criterion for each of the approaches is given in Table 4.

Table 4 Effort to Manage Evolution

	Cases	Manual Document-based	Tool Supported Document-based	Manual Model-based	Tool Supported Model-based	Full Compliance Framework
Definition		Documents	Documents and Links	Models but No Link	Models and Links	Documents, Models and Links
Manage Amendments	**Add a New Clause**	Examine Organization Document	Examine Organization Document	Examine and Update Both Models	Update Legal Model/ Follow links	Update Law Model/ Follow other links
	Modify a Clause with Links	Examine Organization Document	Follow Links	Examine Legal Model/ Update Models	Update Legal Model/ Follow links	Follow Links
	Delete a Clause	Examine Organization Document	Follow Links	Examine Legal Model/ Update Models	Update Legal Model/ Follow links	Follow Links
	Modify a Clause without Links	Examine Organization Document	Examine Organization Document	Examine and Update Both Models	Update Legal Model/ Follow links	Update Law Model/ Follow other links
Manage Business Process Evolution	**Modify Existing Process**	Examine Legal Document	Follow Links	Examine Legal Models/Update Model	Follow Links	Follow Links
	Add New Process	Examine Legal Document	Examine Legal Document	Examine Legal Models/ Update Models	Update the Model and Links	Update Model and Links
	Remove a Process	Examine Legal Document	Follow Links	Examine Legal Model/ Update Models	Follow Links	Follow Links
Effort		Highest	High	Very High	Medium	Low

6.6. Coverage of Model

6.6.1 Document-based Approach

Manual Document-based Compliance

This approach includes the organizational and legal documents in text format. As a result, the coverage offered by this document-based approach is complete.

Tool Supported Document-based Compliance

The inclusion of tool support to a document-based compliance approach has no impact on coverage. Since the source documents are used, the coverage is defined as complete.

6.6.2 Model-based Approach

Manual Model-based Compliance

Most parts of the law can be modeled with URN, but there are also items, i.e. definitions, exceptions and additional explanations, that do not lend themselves well to being modeled. These items need to be connected to the model for clarity, but in this approach, since there are no links, they are left out and coverage is not completely achieved.

Tool Supported Model-based Compliance

The only difference between this and the manual model-based approach is that in this case, links are included. Therefore, both approaches provide the same level of modeling coverage.

6.6.3 Full Compliance Framework

With the full compliance framework, the URN models are connected to each other, but also to their source documents. Therefore, links do exist to the definitions, exceptions and additional explanations contained in the legal documents which cannot be modeled in URN. Since the coverage of the items not in the model is addressed, full model coverage for this approach can be achieved.

6.6.4 Summary

The document-based approaches (both manual and tool supported) rely on the complete document text and therefore achieve full coverage of the source legal document. Model-based approaches (both manual and tool supported) cover most aspects of the legal documents but not all. There are some definitions and exceptions that cannot be modeled in URN. Therefore, the coverage is labelled as mostly achieved rather than complete. The full framework approach also achieves full coverage of the legal documents since its

models can be linked to the source documents if necessary. A comparison of the different approaches based on this criterion is given in Table 5.

Table 5 Coverage of Model

	Manual Document-based	Tool Supported Document-based	Manual Model-based	Tool Supported Model-based	Full Compliance Framework
Definition	Documents	Documents and Links	Models but No Link	Models and Links	Documents, Models and Links
Coverage	Complete	Complete	Almost Complete	Almost Complete	Complete

6.7. Coverage of Documentation of Compliance

6.7.1 Document-based Approach

Manual Document-based Compliance

With the manual document-based approach, there are no links and therefore it is not possible to document compliance. As a result, whenever a process needs to be checked against legal documents, the entire documents must be reviewed by a competent person.

Tool Supported Document-based Compliance

Since this approach implements links between the process document and the legal document, compliance itself can be documented. Using these links, the parts of the law that are not addressed by the process can be identified. However, the documentation produced is not complete and is often disorganized since the task is complicated by virtue of the language and terminology being different in the two documents. The coverage of the compliance documentation is very unlikely to be complete.

6.7.2 Model-based Approach

Manual Model-based Compliance

This approach has both models defined in jUCMNav in separate files without any links between them. It is therefore not possible to track compliance between the two models. In addition, since there are no links between the source documents and the models, the parts

of the legislation documents that cannot be modeled with URN will be missing. Thus, documentation of compliance cannot be fully achieved.

Tool Supported Model-based Compliance

With the inclusion of tool support, links between the models can be defined in DOORS. Using these links, the task of documenting compliance can be largely achieved. In using models for the legal component and for the business process description, the linking is performed in a more formal manner where the interpretation of each is clearer in comparison with the tool supported document-based approach. However, with this approach the parts of the legislation that are not modeled in URN are not represented in the documentation and thus it is not fully complete.

6.7.3 Full Compliance Framework

With the full compliance framework, the source documents, URN models and their links are all defined in DOORS. Since the source documents, their URN models and the links between them exist, the documentation of compliance could be complete.

6.7.4 Summary

From our analysis, we can see that links between the legislation and business process descriptions are essential for documenting compliance. Without links, it is very time consuming to verify that a business process adheres to the law. Hence, with the manual document-based approach or the manual model-based approach documenting compliance cannot be achieved. On the other hand, with the tool support this is possible, although this is not very accurate on account of the subjectivity involved. If models are used, source documents must also be included so that the parts of the law that are difficult to model can be considered. The full framework offers the best option for documenting compliance because it defines processes and legislation by URN models, it provides links between them and includes links from these models to the source documents. Table 6 provides a summary of the coverage of documenting compliance criterion:

Table 6 Coverage of Documenting Compliance

	Manual Document-based	Tool Supported Document-based	Manual Model-based	Tool Supported Model-based	Full Compliance Framework
Definition	Documents	Documents and Links	Models but No Link	Models and Links	Documents, Models and Links
Coverage	Almost Zero	Low	Incomplete	Almost Complete	Complete

6.8. Coverage of Evolution Impact

6.8.1 Document-based Approach

Manual Document-based Compliance

When a document is amended or the business process evolved, the documents themselves must be reviewed completely and new versions built step by step. Given that these documents are usually long and complicated, this procedure is tedious. It is more likely with this approach that mistakes or assumptions are made when performing the update. As a result, this approach is not a good at handling evolution.

Tool Supported Document-based Compliance

With this approach, since there are links between the two documents defined in DOORS, changes can be tracked. DOORS will highlight the impact of the changes in other dependent documents. Dealing with change, however, still remains a difficult task since the links between documents are difficult to make precise. This difficulty results in an incomplete process for dealing with evolving business and legal components.

6.8.2 Model-Based Approaches

Manual Model-based Compliance

Without the presence of links between the legal document and its URN model, the impact of any amendment cannot be tracked directly. Therefore, the coverage of this approach in managing evolving legislation is not complete. In addition, the fact that there are no links between the two URN models makes tracking changes to the business processes more

difficult since some parts of the law may be left out. Thus the management of evolution cannot be performed well with this approach.

Tool Supported Model-based Compliance

If the model-based approach is supported by a tool such as DOORS, links can be established between the URN models. Unfortunately, since only the models themselves are used and the source documents left out, the effect of change cannot be highlighted immediately. Therefore, this approach cannot cover the impact of evolution completely.

6.8.3 Full Compliance Framework

The full compliance framework establishes some links between the legal document and its URN model. Therefore, the impact of any change to the legal document can be immediately reflected in the model. Additionally, through links that exist between the two URN models, the impact can also be highlighted in the organization's URN model. Conversely, using the links between the URN models, any change in the organization's business process or policies can be tracked directly and its compliance confirmed in the related law. Full coverage for compliance tracking in the face of evolution can be achieved with this approach.

6.8.4 Summary

Tracking change is made easier with the presence of links. It is made complete with the inclusion of source legal documentation and links from it to the legislation URN model. The manual documents-based and model-based approaches suffer from the lack of links. Tracking change is made difficult and the impact of change cannot be immediately identified. With tool support, these approaches can be adapted to track and identify change. However, since the links defined for the tool supported document-based approach are not precise, the level of coverage is not complete and imprecise. Lack of links to the source document in the tool supported model-based approach results in coverage that is incomplete. The full compliance framework approach which offers these links has the most complete coverage. Table 7 provides a summary of the coverage of evolution impact criterion:

Table 7 Coverage of Evolution Impact

	Manual Document-based	Tool Supported Document-based	Manual Model-based	Tool Supported Model-based	Full Compliance Framework
Definition	Documents	Documents and Links	Models but No Link	Models and Links	Documents, Models and Links
Coverage	Almost Zero	Low	Low	Medium	Almost Complete

6.9. Summary of Analysis

In order to verify the compliance of business processes and policies to the law, organizations can apply two different approaches: a document-based approach or a model-based approach. Document-based compliance comes in two flavours: manual or tool-supported. The model-based approaches are similarly divided into manual and tool-supported compliance. Our proposed framework is also available, which offers the combination of the document-based approach and the model-based approach with tool support.

The manual document-based approach is currently the most common way of handling compliance. Based on our analysis, however, this approach requires the largest effort among the five approaches presented to document compliance and manage evolution. These textual documents are usually more complex and harder to understand than model-based representations. Moreover, the coverage of the compliance documentation and of the evolution impact with this approach is lower than with all other approaches. This poor coverage can be attributed to the absence of links between the legislation and business process documentation. By not having links, some necessary aspects of compliance may not be correctly documented and the impact of change may not be easy to track.

Tool-supported document-based compliance introduces the concept of permanent links between legislative and organizational documents. These links provide the mechanism with the ability to track compliance and manage interdependencies between the two types of documents. In terms of effort, this approach has no modeling requirement but it does require that links be set up between the two documents. However, with the investment in time to set up these links comes the benefit of reduced effort for documenting the compliance and managing process and legislation evolution. The tool-supported document-based approach also benefits over the plain version by increased coverage of docu-

menting compliance and evolution impact. Although the coverage is better, it is still unsatisfactorily low since many of the links are poorly defined due to the difficulty in relating text documents with each other. Furthermore, when dealing with text documents, the level of comprehensibility is generally lower than for a model-based approach, hence making the document-based approaches less desirable.

The only benefit manual model-based compliance has over tool-supported document-based compliance is its greater level of comprehensibility. It does, however require a significant amount of effort to develop the model. Documenting compliance is easier with this approach than it is with text documents since the two models are defined at the same level of abstraction. The lack of links, however, does not allow for a high degree of coverage and makes the process of documenting compliance a lengthy one. It also makes the management of evolution difficult to achieve and results in incomplete coverage of impact.

As for tool-supported model-based compliance, it is the best solution compared to the other approaches discussed thus far in that it deals with models instead of documents and it also includes some level of linkage between two models. However, this approach lacks links between the models and the source documents and results in increased difficulty in managing evolution and an imperfect documentation of compliance.

The best of all the approaches presented in this thesis, when considering all the criteria presented, is our full compliance framework. Although the approach requires the most effort up front, it is the easiest to use for documenting compliance and managing evolution. In addition, since this approach includes both source documents and graphical models, the level of comprehensibility will be higher than all others. Other benefits include complete coverage for the model, compliance documentation and evolution impact. Table 8 provides a summary for all the criteria:

Table 8 Summary of Criteria

		Manual Document-based	Tool Supported Document-based	Manual Model-based	Tool Supported Model-based	Full Compliance Framework
Definition		No Model and No Link	No Model but Links	Models but No Link	Models and Links	Models, Documents and Links
Effort	**Modeling**	Zero	Almost zero	High	High	High
	Documenting Compliance	Highest	High	High	Medium	Low
	Managing Evolution	Highest	High	Very High	Medium	Low
Covrage	**Modeling**	Complete	Complete	Almost Complete	Almost Complete	Complete
	Documenting Compliance	Almost Zero	Low	Incomplete	Almost Complete	Complete
	Managing Evolution	Almost Zero	Low	Low	Medium	Almost Complete
Comprehensibility		Low	Low	High	High	High

6.10. Comparison with Other Related Methods

In this section, we compare our compliance framework with some of the previous work mentioned in Chapter 2. As discussed in Section 2.5, none of the previous methods has an integrated compliance framework and they either focus on business processes or on policies. Table 9 categorizes related methods based on the 5 categories of approaches discussed above.

Table 9 Summary of Related Methods

	Document-based	Tool Supported Document-based	Model-based	Tool Supported Model-based	Integrated Model and Document
Breaux *et al.*			✓		
Darimont *et al.*				✓	
He *et al.*				✓	
Rifaut *et al.*			✓		
ORCA				✓	
Compliance Framework					✓

Breaux *et al.*[4] provide a methodology to extract rules and obligations from regulations but their work does not provide any link to the organization's policies and procedures documents. Darimont *et al.* [6] apply the KAOS methodology to model regulations and they explain how to transform regulation documents to goals, objects and threats models. They provide a level of traceability between the source documents and these three models but this traceability is not expanded to the organization's document. He *et al.* [15] apply ReCAPS to integrate the components of access control analysis, improve software quality and ensure policy- and requirements-compliant systems. This method provides traceability from source documents to the access control policies but it does not include business processes. The scope of this method is narrow and only focuses on the software development process. Rifaut *et al.* [24] apply goal-based models on the implementation of a financial system to ensure it is compliant with Basel II regulations. In their method, they divide organization and their business processes based on the organizational layers and assign the elements of the related goal model to those layers. However, their method does not provide any kind of traceability. The ORCA group [3] develops a system to help standardize the representation of compliance documents and they are providing a dynamic mapping between regulations and the internal policies of the organization. However, they still do not provide an integrated framework that includes both business processes and policies in a model at the same time. Note however that the ORCA project is still ongoing.

Chapter 7. Conclusions

7.1. Summary of Contributions

In this thesis, we introduced a requirements- and model-based framework to help with the understanding and verification of legislative compliance for business processes. The framework is especially important since legal documents are usually difficult to understand and any violation of the law is accompanied by financial penalty and loss of public trust. Furthermore, the auditing and verification of compliance is a very expensive exercise, especially in a context of constant changes. In applying URN to model legislative documents, we provided a methodology to better understand them. We used a portion of PHIPA (related to the disclosure of personal information to researchers) and modeled it with URN in order to validate our work.

We also defined a new set of compliance links as an extension to previous work on URN-oriented requirements management to help with documenting and tracking compliance. These links provide traceability between legal documents and business processes and they also serve to facilitate the task of maintaining privacy compliance for the entire model. This compliance can be verified at any time by following the links and identifying those which cause potential violations. In our case study, we established links between hospital models of policies and business processes (on information access) and legal privacy documents and models in order to find instances of potential non-compliance.

Moreover, with the help of these links, we provided an approach to manage compliance as legislation or business processes evolve. This approach becomes very useful over time since, through the links, we can track changes as they happen and prevent violations to the law. The utility of this component is shown in our case study by considering legislative amendments and also by addressing some business process modifications. We evaluated our framework according to how well it was able to manage the changes.

Finally we implemented our framework using jUCMNav to create and maintain our models and Telelogic DOORS to link them to each other and to original documents.

We also determined that in order to reduce the complexity of the management task for our framework, it was necessary to update the DXL import and analysis library to enable many links to be added automatically. This transitive auto-linking mechanism enables users to exploit DOORS management and analysis capabilities (suspect links, impact analysis, filtering and others) to their fullest extent.

7.2. Conclusion

This thesis validated various aspects of the proposed compliance framework in the context of a limited case study at a major hospital. This work illustrated that requirement engineering models represent a viable approach to track compliance. This improvement can be attributed to the increased ability for people to understand the processes and provide input. This advantage of models over verbose text is generally accepted to be true, especially for complex texts. By modeling the legal component with URN, these benefits are also offered. Although refinement is not an issue with the law (it is controlled by lawmakers), its comprehension by non-legal individuals is critical to the development of a business process that respects the law. The greatest benefit comes with having both the applicable portions of the law and business process modeled in a common language.

Second, the effort required to setup and maintain the framework is reasonable given the potential benefits .Modeling the compliance is mainly dependent on adequate tools support as well as up front investment by an organization. Since the cost of non-compliance is high and any non-compliance can lead to a high amount of penalty from the government, legal actions from customers or damage to their reputation. Therefore, although establishing the framework needs some amount of investment, this investment probably happens only once and organization can reuse this framework forever. As well, this framework ensures that organizations can more easily maintain compliance of business processes with legal documents even if they evolve. Therefore, when a change happens, with a small amount of investment, this framework helps the legal model complies with its source document again. This is also very important, since the cost of non-compliance is usually high.

Third, this thesis showed that in introducing a finite set of links, we are able to connect the URN models of the law and of business processes and build a framework to

successfully model privacy compliance. The resulting framework makes it possible to tie each step in the business process to its legal requirements thereby ensuring that the process as a whole complies with the law. Using this framework for privacy compliance has the benefit of providing managers and privacy officers the ability to track and maintain compliance if either the business processes change or the legislations change. This conclusion is supported by our real-life case study that describes the gains provided by this framework, especially in comparison with related methods.

7.3. Future Work

The development of the framework presented in this thesis is an initial step in a new direction for managing compliance with legislation, regulation and organizational guidelines. Like any initial work, we made some simplifying assumptions and solely focused on validating its effectiveness for one process and one law in a given healthcare organization. However, other domains need to be researched and validated as well. There may also be current approach limitations that can be improved. Removing these assumptions and making the framework more generally applicable is the direction we will take in our future work.

The first opportunity is to address the issues related to how the framework treats legislation documents. In our current framework, we assume the existence of only one legal document and one policy document. In practice, we need to determine how best to support a variable number of source documents. In addition, it is possible that policies and regulations are contradictory, and we would have to determine how the framework can support clauses that conflict.

The second area of future work is to study how we can reuse modeled components of legislation in other contexts. We have shown that it is possible, given some effort, to create URN models of legislative source documents for the clauses that applied to our case study. We could study a similar situation and try to maximize the amount of reuse in our legislation URN model. If we can successfully demonstrate legislation model reuse, then we will have a stronger argument for why the effort needed to develop them is well spent. Also, the more models are built, the more understandable the law becomes and eventually the models would just need to be confirmed by lawyers, and they would

not have to lead the modeling process. Some automatic extraction might even be possible, especially as ORCA-based representations of laws become available.

With more case studies as well, we acquire more evidence about how much effort is required to implement a compliance management system using this framework. Our third element of future work is to present a more quantitative assessment of our framework with the hope of arriving at a tool-supported method capable of more easily ensuring policy legality and procedural compliance to these policies.

The forth step in our future work is to have some survey in the areas of deontic logic and artificial intelligence, more particularly on legal reasoning.

Finally, we will try to encourage hospitals to adopt our framework especially when they are defining new business processes such as online processes or for some of their critical processes such as accessing to the hospital's data warehouse.

References

[1] AMR Research Inc.: *AMR Research Finds Spending on Sarbanes-Oxley Compliance Will Remain Steady at $6.0B in 2007.* February 22, 2007. Accessed May 2007. http://www.amrresearch.com/Content/View.asp?pmillid=20232.

[2] Amyot, D.: Introduction to the User Requirements Notation: Learning by Example. *Computer Networks*, 42(3), 285-301, 21 June 2003.

[3] Bowles, A.: The Global Regulatory Information Database: An Open IP Project, *OMG Regulatory Compliance Alliance (ORCA),* February 2007.

[4] Breaux, T., D., Vail, M., V., and Antón, A., I.: Towards Regulatory Compliance: Extracting Rights and Obligations to Align Requirements with Regulations. *14th IEEE Requirements Engineering Conference*, Minneapolis, USA, 2006, 49–58.

[5] Caetano, A., Silva, A. R., Tribolet, J.: Using Roles and Business Objects to Model and Understand Business Processes, *2005 ACM Symposium on Applied Computing,* Santa Fe, USA, March 2005, 1308–1313.

[6] Darimont, R., Lemoine, M.: Goal-oriented analysis of regulations. *REMO 2V06: Int. Workshop on Regulations Modelling and their Verification & Validation,* Luxemburg, June 2006.

[7] European Union: *Directive on Privacy and Electronic Communication*, 2002. http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf, Accessed: May 2007.

[8] European Union: *Final EU Data Protection Directive*, http://aspe.hhs.gov/datacncl/eudirect.htm, Accessed May 2007

[9] Fairfield, D.: The Ottawa Hospital Data Warehouse - Governance and Operation Procedures - Phase 1 Research, December 17, 2004.

[10] Gingerich, B.: Evaluating Your Compliance Plan: A Corporate Compliance Program Evaluation Model, *Home Health Care Management Practice*, Vol. 14, No. 2, 2002, 153–154.

[11] Government of Canada, *Health Information Custodians in the Province of Ontario Exemption Order*, http://canadagazette.gc.ca/partII/2005/20051214/html/sor399-e.html, Accessed May 2007.

[12] Government of Ontario: *Personal Health Information Protection Act, 2004, ONTARIO REGULATION 329/04, Amended to O. Reg. 537/06*, http://www.e-laws.gov.on.ca/DBLaws/Regs/English/040329_e.htm, Accessed May 2007

[13] Government of Ontario: *Personal Health Information Protection Act, 2004*, http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/04p03_e.htm, accessed May 2007.

[14] GRL: *Goal-oriented Requirement Language*, http://www.cs.toronto.edu/km/GRL/, Accessed May 2007.

[15] He, Q., Otto, P., Antón, A.I., Jones, L.: Ensuring compliance between policies, requirements and software design: A case study. *In: IWIA 2006: Proc. Fourth IEEE Int. Workshop on Information Assurance,* Washington, USA, IEEE Computer Society (2006) 79–92.

[16] Industry Canada: *Electronic Commerce in Canada- PIPEDA awareness raising tool*. January 2004, http://strategis. ic.gc.ca/epic/site/ecic-ceac.nsf/en/gv00211e.html, Accessed May 2007.

[17] International Data Protection Legislation and Initiatives: *Ensuring Trans-Border Compliance*, http://www.mccarthy.ca/pubs/publication.asp?pub_code=1110#_Toc499112768, Accessed May 2007

[18] ITU-T: User Requirements Notation (URN) – *Language Requirements and Framework. ITU-T Recommendation Z.150*. Geneva, Switzerland, February 2003.

[19] Jiang, B.: *Combining Graphical Scenarios with a Requirements Management System*. M.C.S. thesis, SITE, University of Ottawa, June 2005.

[20] Kealey, J., Kim, Y., Amyot, D., and Mussbacher, G.: Integrating an Eclipse-Based Scenario Modeling Environment with a Requirements Management System, *2006 IEEE Canadian Conf. on Electrical and Computer Engineering (CCECE06),* Ottawa, Canada, May 2006, 2432–2435.

[21] London Health Science Centre: *Privacy Laws in Canada, Personal Health Information Protection Act*, 2004 (PHIPA), http://www.lhsc.on.ca/privacy/laws.htm, Accessed May 2007

[22] NYMITY: *Interview with Murry Long*, http://www.nymity.com/privaviews/2004/long.asp, Accessed May 2007.

[23] Peyton, L., Hu, J., Liu, H., Al-Saleh, M., El-Saddik, A.: A Collaborative Approval Process for Accessing Sensitive Data. *International Journal of Computer Applications in Technology,* Inder-science Publishers, Geneva, Switzerland. Accepted October 2005, to appear 2007

[24] Rifaut, A., Feltus, C.: Improving operational risk management systems by formalizing the Basel II regulation with goal models and the ISO/IEC 15504 approach. *REMO2V06: Int. Workshop on Regulations Modelling and their Verification & Validation,* Luxemburg (2006).

[25] Roy, J.-F.: *Requirement Engineering with URN: Integrating Goals and Scenarios,* M.C.S. thesis, SITE, University of Ottawa, January 2007.

[26] Roy, J.-F., Kealey, J., and Amyot, D.: Towards Integrated Tool Support for the User Requirements Notation, *SAM 2006: Fifth Workshop on System Analysis and Modelling*, LNCS 4320, Springer, 198–215, 2006.

[27] *Seven Guiding Principles of HIPAA Privacy Rules*, http://www.umsl.edu/~optrgarz/hipaa/sevenguidingprinciples.htm, Accessed May 2007

[28] Staccini, P., Joubert, M., Quaranta, J.F., Fieschi, D., and Fieschi, M.: Modelling healthcare processes for eliciting user requirements: a way to link a quality paradigm and clinical information system design. *International Journal of Medical Informatics*, 64:2-3, 129–142, Elsevier, 2001.

[29] Telelogic AB: *DOORS*. http://www.telelogic.com/products/doors/doors/. Accessed May 2007

[30] The Eclipse Foundation: *Eclipse - an open development platform.* http://www.eclipse.org/ Accessed May, 2007.

[31] Ting, T. C.: Privacy and Confidentiality in Healthcare Delivery Information System, *Proc. IEEE Symposium on Computer-Based Medical Systems*, 1999, 2–4.

[32] Tousaw, K.: Securing Compliance, Protecting Privacy, The PIPEDA Enforcement Evaluation Research Project, *B.C. Civil Liberties Association (bccla.org)*, March 2006.

[33] United States Department of Health and Human Services, Medical Privacy: *National Standards to Protect the Privacy of Personal Health Information*, http://www.hhs.gov/ocr/hipaa/, Accessed May 2007.

[34] US Department of Health and Human Services: *HIPAA General Information,* http://www.cms.hhs.gov/HIPAAGenInfo/, Accessed May 2007.

[35] Weiss, M. and Amyot, D.: Business Process Modeling with URN, *International Journal of E-Business Research*, Vol. 1, No. 3, 63–90, July-September 2005.

[36] Weiss, M., Amyot, D., Designing and Evolving Business Models with URN, *MCeTech Conference*, 2005, 149–162.

Appendix A: PHIPA- Disclosure for Research

PART IV- COLLECTION, USE AND DISCLOSURE OF PERSONAL HEALTH INFORMATION

44. (1) A health information custodian may disclose personal health information about an individual to a researcher if the researcher,

(a) submits to the custodian,

i. an application in writing,

ii. a research plan that meets the requirements of subsection (2), and

iii. a copy of the decision of a research ethics board that approves the research plan; and

(b) enters into the agreement required by subsection (5). 2004,c.3, Sched.A,s.44 (1).

Research plan

(2) A research plan must be in writing and must set out,

(a) the affiliation of each person involved in the research;

(b) the nature and objectives of the research and the public or scientific benefit of the research that the researcher anticipates; and

(c) all other prescribed matters related to the research. 2004, c.3, Sched. A, s. 44 (2).

Consideration by board

(3) When deciding whether to approve a research plan that a researcher submits to it, a research ethics board shall consider the matters that it considers relevant, including,

(a) whether the objectives of the research can reasonably be accomplished without using the personal health information that is to be disclosed;

(b) whether, at the time the research is conducted, adequate safeguards will be in place to protect the privacy of the individuals whose personal health information is being disclosed and to preserve the confidentiality of the information;

(c) the public interest in conducting the research and the public interest in protecting the privacy of the individuals whose personal health information is being disclosed; and

(d) whether obtaining the consent of the individuals whose personal health information is being disclosed would be impractical. 2004, c. 3, Sched. A, s. 44 (3).

Decision of board

(4) After reviewing a research plan that a researcher has submitted to it, the research ethics board shall provide to the researcher a decision in writing, with reasons, setting out whether the board approves the plan, and whether the approval is subject to any conditions, which must be specified in the decision. 2004, c. 3, Sched. A, s. 44 (4).

Agreement respecting disclosure

(5) Before a health information custodian discloses personal health information to a researcher under subsection (1), the researcher shall enter into an agreement with the custodian in which the researcher agrees to comply with the conditions and restrictions, if any, that the custodian imposes relating to the use, security, disclosure, return or disposal of the information. 2004, c. 3, Sched. A, s. 44 (5).

Compliance by researcher

(6) A researcher who receives personal health information about an individual from a health information custodian under subsection (1) shall,

(a) comply with the conditions, if any, specified by the research ethics board in respect of the research plan;

(b) use the information only for the purposes set out in the research plan as approved by the research ethics board;

(c) not publish the information in a form that could reasonably enable a person to ascertain the identity of the individual;

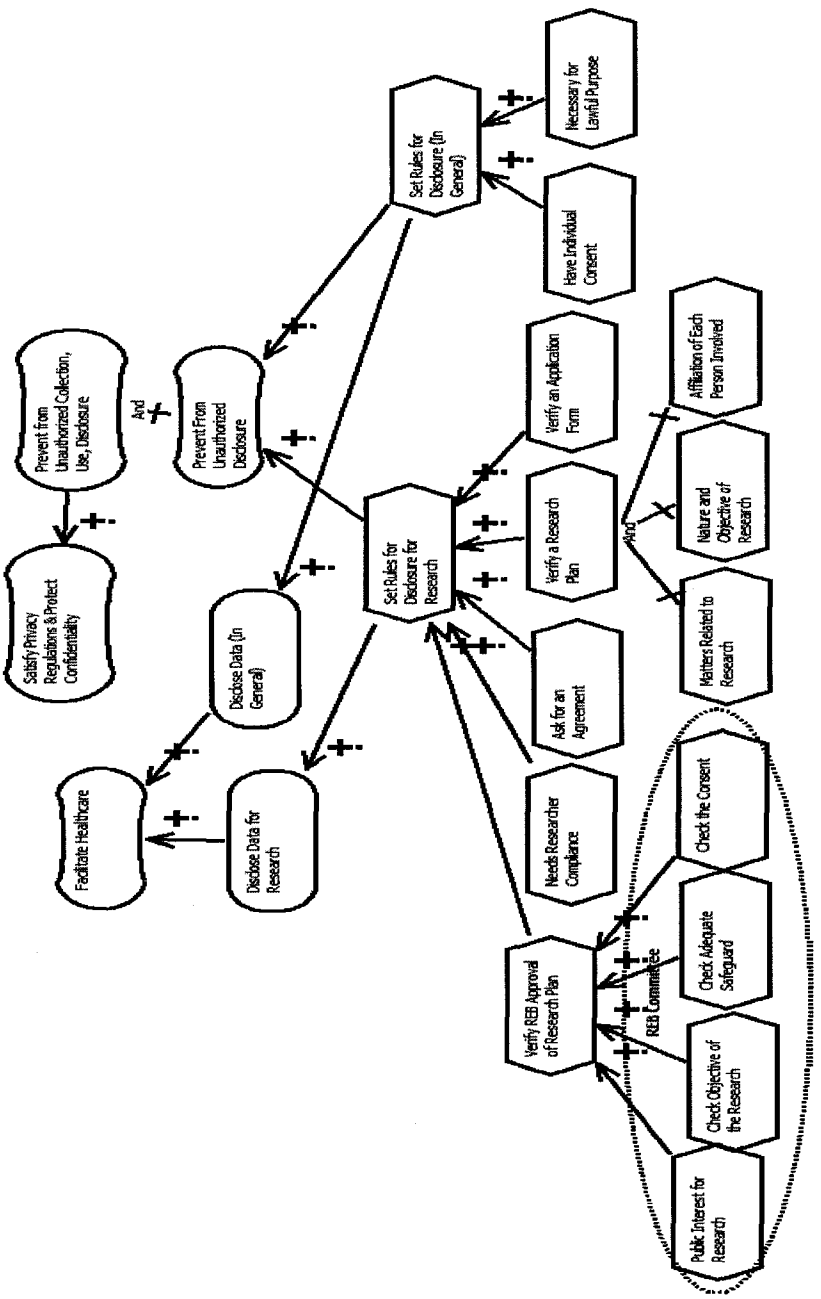
(d) despite subsection 49 (1), not disclose the information except as required by law and subject to the exceptions and additional requirements, if any, that are prescribed;

(e) not make contact or attempt to make contact with the individual, directly or indirectly, unless the custodian first obtains the individual's consent to being contacted;

(f) notify the custodian immediately in writing if the researcher becomes aware of any breach of this subsection or the agreement described in subsection (5); and

(g) comply with the agreement described in subsection (5). 2004, c.3, Sched. A, s.44 (6).

Appendix B: Simplified GRL Model of PHIPA



Appendix C: The Hospital Approval Process URN Model

The approval process of the hospital explained in Section 5.1.2 is modeled here with UCM. This model includes a root map, which is a high-level overview of the process, as well as six sub-maps.

The root map (Figure 45) shows the causal relationships necessary between the researcher and the hospital in order to get health information from the data warehouse. This map contains "Request for PHI" and "Review Request" stubs (shown as *diamonds)* which represent the "Submit a request form" process and "Review the Data Request Form" process.

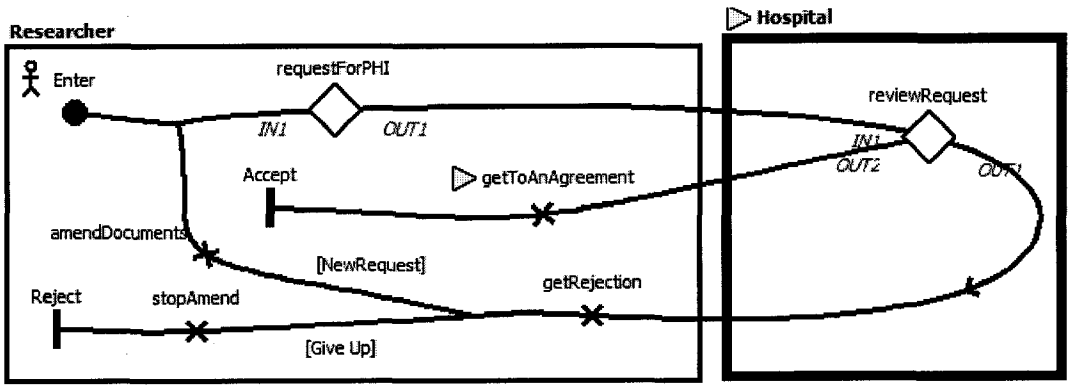


Figure 45 Top Level Map

The "Request for PHI" sub-map (Figure 46) provides the view of what the researcher needs to submit to the hospital. These are the request form and the documents required by the research ethics board (REB).

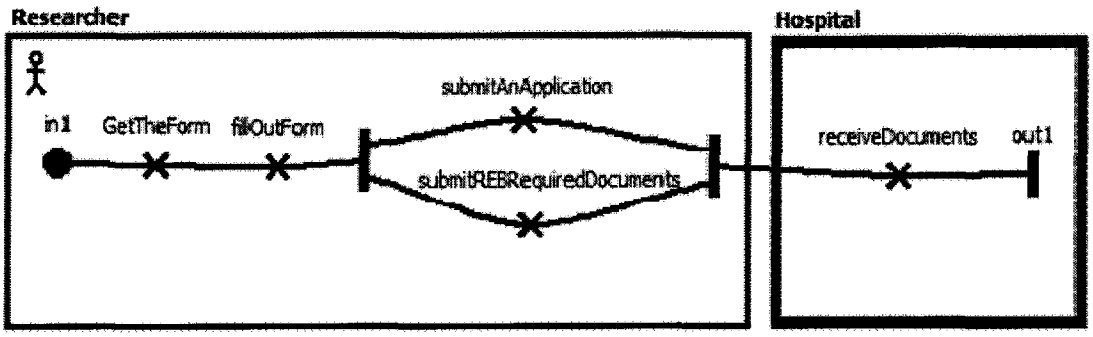


Figure 46 Request for PHI Map

The interaction between the individuals and the teams in charge of the approval process (privacy officer, data warehouse administrator, research ethics board, and data warehouse support teams) and the researcher is modeled in following maps. Figure 47 shows the "Review Request" sub-map. This sub-map includes a "Privacy Officer Review" sub-map (inside the "CPO Review" stub), a "Research Ethics Board Approval" sub-map (inside the "REBApproval" stub), and a "Review Request Technically" sub-map (inside the "technicalReview" stub), which collectively represent the processes that have to be taken to get approval. The detail of each of these processes is shown in separate maps.

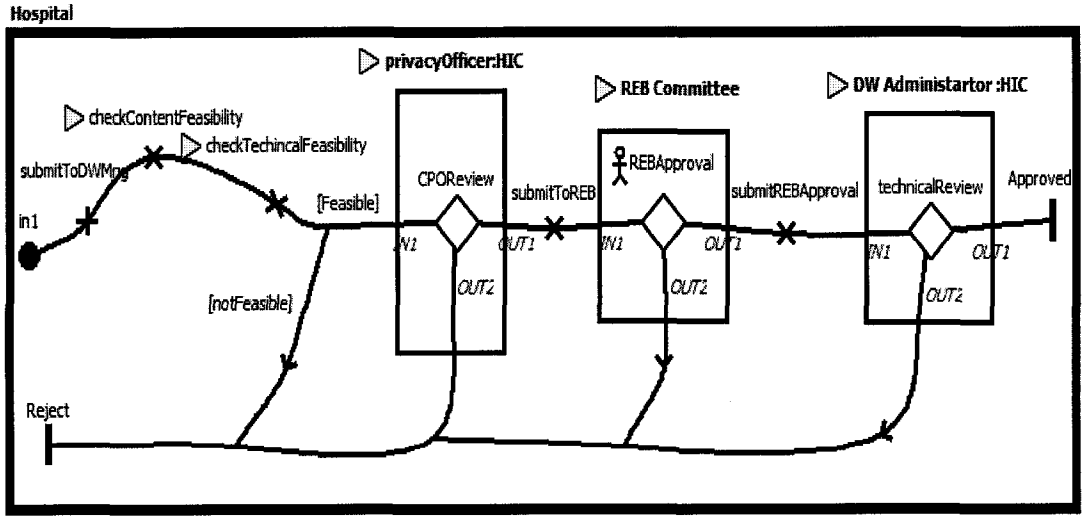


Figure 47 Review Request Map

As is shown in Figure 47, after the approval of the data warehouse manager, the privacy officer will check the request form with legislations and decide whether to reject or accept the request (See Figure 48).

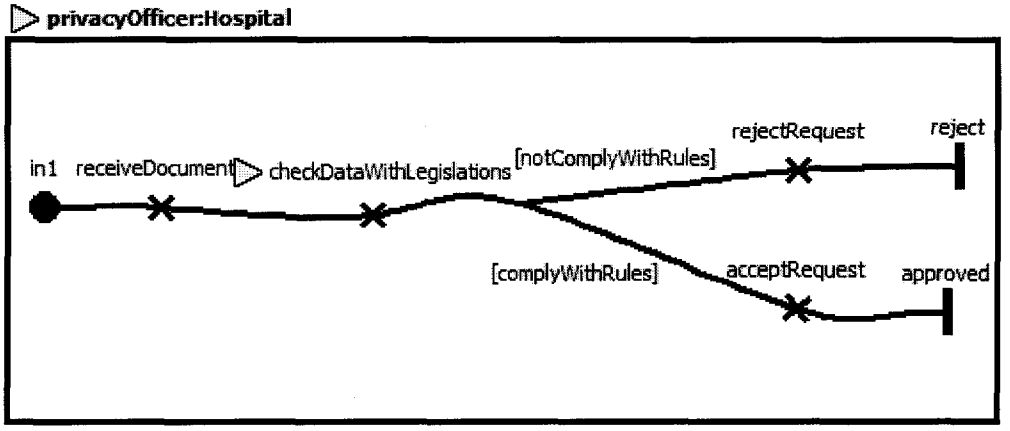


Figure 48 Privacy Officer Review

After getting approved by the privacy officer, the data request form is submitted to the research ethics board to review (submitToREB). Research ethics board reviews the request form based on ethical issues (checkEthicalIssues), disposal method (checkDisposalMethod) and use of identifiable or de-identifiable data (checkIdentifiableDataType) and decide to whether approve or reject the request. This process is presented in Figure 49.

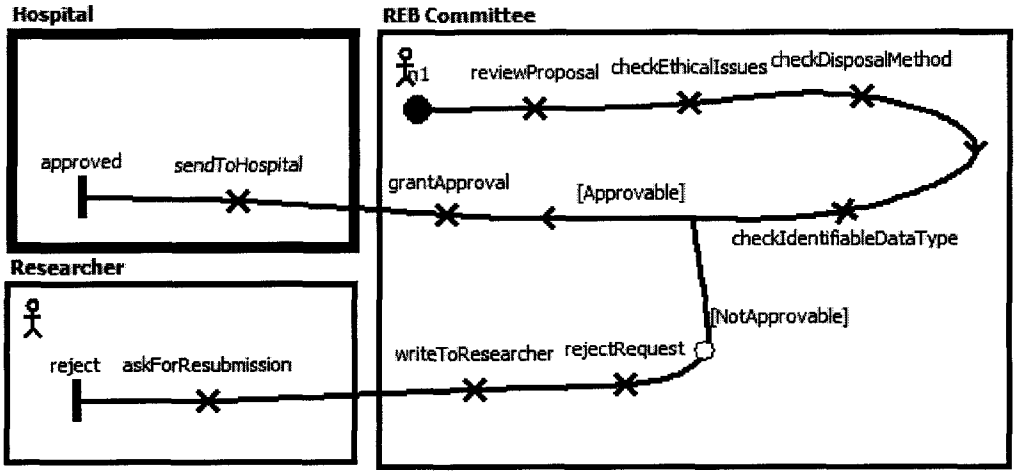


Figure 49 REB Review Sub-map

Finally, the data warehouse support team and administrator review technical issues related to the request. At first they check to see if data is available (verifyDataFeasibility), and they verify the technical competency of the researcher (checkTechnicalCompetency) and safeguards methods (checkSafeguards) he or she provides to protect the data. If the request is approved, the data warehouse administrator grants access to data by paper reports, files or through a username and a password (See Figure 50).

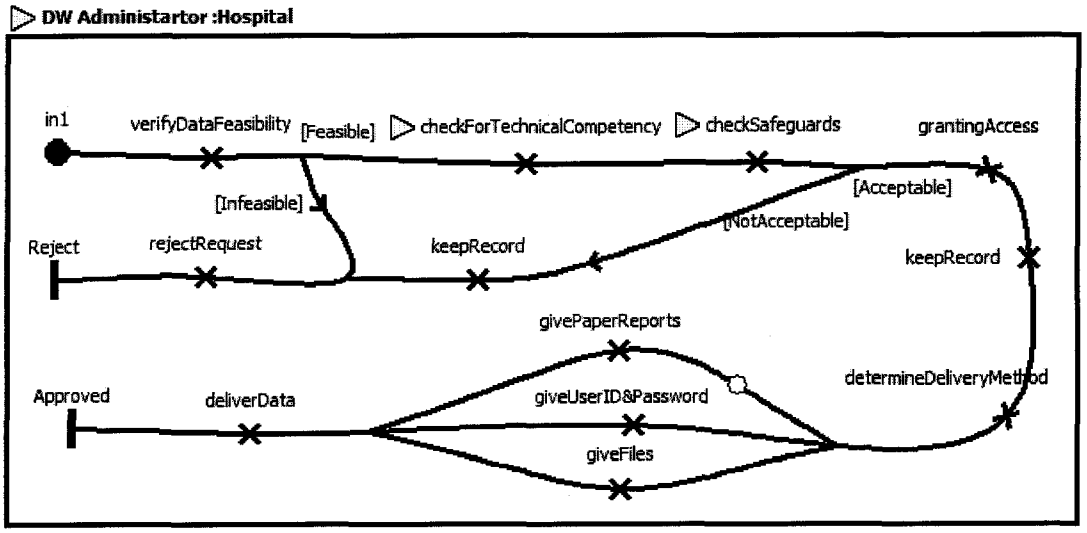


Figure 50 Review Request Technically

Appendix D: Amendments to PHIPA [12]

Requirements for research plans

16. The following are prescribed as additional requirements that must be set out in research plans for the purposes of clause 44 (2) (c) of the Act:

1. A description of the research proposed to be conducted and the duration of the research.
2. A description of the personal health information required and the potential sources.
3. A description of how the personal health information will be used in the research, and if it will be linked to other information, a description of the other information as well as how the linkage will be done.
4. An explanation as to why the research cannot reasonably be accomplished without the personal health information and, if it is to be linked to other information, an explanation as to why this linkage is required.
5. An explanation as to why consent to the disclosure of the personal health information is not being sought from the individuals to whom the information relates.
6. A description of the reasonably foreseeable harms and benefits that may arise from the use of the personal health information and how the researchers intend to address those harms.
7. A description of all persons who will have access to the information, why their access is necessary, their roles in relation to the research, and their related qualifications.
8. The safeguards that the researcher will impose to protect the confidentiality and security of the personal health information, including an estimate of how long information will be retained in an identifiable form and why.

9. Information as to how and when the personal health information will be disposed of or returned to the health information custodian.
10. The funding source of the research.
11. Whether the researcher has applied for the approval of another research ethics board and, if so the response to or status of the application.
12. Whether the researcher's interest in the disclosure of the personal health information or the performance of the research would likely result in an actual or perceived conflict of interest with other duties of the researcher. O. Reg. 329/04, s. 16.

Appendix E: DXL Script Source Code

Compliance.hlp

```
This DXL library supports the creation
of compliance between organization and
legislation URN models in DOORS.

DXL files can be exported bu UCMNav and
jUCMNav. Running them requires this
library to be installed in the
'Program Files\Telelogic\DOORS_8.0\lib\
dxl\addin' directory.

An additional features is provided
(accessible via the Compliance DOORS menu):

- Auto Complete Links
```

Compliance.idx

```
URNAutoCompleteLinks A   Auto Complete Links
```

URNAutoCompleteLinks.dxl

```
/*********************************************************************
// Author Sepideh Ghanavati, April2007
// -- Based on initial version by Gunter Mussbacher
*********************************************************************/
#include "addins/Compliance/lib/URNUtilities.dxl"
pragma runLim,0

completeLinks()
```

URNUtilities.dxl

```
/*********************************************************************
// Author Sepideh Ghanavati, April2007
// - Original version by Gunter Mussbacher, May-Jun2005
// - Based on initial version by Bo Jiang
*********************************************************************/
#include "addins/Compliance/lib/URNGlobal.dxl"
#include "addins/Compliance/lib/URNModuleUtilities.dxl"
#include "addins/Compliance/lib/URNInitExit.dxl"
#include "addins/Compliance/lib/URNLinks.dxl"
#include "addins/Compliance/lib/URNCompleteLinks.dxl"
```

URNGlobal.dxl

```
/*****************************************************************
// Author  Sepideh Ghanavati, April2007
// - Original version by Gunter Mussbacher, May-Jun2005
// - Based on initial version by Bo Jiang
*****************************************************************/
// global constants
const string projectFolderName = "/Compliance/"
const string orgFolderName = "Organization/"
const string legFolderName = "Legislation/"

// global constants for the legislation link and formal modules
const string fileNameLegSources = "Sources"
const string fileNameLegDef = "Legislation-Definition"
const string fileNameLegClause = "Legislation-Clause"
const string fileNameLegActors = "Actors"
const string fileNameLegIntentionalElements = "Intentional Elements"

// global constants for the organization link and formal modules
const string fileNameOrgIntentionalElements = "Intentional Elements"
const string fileNameOrgActors = "Actors"
const string fileNameOrgComponents = "Components"
const string fileNameOrgResponsibilities = "Responsibilities"
const string fileNameOrgComplies = "Complies"
const string fileNameOrgResps = "resps"
const string fileNameOrgTraces = "Traces"
const string fileNameOrgUrnLinks = "Urn Links"

// organization formal modules
Module orgActorModule
Module orgIntentionalElementModule
Module orgComponentModule
Module orgResponsibilityModule

// organization link modules
Module orgTracesLinkModule
Module orgRespLinkModule
Module orgCompliesLinkModule
Module orgRespsLinkModule
Module orgUrnLinksModule

// legislation formal modules
Module legDefModule
Module legClauseModule
Module legIntetionalElementModule
Module legActorsModule

// legislation link modules
Module legSourcesLinkModule
```

URNModuleUtilities.dxl

```
/*****************************************************************
// Author Gunter Mussbacher, May-Jun2005
// - Based on initial version by Bo Jiang
// - provides services for a module
*****************************************************************/
//Global variable for the debug_level
//From 0 (no debug) to 5 (complete debug)
int debug_level = 5

/* method to print out debug messages */
void debug( string description, int level ) {
  if (level <= debug_level){
    print ("debug: " description)
  }
}
```

URNCompleteLinks.dxl

```
/*****************************************************************************
// Author Sepideh Ghanavati, April2007
// - Original version by Gunter Mussbacher, May-Jun2005
// - Based on initial version by Bo Jiang
*****************************************************************************/
/* initial entry point to the auto complete links script */
bool completeLinks() {
  current = folder (projectFolderName "")
  string legSources = projectFolderName "" legFolderName "" fileNameLegSources ""

  beginCompleteLinks()
  completeTransitiveLinks(orgIntentionalElementModule, fileNameOrgTraces, legSources,
fileNameOrgComplies)
  completeTransitiveLinks(orgActorModule, fileNameOrgTraces, legSources, fileNameOrgCom-
plies)
  completeTransitiveLinks(orgComponentModule, fileNameOrgUrnLinks, fileNameOrgTraces,
fileNameOrgResps)
  completeTransitiveLinks(orgResponsibilityModule, fileNameOrgUrnLinks, file-
NameOrgTraces, fileNameOrgResps)
  endCompleteLinks()
  return true
}
/* open all the references to the modules and link modules */
bool beginCompleteLinks() {
  int initOK = 1
  string buttons1[] = { "Complete", "Quit" }, buttons3[] = { "Ok" }

  initOK = messageBox( "Do you want to automatically complete links\nbetween the organi-
zation and the legislation?\n", buttons1, msgWarning )
  if( initOK == 1 )
    halt

  debug("init OK\n",3)
  // open all organization UCM modules for editing
  if( !( openOrgModules(orgFolderName) ) ) {
    messageBox( "One or more organization UCM modules could not be opened for edit-
ing.\nAuto Complete Links cannot proceed.\n", buttons3, msgError )
    halt
  }
  debug("opened all organization UCM modules for editing\n", 3)

  // open all required organization URN link modules for editing
  if( !( checkCreateOrgLinkModules(orgFolderName) ) ) {
    messageBox( "One or more organization URN link modules could not be opened for edit-
ing.\nAuto Complete Links cannot proceed.\n", buttons3, msgError )
    halt
  }
  debug("opened all required legislation URN link modules for editing\n", 3)
  // open all legislation UCM modules for editing
  if( !( openLegModules(legFolderName) ) ) {
    messageBox( "One or more legislation UCM modules could not be opened for edit-
ing.\nAuto Complete Links cannot proceed.\n", buttons3, msgError )
    halt
  }
  debug("opened all legislation UCM modules for editing\n", 3)

  // open all required legislation URN link modules for editing
  if( !( checkCreateLegLinkModules(legFolderName) ) ) {
    messageBox( "One or more legislation URN link modules could not be opened for edit-
ing.\nAuto Complete Links cannot proceed.\n", buttons3, msgError )
    halt
  }
  debug("opened all required legislation URN link modules for editing\n", 3)
  return true
}

/* save and close the modules and link modules */
bool endCompleteLinks() {
```

```
  string buttons[] = { "Ok" }

  bool saved = saveCloseFinal();
  debug("saved and closed\n", 3)
  messageBox( "Automatic link generation complete!", buttons, msgWarning)

  return true
}
```

URNInitExit.dxl

```
/*****************************************************************************
// Author Sepideh Ghanavati, April2007
// - Original version by Gunter Mussbacher, May-Jun2005
// - Based on initial version by Bo Jiang
*****************************************************************************/
/* open the references to the organization modules */
bool openOrgModules(string folderName) {
  Module currentModule
  bool preparationOKActors = false, preparationOKIntentionalElements = false
  bool preparationOKComponent = false, preparationResponsibility = false

  current = folder folderName

  orgActorModule = edit (fileNameOrgActors, false)
  orgIntentionalElementModule = edit(fileNameOrgIntentionalElements, false)
  orgComponentModule = edit(fileNameOrgComponents, false)
  orgResponsibilityModule = edit(fileNameOrgResponsibilities, false)

  for currentModule in current Folder do {
    if (currentModule."Name" "" == fileNameOrgActors)
      preparationOKActors = true
    if (currentModule."Name" "" == fileNameOrgIntentionalElements)
      preparationOKIntentionalElements = true
    if (currentModule."Name" "" == fileNameOrgComponents)
      preparationOKComponent = true
    if (currentModule."Name" "" == fileNameOrgResponsibilities)
      preparationResponsibility = true
  }
  current = folder projectFolderName
  return ( preparationOKActors && preparationOKIntentionalElements && preparationOKCompo-
nent && preparationResponsibility )
}

/* open the references to the organization link modules */
bool checkCreateOrgLinkModules(string folderName) {
  Module currentModule
  bool tracesOK = false, respOK = false, compliesOK = false, urnLinksOK = false

  current = folder folderName

  //complies link module
  if ( !( exists module fileNameOrgComplies ) ) {
    create( fileNameOrgComplies, "Complies", manyToMany, false )
  }
  orgCompliesLinkModule = edit( fileNameOrgComplies, false )

  //traces link module
  if ( !( exists module fileNameOrgTraces ) ) {
    create( fileNameOrgTraces, "Traces", manyToMany, false )
  }
  orgTracesLinkModule = edit( fileNameOrgTraces, false )

  //responsibility link module
  if ( !( exists module fileNameOrgResps ) ) {
    create( fileNameOrgResps, "resps", manyToMany, false )
  }
  orgRespLinkModule = edit( fileNameOrgResps, false )
```

```
  //urnlinks link module
  if ( !( exists module fileNameOrgUrnLinks ) ) {
    create( fileNameOrgUrnLinks, "urnlinks", manyToMany, false )
  }
  orgUrnLinksModule = edit( fileNameOrgUrnLinks, false )

  for currentModule in current Folder do {
    if( isEdit( currentModule ) ) {
      if( currentModule."Name" "" == fileNameOrgComplies )
        compliesOK = true
      if( currentModule."Name" "" == fileNameOrgTraces )
        tracesOK = true
      if( currentModule."Name" "" == fileNameOrgResps )
        respOK = true
      if( currentModule."Name" "" == fileNameOrgUrnLinks )
        urnLinksOK = true
    }
  }
  current = folder projectFolderName
  return (compliesOK && tracesOK && respOK && urnLinksOK)
}

/* open the references to the legislation modules */
bool openLegModules(string folderName) {
  Module currentModule
  bool actorsOK = false, intentionalElementsOK = false, clauseOK = false, defOK = false

  current = folder folderName

  legActorModule = edit(fileNameLegActors, false)
  legIntetionalElementModule = edit(fileNameLegIntentionalElements, false)
  legDefModule = edit(fileNameLegDef, false)
  legClauseModule = edit(fileNameLegClause, false)

  for currentModule in current Folder do {
    if (currentModule."Name" "" == fileNameLegActors)
      actorsOK = true
    if (currentModule."Name" "" == fileNameLegIntentionalElements)
      intentionalElementsOK = true
    if (currentModule."Name" "" == fileNameLegClause)
      clauseOK = true
    if (currentModule."Name" "" == fileNameLegDef)
      defOK = true
  }
  current = folder projectFolderName
  return (actorsOK && intentionalElementsOK && clauseOK && defOK)
}

/* open the references to the legislation link modules */
bool checkCreateLegLinkModules(string folderName) {
  Module currentModule
  bool sourcesOK = false

  current = folder folderName

  //complies link module
  if ( !( exists module fileNameLegSources ) ) {
    create( fileNameLegSources, "Sources", manyToMany, false )
  }
  legSourcesLinkModule = edit( fileNameLegSources, false )

  for currentModule in current Folder do {
    if( isEdit( currentModule ) ) {
      if( currentModule."Name" "" == fileNameLegSources )
        sourcesOK = true
    }
  }
  current = folder projectFolderName
  return (sourcesOK)
}
```

```
/* save and close all modules for a specified folder */
bool saveCloseAllModules( Folder theFolder ) {
  Module currentModule
  bool allClosed = true

  // loops through all OPEN modules in a folder
  for currentModule in theFolder do {
    save currentModule
    close( currentModule, true )
  }
  for currentModule in theFolder do {
    allClosed = false
    break
  }
  return allClosed
}

/* save and close the modules for this library */
bool saveCloseFinal() {
  bool finalOK1 = false, finalOK2 = false, finalOK3 = false

  current = folder (projectFolderName "")

  //close the legislation folder
  current = folder (legFolderName "")
  finalOK2 = saveCloseAllModules( current() )
  closeFolder()

  //close the organization folder
  current = folder (orgFolderName "")
  finalOK1 = saveCloseAllModules( current() )
  closeFolder()

  //close the project
  finalOK3 = saveCloseAllModules( current() )

  return ( finalOK1 && finalOK2 && finalOK3  )
}
```

URNLinks.dxl

```
/*************************************************************************
// Author Sepideh Ghanavati, April2007
// - Original version by Gunter Mussbacher, May-Jun2005
// - Based on initial version by Bo Jiang
*************************************************************************/
/* verify the existence of a link */
bool alreadyLinked( Object sourceObject, Object targetObject, string theLinkModuleName )
{
  Link l

  for l in sourceObject->theLinkModuleName do {
    if( target l == targetObject ) {
      return true
    }
  }
       return false
}

/* build transitive links from one organization formal module to the others specified by
the link modules */
bool completeTransitiveLinks ( Module elementModule, string link1, string link2, string
transitiveLink ) {
  Object currentObject
  Object targetObject_L1, sourceObject_L1
  Object targetObject_L2, sourceObject_L2
```

```
  Link l, l2, newLink

  current = folder (projectFolderName "" orgFolderName "")
  for currentObject in elementModule do {
    for l in (currentObject)->link1 do {
      targetObject_L1 = target l
      sourceObject_L1 = source l
      if(!null(targetObject_L1)) {
        for l2 in (targetObject_L1)->link2 do {
          sourceObject_L2 = source l2
          targetObject_L2 = target l2
          if(sourceObject_L2 == targetObject_L1) {
            if( !( alreadyLinked( sourceObject_L1, targetObject_L2, transitiveLink) ) ) {
              newLink = sourceObject_L1-> transitiveLink->targetObject_L2
              Module sourceM = module(sourceObject_L1)
              Module targetM = module(targetObject_L2)
              debug("created " transitiveLink " link from " sourceM."Name" "-" num-
ber(sourceObject_L1) " to " targetM."Name" "-" number(targetObject_L2) "\n", 3)
            }
          }
        }
      }
    }
  }
       return true
}
```